Find out more
www.thebci.org

Thought Leadership

BCI Horizon Scan Report 2022

bsi.

Leading the way to resilience

Contents

Foreword

I am pleased to introduce the 2022 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.

This year's report falls at a critical point. Organizations are, in many countries, starting to return to a degree of normality after COVID-19 severely disrupted operations for two years. However, with the waning of COVID-19, the world is now faced with the Ukraine crisis.

We noted in our 2020 report how organizations were sorely unprepared for COVID-19. The statistics showed that non-occupational disease — which includes pandemic — was at the second bottom of the list in terms of concerns for 2020. The survey closed at the end of December 2019. Meanwhile, this year's report shows that Business Continuity, Resilience and Risk professionals' thoughts remain dominated by the pandemic, with incidents such as exchange rate volatility, political change, violence and civil unrest and natural resources shortages ranking towards the bottom of the table for concerns for 2022. The survey for this year's report closed just before news of the escalating situation in the Ukraine was first discussed in the media.

Organizations have made significant learnings from the pandemic — business continuity and resilience staff have been propelled to the forefront of many organizations by senior management. This has resulted in practitioners' roles becoming more strategic with leadership and boards asking for guidance about how new strategies will work from a business continuity and resilience perspective. Funding has increased, staffing levels have risen and there is an increased demand for training and exercising. There has also been an eleven percentage point increase in the number of organizations who are now using the ISO 22301 standard as a framework.

However, while our industry has made significant progress since the start of the pandemic, horizon scanning and risk mapping still needs improvement for many organizations. The most astute professionals had seen issues developing in Ukraine weeks before the mainstream news broke out and spent time firming up cyber security and reviewing supply chains.

The primary learning from this report is that we still need to be prepared for the unexpected. While we have seen many members breathe new life into their programs and our industry over the past two years, there is still work to be done in terms of risk planning and ensuring organizations are prepared for anything — however unlikely it may appear at the time.

I would like to thank our members and contacts once again for their valuable insight in making this report possible. We have once again been inspired by some of the stories we have heard in our interviews and would like to thank practitioners for being at the forefront of ensuring their organizations and industries are truly resilient. I would, once again, like to offer my sincere appreciation to the BSI for the continued and valued support of this report.

Christopher Horne FBCI
Chair of the BCI

Foreword

The latest BCI Horizon Scan Report 2022 reveals the key issues that have dominated organizations' risk landscapes over the last year and the ones expected to dominate in the coming years.

Organizational Resilience is an overarching topic on which BSI has been working for many years, and we are pleased to continue the collaboration with the BCI on how business continuity expertise and best practices contribute to resilience.

The latest insights shed light on the ongoing and emerging global risks and threats for organizations, their people, their data, and their extended value chains and ecosystems.

This year's report recognises the inter-connected world we live in as business continuity has been challenged yet again in the face of economic uncertainty. It has proven once again increasing relevance in helping organizations better prepare to face the climate crisis, changing working practices and other major disruptions.

The report makes clear the threat of the pandemic still lingers in 2022, with non-occupational disease becoming the primary perceived risk to organizations and their staff.

Hybrid workplace environments are increasingly testing organizations and bringing additional risks — from health and safety concerns to wellbeing issues to ensuring homeworkers' remote environments are as resilient as those in the office — meaning cyberattacks and data breaches will be critical considerations for organizations for years to come.

The findings show that the consequences of any disruption are not just organizational but predominantly human, particularly on staff morale and wellbeing. That is why those companies that focus on their people will in turn increase their potential agility and ultimately their resilience.

It is encouraging to see the progress achieved in using best practice standards, not only the international standard on Business Continuity Management Systems (ISO22301) but also other good practices that contribute to the resilience of companies, large and small.

Organizations that continue to embed best practice to increase the agility of their teams will be better prepared to adapt to new, emerging global risks as well as to unpredicted and somewhat unpredictable events.

This report, even more than previous editions, confirms that leaders who continue to focus on enhancing the resilience of their organizations in the constantly changing and turbulent business environment will become more trusted, more resilient and, ultimately, future-ready.

Pietro Foschi
Group Executive Director Assurance Services
BSI

Horizon Scan 2022
Executive summary

Executive summary

Preparing for the unexpected: The 2020 and 2021 editions of Horizon Scan showed that many organizations were not prepared for the disruption caused by COVID-19. Plans had to be rewritten from scratch, technology hardware had to be sourced through disrupted supply chains and workplace environments had to be altered to ensure staff could work remotely and, for those that could not, strict social distancing policies had to be adhered to. Organizations spoke about how they will now be considering risk on a much broader scale, so similar 'surprises' could be mitigated for the future. Whilst progress has been made, the crisis in the Ukraine has also caught many organizations by surprise. Respondents spoke how they would now change their answers to the survey, ranking risks such as 'political conflict' higher, had they known about the Ukraine crisis earlier. Preparing for the unexpected is a primary theme for this year's report.

Hybrid workplace environments are testing organizations: Organizations are now 'normalising' their working environments now COVID is proving less of a threat to life and staff are able to return to offices. For many organizations, this means continued remote working or working in hybrid environments which both come with risks: from health and safety concerns and mental health issues to ensuring homeworkers' remote environments are as resilient as those they would expect in the office.

Non occupational disease remains the primary perceived threat to organizations and their staff: Risks belonging to natural domain, ranging from the possibility of new viruses to extreme weather events, are something practitioners need to address regardless of industry, country, and size. In this regard, respondents state that climate change will be one of the greatest threats in the next five years.

Cyber threats increased during the pandemic – and are now on a steep rise again: Cyber security is the second-ranked concern for the following year after non-occupational disease. Cyber-security concerns increased during the pandemic with criminals exploiting homeworkers through social engineering and targeting hastily constructed networks that lacked security. The crisis in the Ukraine has caused a four-digit percentage point rise in cyber-crime since the invasion began, with attacks causing more devastation for some organizations than ever noted previously.

Supply chain disruptions are also on the rise, as the global shortage for several types of products and services continues: Supply chain threats can arise from several types of challenges, whether these are human resource management, biological and environmental risks, civil unrest or cyber resilience issues. Indeed, as recently as 1 March, Toyota announced that it was halting production due to a cyber-attack on one of its critical suppliers.

Management are better understanding the importance of resilience and business continuity management in their organizations: Respondents reported better management of disruptions in the past year thanks to international best practices. Indeed, Management were driving greater adherence to international standards (such as the ISO 22301 standard) leading to improved relationships between resilience-orientated departments. It is time for the several management disciplines to come together and work with units that so far have not been included enough in the resilience discourse, such as change management.

Risk and threat assessment

Past twelve months

Non-occupational disease has continued to dominate agendas during 2021

Non-occupational disease:
24.5

Remote work:
24.3

Travel restrictions:
21.5

Health incident:
17.9

Lack of talent:
17.3

Next twelve months

Are we prepared for the unexpected? Non-occupational disease is still considered the primary risk for 2022

Non-occupational disease:
7.8

Cyber attack & data breach:
6.9

Travel restrictions:
5.6

Remote work:
5.0

IT and telecom outage:
4.9

Consequences of disruption

The human consequence of disruption is having the most impact on organizations

Negative impact on staff morale/wellbeing/ mental health:
68.1%

Loss of productivity:
62.1%

Staff loss or displacement:
44.3%

Loss of revenue:
42.0%

Supply chain disruption:
41.3%

ISO 22301 update

Certifications were down slightly in 2021, but uptake of the standard as guidance has increased by eleven percentage points

We use ISO 22301 as a framework but are not certified to it:
56.0%

We use ISO 22301 as a framework, are not certified to it, but are in the process of getting certified:
5.3%

We use ISO 22301 as a framework and certify to it:
9.8%

We don't currently use ISO 22301 as a framework but we intend to move towards this during 2022:
7.6%

We don't use ISO 22301 as a framework and have no plans to move towards this during 2022:
21.3%

Benefits of certification

The external benefits of certification and exhibiting to stakeholders the effectiveness of BCM programmes are the prime certification benefits for organizations

Allows us to demonstrate the effectiveness of our BCM programme to external stakeholders:
74.0%

Increases our organization's resilience:
74.0%

Enables the management of disruption:
60.0%

Enables consistent BCM measurement and monitoring:
60.0%

Enables faster recovery after a disruption:
54.0%

Benchmarking longer-term trend analysis

Most organizations carry out risk and threat assessments to perform trend analysis, but use of other sources is sporadic in some organizations

Internal risk and threat assessment:
88.2%

External reports/ industry insight:
77.3%

Risk registers:
71.4%

Participation to industry events/conferences:
62.3%

Social media monitoring:
39.6%

Investment in business continuity

Just 8% of organizations expect invest in business continuity to be cut in 2022

Investment levels will be increased:
33.9%

Investment levels will be maintained:
46.6%

Investment levels will be decreased:
8.1%

Overview

Last year's Horizon Scan Report captured a risk landscape that remained dominated by COVID-19 and told how the virus had caught most practitioners unaware. The 2020 report — published at the beginning of the pandemic — had non-occupational disease featuring second from bottom as a future risk. The survey for the 2020 report closed just a day before the news of COVID-19 first broke out.

The 2021 report served as a lesson in being prepared for the unexpected. Respondents explained how the experience of COVID-19 had encouraged their organization to take a broader view of risk and consider more of those risks which had previously been deemed unlikely to happen. This year's report shows a similar picture to the 2020 Horizon Scan. Respondents filled in the survey in December and early January, and still placed non-occupational disease as their top threat for 2022. However, when speaking to some of the respondents, many told how they would now change their answers given the escalating situation in Ukraine.

The Ukraine conflict is affecting global supply chains and setting financial markets into shock. According to a large managed services provider in the United States, cyber-attacks have increased by 800%[1], causing major damages to organizations' operations.[2].

That said, being aware of wider risks is a theme which came from both the survey and interviewees, and the attention of management towards the risk and the business continuity processes around this remains heightened. A greater appreciation of resilience is now widespread amongst organizations: 22.2% of interviewees reported their organizations had created the role of Chief Resilience Officer at board-level in the past year.

Some of this heightened awareness by management is also being seen in the uptake of standards. We have noted an 11-percentage point increase in the number of organizations who are choosing to align to ISO 22301 standard. Moreover, whilst there has been a slight dip in certifications this year, many practitioners report that certification is now a possibility for their organization for the first time.

Once again, this report continues to be a lesson on preparing for the unexpected, as well as for incidents that can arise from a crisis such as COVID-19 and the escalating situation in Ukraine.

1. Burt, J. (2022). Dunno about you, but we're seeing an 800% increase in cyberattacks, says one MSP. The Register [online]. 11 March 2022. Available at : https://www.theregister.com/2022/03/11/russia-invasion-cyber-war-rages/ [accessed 15 March 2022]
2. Tidy, J. (2022). Ukraine crisis: 'Wiper' discovered in latest cyber-attacks. BBC News [online]. 24 February 2022. Available at: https://www.bbc.co.uk/news/technology-60500618 [accessed 15 March 2022]

Risk and threat assessment: past twelve months

Risk and threat assessment: past twelve months

- **The pandemic continued to dominate organizations' agendas in 2021.**
- **Supply chain concerns continued into 2021. The Suez Canal incident had a major impact, but global shortages of certain goods (such as microchips) remain endemic.**
- **Organizations are working hard to ensure they have failsafe cyber-security measures, but staying one-step ahead of attackers remains challenging, particularly with the ever-increasing number of attacks.**

For the second year running, the pandemic makes the top of the risk score index, with non-occupational disease (24.5) being the most impactful event of the last 12 months. However, whilst the risk score is significantly higher than that noted in 2020 (18.6), this is down to the frequency of events related to the pandemic. The impact score decreased year-on-year to 2.5 out of a possible 4 (2021: 3.2) as organizations started to understand COVID-19 better and adapted their processes and procedures accordingly. Indeed, interviewees described how COVID-19 had been increasingly considered business-as-usual (BAU) during 2021.

However, whilst organizations are getting better at managing the threat posed by COVID-19, the first four ranked incidents are directly related to the pandemic and its resultant effects on organizations. The responses demonstrated how COVID-19 caused a long series of knock-on effects in various areas, ranging from the transformation of business processes to the deterioration of mental health for personnel.

In this year's index, issues arising from remote work, or a new workplace environment were in second place with a score marginally lower than non-occupational disease (24.3). The shift to a different office paradigm is something which few organizations would have envisaged 24 months ago. As organizations around the world adapted to a significantly different way of working, employers had to ensure their workforce had the right equipment (e.g., laptops, stable connections) and that the office IT infrastructure was suitable enough to stand the test of physical restrictions. From a business continuity (BC) perspective, plans had to be rewritten to ensure workers had the same BC backup that they would if they were working in the office. Although many respondents admitted that there was still work to be done to ensure remote workers were covered from a BC perspective, some organizations have this firmly integrated within their plans. One interviewee highlighted that they had gone so far as to request remote senior management staff purchase generators. Another said they ensured they had dual backup when operating in a remote environment.

"I meet with the department heads and senior management regularly and we discuss remote risks, what the impacts could be and how to mitigate those risks. Not only are we continually looking at them, but senior management is also continuously looking at it and keeping it in mind when trying to decide whether or not to keep certain people remote in certain locations. So, for example, when hurricane season is approaching we need to decide whether to bring workers into the office, make them remote, or ask them to work in another location. We are just trying to keep our options open. One of the things we have also done is asking some of the executive remote staff if they could purchase power generators. This decision was made after learnings from the Texas freeze last year. We had executive management that were unable to work for two weeks because cars were in the garage and the garage froze shut. Thus they were unable to use their car as a power source for their laptops. And they obviously couldn't go into the garage to start the car without the risk of carbon monoxide poisoning."

Senior Business Resiliency Manager,
Healthcare, United States

"For some critical roles which became remote, we had to give them dual links; dual service providers. This ensured that if one service process went down, we could give them an alternative by switching them across immediately. That's what we did for the critical teams that were managing those areas, and teams that are time bound by processes."

Head of Continuity Management,
Financial Services, Zambia

Our interviewee from Zambia - where internet banking is not widespread - explained that remote working has been an issue as most customers still want a 'bricks and mortar' bank. However, the particular practitioner used his experiences with a previous employer to ensure his current organization could run as effectively.

"My previous employer was [another major bank] where we had already established structures around remote working. So when I came here, I quickly set up the remote working and ensured testing took place. So when you do the testing many won't agree to it, but it's something that I have now had to start initiating as a way of testing the business continuity plans. There was a lot of pushback; they didn't realize what was coming up until COVID-19 hit the country. That's when everybody appreciated the testing that had gone on. Then we had to put in a hybrid working and put about 80% staff work remotely. For our branch network, we got branches to start rotating opening days and times. This impacted on our customer service as many people in Zambia still believe in brick and mortar queues and carrying out processes within a branch. Whilst there were lots of queues, we have now started delivering on the digital products."

Head of Continuity Management,
Financial Services, Zambia

In last year's Horizon Scan Report[3], Members also discussed the problem of 'double whammy' events. This was a particular concern for organizations in areas prone to extreme weather, where BC professionals were not only having to ensure continuity of operations during the pandemic, but also sometimes during 'double whammy' scenarios (such as bushfires and concurrent flooding). Many have learned from this and, as a result, are more prepared for future events.

One interviewee mentioned how they had had to alter their whole operating model to be able to cope with the changing consumer environment during the pandemic. This obviously required additional resource from business continuity.

In the near future, remote work is set to become a must-have for most organizations[4]. Furthermore, today's workforce is more aware of their right to choose an employer as much as an employer chooses them. Thus, a well-developed remote work policy has the potential to become a competitive advantage in attracting and retaining talent. Another effect of such change could lead organizations to move away from the mere quantification of work and pay greater attention to outcomes. In addition, remote work appears more environmentally friendly and socially responsible for a variety of reasons, such as fewer commutes and better management of stress levels.

Such changes lead to another risk for organizations that of talent attrition. This is why, in 2022, it is not surprising to see this lack of talent/key skills in fifth position, with a score of 17.3 (2021: seventh position; 12.1). One interviewee, based in Australia, commented that the lack of available IT personnel was creating a threat to the resilience of IT and telecommunications systems within their educational establishment. Another interviewee from a larger corporation also spoke about the lack of available IT and technical staff.

"One thing that is really prominent is the dependency on IT and telecom management and the consideration that there's not been any testing of our backup. So over the last two years I've been working with a number of IT managers, because of staff turnover, to understand this. Also, now schools are using technology to deliver education there has been little consideration for what would happen if it didn't work the way they thought it would. As a result, we're doing some scenario analysis across the school about what would happen if we actually lost communications for a day, a week, year? And the reliance on physical servers for so much raises additional questions."

Risk & Compliance Officer, Education, Australia

3. Elliott, R: BCI Horizon Scan 2021. The BCI. March 2021. Available at: https://www.thebci.org/resource/bci-horizon-scan-report-2021.html [accessed 15 March 2022]
4. Granieri, A (2020). How the Remote Work Revolution Will Change the Employer/Employee Relationship. Gartner.com. July 2020. Available at: https://www.gartner.com/en/human-resources/trends/remote-work-revolution [accessed 15 March 2022]

The same interviewee also commented how the pandemic had changed employees' working preferences. Many had become demoralised with the teaching environment, or with the possibilities of remote working, and wanted to work in a role which did not require a lengthy commute.

> **"Through the pandemic, the loss of staff experienced presents a loss of good talent and difficulty in finding suitable replacements. It's driven predominantly by people who just don't want to do this kind of work anymore or don't want to commute. Having to teach within an online environment didn't suit a lot of people in the industry. Initially I was concerned, but found it's widespread across Australia and some parts of the world. So that made me feel better. But it doesn't negate the issue that we have. I just don't have confidence in the IT process in itself."**
>
> Risk & Compliance Officer, Education, Australia

> **"The shortfall in availability of talent with key skills is a risk which has been openly acknowledged across the organization, such as IT engineers and cybersecurity specialists. COVID resulted in our migrant stream being stopped in Australia, which has always been a very strong source of talent for those sorts of skills for all organisations. Therefore, this is one that the organisation is looking at very hard as we build and improve our technology stack and the resilience."**
>
> Group Business Resilience Manager, Financial Services, Australia

Travel restrictions — another direct consequence of the pandemic — ranks third in the risk table, with a score of 21.5. Hindrances to free movement, both locally and internationally, have been at the top of the agenda in recent times, with different countries adopting different policies, which have generated confusion and mental fatigue for citizens. It is also worth noting that such policies have often changed due to updates in the rates of infection and vaccination. In this regard, the uneven access to vaccines has led to a significant advantage for some countries who were able to acquire vaccines easily, whereas some were — and still — have not received enough. This means that trade is highly facilitated for richer countries, who can reopen and restart production earlier than those left behind. The world average of individuals having completed the vaccination cycle stands at 62%, and while countries in Europe and North America are well above those levels, several developing countries have yet to reach 10%[5].

Health incidents (non-COVID related) are in fourth place in this year's risk index. The category, which includes occupational disease and mental health, was second in last year's report and, if it were not for the two new incident categories of remote working and travel restrictions being added in this year's report, it would most likely be in second place again.

UK statistics reports on health and safety are a good example of how worrying and complex the situation is. Without considering the direct impacts of COVID-19, 1.7 million workers in the UK suffer from work-related illness, with roughly 800,000 of them dealing with stress, depression, and anxiety, and an additional 500,000 battling musculoskeletal disorders. Furthermore, incidents in the workplace still affect nearly half a million individuals every year[6]. Although the overall risk index score fell marginally this year to 17.9 (2021: 18.2), the frequency score for health incidents is higher this year (9.4) than last year (7.8). It appears that whilst organizations may be getting better at offering support to staff who may be experiencing difficulties, the frequency of such issues shows no signs of abating.

As discussed above, lack of talent and key skills (17.3) rounds up the top five, confirming that today's organizations need to do more than simply advertise a vacancy to get the right candidate for the job.

5. Our World in Data (2022): Coronavirus (COVID-19) Vaccinations. OWID. Available at: https://ourworldindata.org/covid-vaccinations [accessed 15 March 2022]
6. UK Health & Safety Executive (2021): Health and Safety at work. HSE/National Statistics. Available at: https://www.hse.gov.uk/statistics/overall/hssh2021.pdf [accessed 15 March 2022]

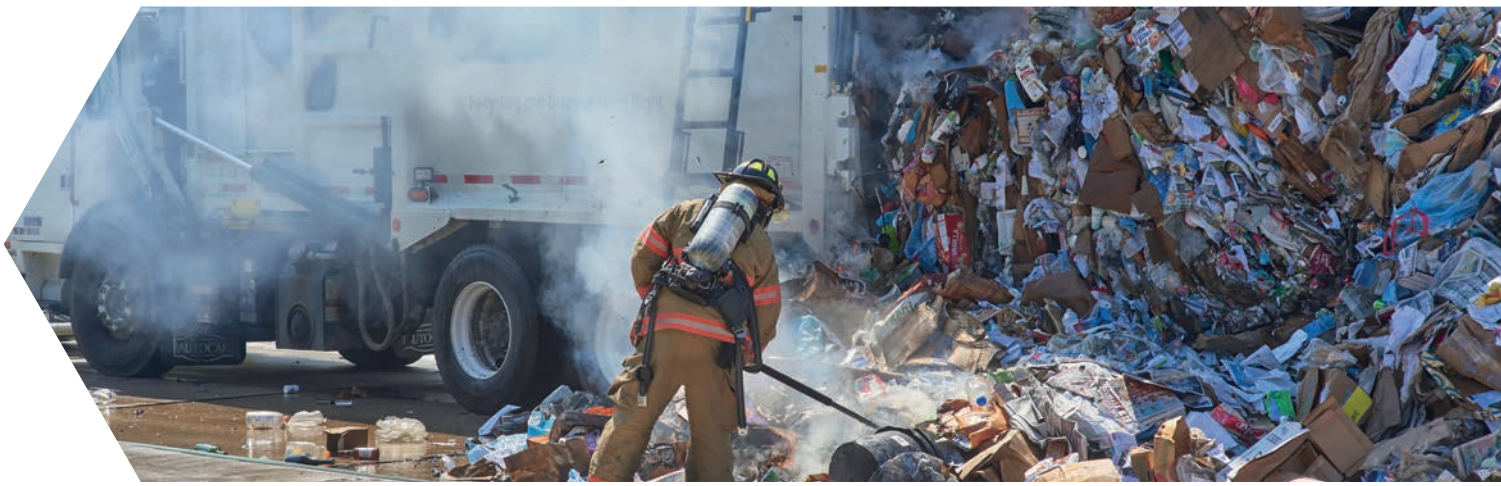
Workers are now more demanding with their requirements for jobs (e.g. requiring full-time remote working, extra benefits), others have left their sectors entirely or, in the case of some, left for other countries because government rule changes stopped them working because of escalating violence, or because they could work for other organizations remotely from abroad.

In the past year, increasing numbers of workers have been leaving their jobs mainly due to working conditions and job satisfaction — so much so that this phenomenon has been nicknamed the 'Great Resignation'[7]. 2020 proved to be a wake-up call for many employers to reassess their priorities and focus on their employees' physical and mental health. Indeed, the way employers behaved through the pandemic showed a tangible link to their ability to retain employees. This, much like remote work, is a challenge that is here to stay; thus, employers should ensure they remain ahead of their peers in terms of employee support and remuneration or they may hit problems with talent retention and acquisition. As a valuable addition to their analyses, organizations should run competitive intelligence programmes and map out competitors' staff packages.

On a similar note, physical safety incidents (14.5) are another prominent issue which relates to workforce retention. In last year's report, this category saw an increased risk score of 16.1; which was blamed in part to staff absences which required unqualified staff to operate machinery, and incidents in remote working environments which had not been subject to risk assessments. This year, thankfully, the lowered score suggests that organizations are now taking more consideration of unsafe working environments, and we are anecdotally hearing that more organizations are undertaking video risk assessments of remote working environments.

However, a recent report by EcoOnline, the Hybrid Working Survey[8], showed that less than half of organizations (47%) have provided training for staff in issues such as home office ergonomics, remote communications or techniques for isolation. Moreover, a third of organizations (32%) have failed to carry out risk assessments for workers' remote environments. As organizations' post-pandemic working models are beginning to be set in stone, and remote/hybrid environments are becoming the norm in many sectors, ensuring that basic risk assessments are carried out on workers' remote setups should be at the top of the list for HR and/or operations management.

An interviewee highlighted how meeting the challenges of operating within different regions in the UK during COVID was difficult as each region had different rules to adhere to which created safety concerns. The same interviewee also added that changing working conditions during the pandemic had resulted in an increase in fires at waste depots as the increased population working from home meant an increase in the number of batteries being incorrectly disposed of. This demonstrates that resilience professionals should not just think about the direct implications on business continuity in the event of a pandemic but consider the wider context of how knock-on effects in changing consumer behaviours will impact the business.



7. Morgan, K (2021). The Great Resignation: How employers drove workers to quit. The BBC [online]. 1 July 2021. Available at https://www.bbc.com/worklife/article/20210629-the-great-resignation-how-employers-drove-workers-to-quit [accessed 15 March 2022]
8. WcoOnline (2021): How have we managed the risks of Hybrid Working? EcoOnline. Available at: https://www.ecoonline.com/how-have-we-managed-the-risks-of-hybrid-working-survey (accessed 15 March 2022)

Supply chain disruption (13.3) ranks seventh in the risk score index (2021: 12.0). It is not surprising that supply chain made it to the top ten again — and with a higher risk score — given the ongoing global supply chain and logistics crisis. As economies struggled, the demand for essential goods increased dramatically, placing an ever-greater pressure on suppliers to deliver, particularly against a backdrop of increasing consumer propensity for online ordering adding additional workload to light haulage. Adding fuel to the fire, the Suez Canal incident led to more delays and backlogs[9]. This, coupled with a general lack of focus on supply chain resilience, created the perfect storm for the global logistics industry to enter into a crisis that seems to be still far from over. Unfortunately, building response and recovery capabilities within supplier networks has not received enough attention by organizations worldwide. As reported in the *BCI's 2021 Supply Chain Resilience Report*[10], most companies (80%) have BC arrangements in their supply chain, but only about half of them seek some sort of verification such as evidence of exercises or proof of certification.

> **"We saw a big disruption to supply of IT equipment in 2021 because of the worldwide post-Covid chip shortage and the Suez Canal blockage, 6 days in March 2021. Anything with a chip, not just computers, but lots of electronic equipment. That was a once-in-a lifetime occurrence. The impact was completely unexpected because nobody realized how much stuff was coming through the Suez Canal to Ireland."**
>
> Business Continuity Professional, Higher Education, Ireland

Moving away from physical threats, eighth and ninth place in the risk score features IT and telecom outage (12.3) and cyber-attacks and data breach (11.7) respectively. While compared to last year, these two risks are down from fifth to sixth place, they still represent a significant challenge for organizations.

Cyber resilience should be a critical asset for modern organizations, and it is a key capability due to the growing digitization of business processes, remote work, and uptake of e-commerce. As the world relies more and more on hybrid workplace environments, it is essential that IT infrastructures are reliable and secure. In the last two years, cyber-attacks have not only increased, but they have also been tailored to current events. Phishing emails with links to fake healthcare portals, targeted attacks to hospitals, and charity donations scams are now among the preferred attack vectors in the online criminal underworld. The larger adoption of virtual processes has broadened the attack surface for perpetrators that can take advantage of weaknesses such as more access points, low computer literacy, and inability to distinguish reliable sources on the internet.

However, with cyber-attack and data breach nearing the top of the table for future risks in 2022, these particular incidents are top of mind for senior management and BC professionals. Furthermore, with global tensions increasing as a result of the Ukraine crisis, cyber security is likely to receive even more attention in organizations' plans.

9. Grynspan, R (2022). Here's how we can resolve the global supply chain crisis. World Economic Forum [online]. 17 January 2022. Available at: https://www.weforum.org/agenda/2022/01/resolve-supply-chains-crisis/ (accessed 15 March 2022)
10. Elliott, R (2021). BCI Supply Chain Resilience Report 2021. The BCI. Available at: https://www.thebci.org/resource/bci-supply-chain-resilience-report-2021.html (accessed 15 March 2022)

"The Board are very concerned about cyber security. Whenever there are any cyber events on the news, they always ask our CIO and CISO that preparedness question, 'What does this particular event mean for us? Could we be susceptible?'. And so that thirst for reporting is ever present. We used to do a quarterly board update, and that's been moved to monthly board updates just in the last few months as well. The pressure from above to demonstrate preparedness is 100% there."

Resilience Professional, Utilities, United Kingdom

"We have several staff who are joint appointments between the University and the Health Service Executive [HSE]. This also applies to other universities in Ireland that offer medical programs. When the HSE system was closed down, this caused knock-on effects with our linked machines too. It was a huge unintended consequence, because the attackers were aiming at the health system, but they got at the university system as well through the links between the university system and the health system."

Business Continuity Professional,
Higher Education, Ireland

An interviewee from the university environment explained how they were particularly vulnerable to cyber-attacks due to links with the health service authority - an external network. This demonstrates that professionals should ensure not only their systems are secure, but also that their linked systems have BC back-up in the event of a cyber-attack. On 14 May 2021, the Irish Health Service Executive (HSE) suffered a major ransomware cyber-attack which caused all of its IT systems nationwide to be shut down. It was the most significant cybercrime attack on an Irish state agency and the largest known attack against a health service computer system.

Rounding up the top ten, lone attacker and active shooter incident scored 11.1, rising from number 21 in the 2021 report. As highlighted in the 2021 Horizon Scan report, it is important that organizations do not disregard a certain risk only because it is not in the top half of the chart. It is always necessary to evaluate critical assets and understand whether they might be vulnerable to a specific event, as every process or service has its own specificities. For instance, facilities might be subject to physical violence, which registers the highest impact score after non-occupational disease. Such incidents also show how different environments can change the risk profile for a specific incident. In 2020, while many organizations were operating partially or entirely remotely, the risk from lone shooters was lessened. Now that organizations are returning to more office-based environments, the risk of onsite incidents (such as lone attackers) is likely to increase as a result.

Another important theme to follow is that of weather events, as the effects of climate change are becoming very visible. Therefore, strategic and operational activity to mitigate against climate risk is required now more than ever, both from a BC and regulatory perspective. The index includes several climate-related risks such as extreme weather (10.9) in 11th position, natural resources shortage (10.3) in 13th position, and natural disasters (7.9) in 22nd position. Although all these are outside the top 10, with increasing attention on climate risk on global corporation agendas, they are now being considered more readily within organizational risk registers — even for regions which were not traditionally associated with climate-related disruption.

Among the trends to watch, it will be important to pay attention to political violence (19th position with a score of 9.4) and energy price shock (18th position with a score of 9.2) as global tensions are on the rise due to the situation in Ukraine and other areas of conflict. Also, regulatory changes, 12th with a score of 10.9, might put pressure on organizations to implement better resilience measures, as in the case of the Operational Resilience directives issued by the Bank of England.

Rank	Event	Frequency	Impact	Risk Index
1	Non-occupational disease (e.g. pandemic)	9.7	2.5	24.5
2	(Issues arising from) remote working/new workplace environment	11.4	2.1	24.3
3	Travel restrictions	10.0	2.1	21.5
4	Health incident (NOT transmissible disease such as COVID but occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	9.4	1.9	17.9
5	Lack of talent/key skills	8.0	2.2	17.3
6	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	7.8	1.9	14.5
7	Supply chain disruption	6.3	2.1	13.3
8	IT and telecom outage	6.1	2.0	12.3
9	Cyber attack & data breach	6.0	2.0	11.7
10	Lone attacker/active shooter incident	4.8	2.3	11.1
11	Extreme weather events (e.g. floods, storms, freeze, etc.)	5.4	2.0	10.9
12	Regulatory changes	5.2	2.1	10.9
13	Natural resources shortage	5.2	2.0	10.3
14	Higher cost of borrowing	5.4	1.9	10.2
15	Interruption to utility supply	5.0	1.9	9.7
16	Exchange rate volatility	4.8	2.0	9.6
17	Political violence/civil unrest	4.9	1.9	9.4
18	Energy price shock	4.5	2.0	9.2
19	Political change	4.0	2.2	8.6
20	Introduction of new technology (IoT, AI, Big data)	4.4	1.9	8.4
21	Critical infrastructure failure	3.9	2.1	8.2
22	Natural disasters (earthquakes, tsunamis, etc.)	4.3	1.9	7.9
23	Enforcement by regulator	3.7	2.0	7.2
24	Product safety recall	3.2	1.8	5.6

Table 1. Please insert the frequency that events have occurred and the associated impact levels on your organization from the list of events below:

Risk and threat assessment: past twelve months

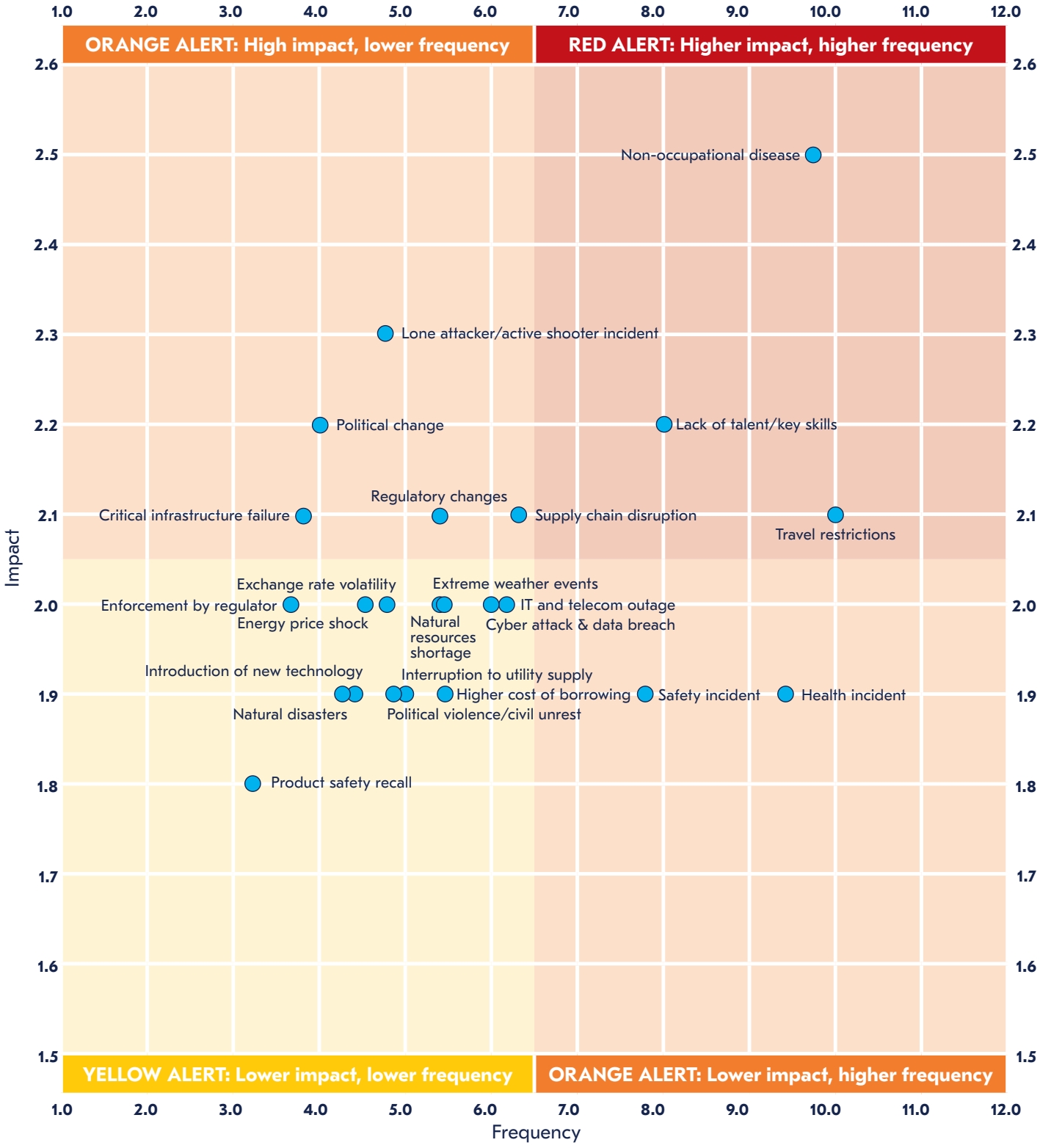


Figure 1. Risk and Threat Assessment: Past 12 Months

In addition to labeling the frequency and impact of all incidents over the past year, respondents were also asked what the cause for their largest disruption of 2021 was. It is of no surprise that the greatest disruption in the last twelve months was caused by non-occupational disease (35.8%), but it is interesting to observe that for 12.6% of the respondents, IT and telecom outage represented the most relevant event. As highlighted in the risk score analysis, the long-term switch to homeworking requires resilient IT networks and doing so on a permanent basis can be challenging. We are also seeing many organizations become increasingly reliant on one particular platform for all their IT and communications solutions. Whilst using a company such as Microsoft for all processes might be a satisfactory solution, from an operations perspective it does come with risks. A global Microsoft outage in April last year meant users were unable to access numerous Microsoft services, including Microsoft Office, Dynamics 365, Teams, OneDrive and Yammer[11].

The *BCI Emergency Communications Report 2022* also showed how many organizations were now routing all voice calls through voice-over-IP (VoIP) — and some even routing through Teams. If a backup solution is not in place, an organization risks losing all access to voice calls. Some organizations are now reverting to having PSTN backups to VoIP solutions but even some of those need careful consideration: in the UK, for example, the PSTN network is being grandfathered in 2025.

Supply chain disruptions (7.1%) were also problematic for organizations in 2021 and the lasting shortage of key components across different sectors is now starting to feel more of an endemic issue rather than a one-off incident. Furthermore, with newer complications entering the landscape, such as the conflict in Ukraine, supply chains are facing even greater challenges in the new future.

Completing the top five, extreme weather events (6.3%), remote work (5.9%), and travel restrictions (5.5%) were all equally significant in disrupting operations - revealing once more how complex and varied the threat landscape has become. In some parts of the world, extreme weather has caused more of an impact than the pandemic. For example, Madrid (Spain) witnessed its heaviest snowfall in 50 years; Fiji experienced category 5 cyclones; in the US, Texas saw heavy winter storms which resulted in 3.5 million businesses and homes left without power, and Oregon saw its largest bushfires in history.

New South Wales (Australia) suffered extreme flooding and in Europe, Germany was hit by heavy floods and Greece experienced extreme heat which sparked wildfires forcing evacuation of the country's island, Crete.

In isolation, these events could be considered as one-off events which can be treated as acute incidents and BC works to get essential services back up and running as soon as possible. However, some organizations are now admitting that climate risk is being seen as more of a 'chronic' risk and they are seeking to try and mitigate against more severe weather going forward (e.g. moving entire operations from at risk areas, providing staff with power backup if they cannot attend their place of work or choosing suppliers who are not located in at risk regions).

"We have invested a significant amount on flood defences in the last decade. Some substations and compressor stations are on flood plains but they've all been strengthened — literally raised up in places — and defences put in place for them. Climate change impacts on our resiliency is a definite concern with the rising temperatures. The more extremes that are becoming apparent, the more our resilience will be tested. We are making efforts to strengthen our whole network."

Resilience Professional, Utilities, United Kingdom

11. Abrams, L (2021). Microsoft outage caused by overloaded Azure DNS servers. BleepingComputer [Online]. 3 April 2021. Available at: https://www.bleepingcomputer.com/news/microsoft/microsoft-outage-caused-by-overloaded-azure-dns-servers/ (accessed 15 March 2022)

Please indicate below which of the above event was your most major disruption in the past year:

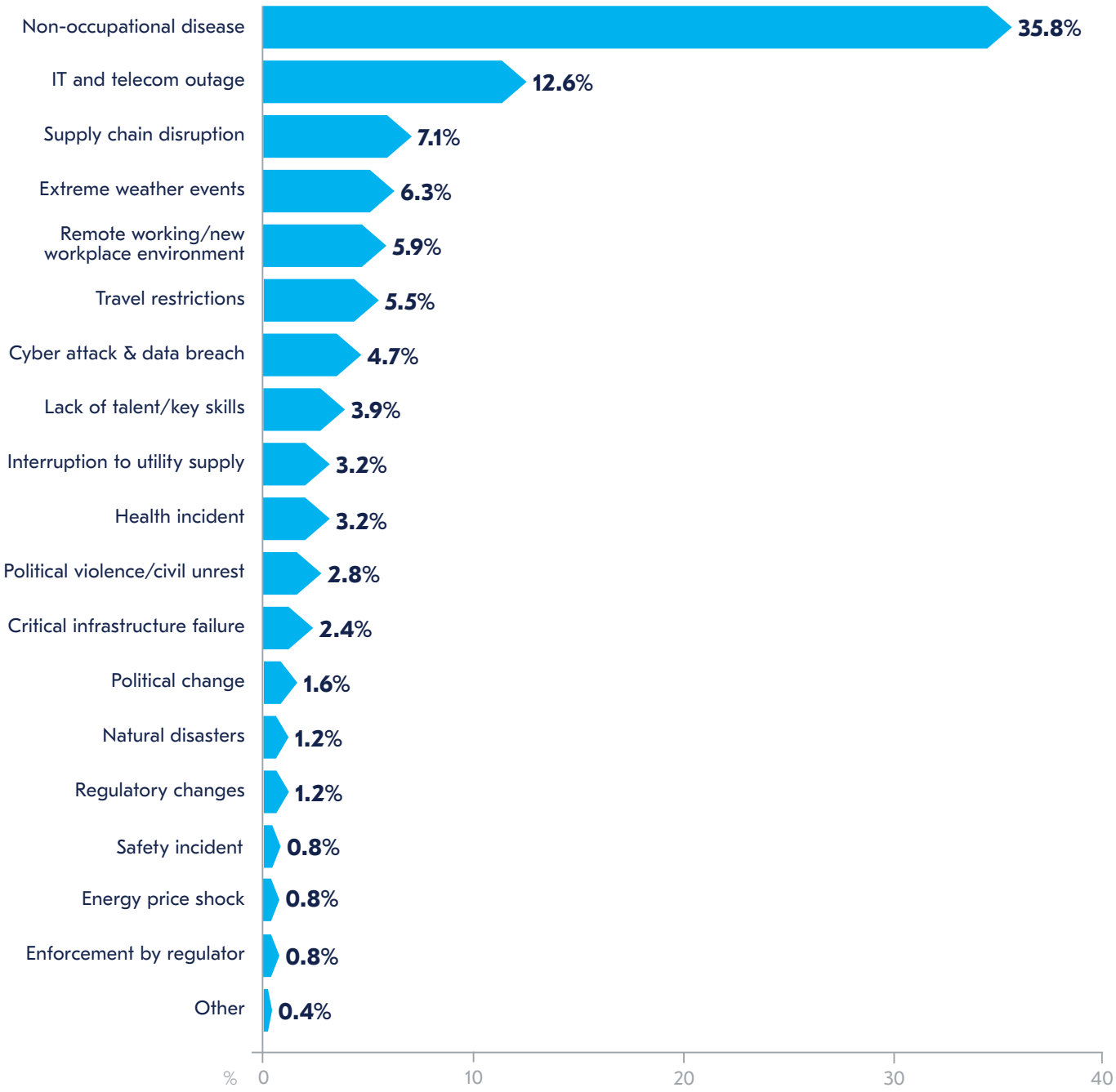


Figure 2. Please indicate below which of the above event was your most major disruption in the past year:

Risk and threat assessment: next twelve months

Risk and threat assessment: next twelve months

- **The pandemic remains top of organizations' concerns for 2022 – but is this still now the case with increasing global tensions?**
- **Cyber security strategies will be tested in 2022, with attacks now targeted towards global supply chains.**
- **IT and telecoms outages remain at the top of the list and, with organizations becoming increasingly dependent on a single platform for all communications, there is concern that many do not have sufficient back-up processes in place.**
- **Severe weather continues to be a concern, although most organizations have yet to consider the chronic threat of climate change in their planning strategies.**

Participants reported non-occupational disease as their biggest concern for the upcoming twelve months, with a risk score of 7.8. This is understandable as the world is still suffering from the impacts of the pandemic, and organizations are still struggling to adjust to a new post-pandemic reality.

However, each year we comment on how the risk landscape is changing, but practitioners' concerns continue to divert to those risks to which they have been most exposed to in the previous year. With COVID being considered less of a threat to life in many countries, it might be considered that other incidents may be considered above non-occupational disease in terms of risk mapping. Indeed, interviewees who had selected the threat of 'non-occupational disease' as minor commented that other issues were now taking precedence in their own organizational risk landscapes. On this note, cyber risk is today one of the largest threats and, according to interviewees, is greater than it ever has been. Indeed, the previous section highlighted that cyber-attacks increased by around 50% in 2021 and concerns around state-sponsored cyber-crime and ransomware attacks are high. Starting in the weeks prior to the beginning of the conflict, the Ukrainian government and other public services were hit by distributed denial of service (DDoS) attacks, which caused significant outages within the region.

This resulted in retaliation towards Russia which experienced similar attacks in the days following[12]. As such, cyber-attack and data breach is the second highest concern for the next twelve months, with an overall score of 6.9 (2021: 6.6) and an estimated impact score of 2.2, the highest of the table. The concerns about cyber security are not just held by resilience professionals within organizations, but also by senior management: an interviewee highlighted how their management team was now requesting monthly meetings to receive updates about cyber security issues.

While these risks should not be overlooked, the 2021 *BCI Cyber Resilience Report*[13] has shown that, in the event of a cyber-attack, ensuring that different management disciplines work together is key to a successful response. Benefits include a shorter time of response, better crisis communications and prevention of cyber incidents. Unfortunately, many organizations still experience internal reluctance to true cooperation, as organizational silos are a real hindrance to building true resilience. A truly resilient mindset should consider external threats, but ultimately focus on its internal resources to orchestrate them in the best possible way to protect its critical assets. This is often not the case, and therefore organizations are not well placed to counter modern threats, which leaves ample room for attackers to exploit internal weaknesses.

An interviewee highlighted how the risks associated with cyber security were a critical concern for their organization. They explained that if their systems went down, it had the potential to not only hit consumers, but the wider Australian economy in general.

> **"The attention on cyber security is significant in terms of exercises, board engagement, expenditure and regulatory engagement. That investment is indicative of our position in the market - because if we have a two hour IT outage, we end up being front page news on the mainstream media because of the span of our digital market and penetration across Australia. We are increasingly realizing that if there is an issue with any of the major banks within Australia it has a large impact, not just on our retail customers, but on other institutions and even the Australian economy. The Australian government is also starting to become very aware of this too. We are, however, very fortunate that our board members have extremely good awareness of cyber issues."**
>
> Group Business Resilience Manager, Financial Services, Australia

Removing the risks associated with COVID-19 such as new workplace environments and travel restrictions, IT and telecom outage again appears towards the top of the risk index in fifth place with an overall score of 4.9. Although this is lower than last year's score of 5.2, interviewees unearthed significant concern for IT and telecom related issues in the year ahead. The *BCI's 2022 Emergency Communications Report* demonstrated how most organizations were now using voice-over-IP (VoIP) solutions for their telecommunications systems. Some were even routing all voice calls through Microsoft Teams. Whilst this is might be advantageous from both a cost and systems management perspective, it does open organizations to a two-fold threat: 1) in the event of an internet outage, no voice calls could be made over company phone systems; 2) an overreliance on a service from a single organization (such as Microsoft) could mean all systems fail in the event of a platform outage. This exemplifies the importance of a reliable back-up solution being put in place, although even this has to be researched carefully. Interviewees explained how they were seeking to reinstall copper line into their organizations to have a PSTN backup, but many countries are now looking to remove this traditional method of communication entirely. For example, in the UK, the PSTN and ISDN networks will be switched off in 2025 . Germany, Japan, Sweden, Estonia and the Netherlands have already made the switch — or are imminently about to do so. The target switch-off globally is 2030.

12. Barrett, B. (2022). Security News This Week: DDoS Attempts Hit Russia as Ukraine Conflict Intensifies. Wired.com [online]. 26 February 2022. Available at: https://www.wired.com/story/russia-ukraine-ddos-nft-nsa-security-news/ (accessed 15 March 2022).
13. Elliott, R. & Lea, D (2021). BCI Cyber Resilience Report 2021. The BCI. Available at: https://www.thebci.org/resource/bci-cyber-resilience-report-2021.html (accessed 15 March 2022)

Ranking respectively third and fourth, travel restrictions and remote working, are two additional consequences of the shift in workplace mode caused by the virus. As discussed in the previous section, they have been a challenge in the past twelve months, and they will continue to be in the upcoming year. This shows that professionals are still battling with problems associated with change management, an overlooked topic when it comes to business continuity and resilience. However, in the past two years, the boundaries between change management and the protective disciplines have become increasingly blurred.

Most changes in the workplace now carry some issues in terms of business continuity, whether it is about being able to fly staff to a different country, choosing a new supplier, or allowing a large part of the workforce to operate remotely. Furthermore, now that many organizations are looking to organise themselves in an entirely remote environment or hybrid environment permanently, 2022 will be the year that the foundations will be made for these new working practices going forward. New business continuity plans will have to be built to cater for the new working environment and the organization is likely to face new risks. Embedding these new practices into organizations will take time and there will be some organizations which will face disruption as a result.

Despite not being among the greatest causes of disruption in the past year, extreme weather events, critical infrastructure failure, and regulatory changes all rank as joint sixth with a score of 4.8, making it to the top ten concerns for 2022. Issues concerning weather events and critical infrastructure are of the utmost importance as they also figure specifically among the seventeen UN Sustainable Development Goals, under Climate Action and Industry, Innovation and Infrastructure. Efforts regarding climate change have intensified noticeably in recent years, increasing pressure on both governments and the private sector to prove they are implementing sustainable policies.

Future requirements in the form of regulations and legislations might turn this into an even more significant challenge for professionals. Thus, if organizations want to stay relevant, they need to show that they are acting ethically and that means respecting global efforts towards a more sustainable, fair and equal society. Going forward, whether or not an organization believes that the increase in severe weather incidents is down to climate change or not, organizations will have to be more prepared and consider reviewing severe weather incidents as chronic, rather than acute risks.

An interviewee in the UK explained how Government legislation on sustainability and carbon reporting was going to be a major challenge for them in the short- to medium-term. Furthermore, if legislation was not adhered to, there was the additional risk of losing a director which could invoke significant financial loss to the business.

Another interesting discrepancy between the risk assessment of the last twelve months and that of the year ahead concerns human resources. Lack of talent and key skills ranked ninth, despite being the fifth cause of disruption, meaning that respondents appear slightly more confident in finding the right candidate for internal vacancies in the next twelve months. Similarly, in 2021, health incidents came fourth in the risk index and slide down to tenth place when it comes to future concerns. This is an interesting trend, as the job market is undergoing important changes, with employees reclaiming a significant part of their negotiating power when it comes to their relationship with current or prospective employers. Equally, mental health formed a large component of those who viewed 'health incidents' as a major disruption in 2021. As organizations return to office environments, the assumption might be that mental health episodes reduce. However, in reality there are other risks that can have an impact on mental health — including global geo-political instability. It is important that organizations retain the focus on mental health and wellbeing that was borne out of the pandemic.

We are at a point in time where physical and mental health are becoming a central part of conversations around hiring and retaining skilled staff. In addition, safety incidents only rank as fourteenth for future concerns, despite ranking as sixth in the 2021 risk index. There is a possibility that as organizations return to office environments, safety incidents may reduce as onsite training can return. With new working practices now endemic, new safety guidelines will have to be drawn up, new equipment may be bought which will require additional training and the risks associated with working in a physical environment will return. Therefore, it might be expected that safety incidents would be higher up the risk agenda for 2022.

Historically, staff safety and wellbeing have been less of a priority than they should be as they do not carry a feeling of imminent threat such as cyber-attacks or natural disasters. However, the way management treat their staff will be a success factor going forward. Those organizations who fail to update health and safety policies and procedures face losing staff in favour of those organizations who acknowledge the importance of the health, safety, and dignity of their workforce.

Supply chain disruptions should not be overlooked too as the global supply chain crisis continues and the importance and complexity of this issue fails to attract the right attention. At the start of the pandemic, several organizations fell short of satisfactory supply chain resilience levels. As such, this needs to be a prime focus going forward. Supply chains are the very fabric of the global economy. The ability to ship goods efficiently across countries is the foundation of sustainable international trade deals, which support healthy national economies and provide access to goods — including primary ones — across the globe.

Unfortunately, because they are so embedded in the fabric of organizations, supply chains are also affected by most types of business challenges that are out there. Transportation and shipping can be affected by new regulations, extreme weather events, political violence and, in recent years, by cyber-attacks.

In the last year only, several energy suppliers (such as the US Colonial Pipeline) experienced cyber-attacks, shedding light on the vulnerability of critical infrastructure towards online threats. Organizations should always understand who their critical suppliers are and engage in conversations to increase resilience levels. It is understandably tough to do so through the entire network.

A good first step is starting with Tier 1 suppliers to establish a first line of defence and then cascade through tier 2, tier 3 and beyond. Equally, ensuring that due diligence of suppliers is done at the procurement stage of the process is encouraged. This enables any potential issues to be raised before entering into a contract which can be too late.

An interviewee highlighted that supply chains are a key vulnerability in terms of resilience. For example, if one of an organization's critical suppliers is hit by a cyber-attack, it can have an immediate effect on supplies, which can lead to stalling of production. Such incidents are already happening globally: Toyota announced at the beginning of March that a cyber-attack had affected one of its critical suppliers and 28 lines of production were halted. As a result, the company lost production of 13,000 vehicles[15].

"One are that we are focussing on is supply chain disruption. Recent incidents have shown to everyone how fragile supply chains are. And even with our key suppliers that we work very closely with, there's a degree of uncertainty and lack of control over all aspects. So for instance, if one of our major technology partners who provide critical services to us was to have a major ransomware attack that would potentially have quite a large impact upon us."

Group Business Resilience Manager,
Financial Services, Australia

15. Green, W. (2022). Cyber-attack on supplier halts Toyota production. CIPS [online]. 1 March 2022. Available at: https://www.cips.org/supply-management/news/2022/march/cyber-attack-on-supplier-halts-toyota-production/ (accessed 15 March 2022)

It is important that organizations rely on processes to establish resilience and not only on technological solutions. The introduction of new technology (which ranks twelfth) is an opportunity as well as a challenge. For example, when considering more automated processes, relying on algorithms only can be a double-axed sword as the machine can still be imperfect due to mistakes and biases in the programming phase. For instance, aggregators of large data are great for understanding the big picture of a certain phenomenon, but there may be inaccuracies when it comes to understanding more nuanced events. In this sense, over confidence in large aggregators of business data can be a risk in itself[16]. In addition to this, many organizations found themselves adopting new systems and technologies during the pandemic and are now looking to fully embed them within their organizations. The 2022 *BCI Emergency Communications Report*[17] showed that, during the pandemic, several organizations had bought in new solutions to aid with emergency communication in new work environments, but for 2022, they were concerned that embedding this new technology may lead to unwanted disruption of operations. One interviewee described how their organization had moved over to Google Suite which has helped to make their whole IT infrastructure both secure and adaptive to working in remote environments. Another highlighted how planned software upgrades had the potential to add a risk with severe impact to their organization. In this case, the resilience manager was working with the IT department to ensure several types of hosting environments were present to mitigate that risk.

"The more interconnected you make the networks and the way that we do business, the greater influence any breach can have within the day to day running of a business. Traditionally, it would have been in much more segregated from the outside world than it is today."

Resilience Professional, Utilities, United Kingdom

"One of our major concerns is IT, especially with the possibility of an outage. We've got a lot of proprietary software which we are upgrading at the moment. Because you're messing with the system, there's the possibility that it can go down. We have found that this has happened a lot – with a significant impact – but enough to stop our staff working for a number of hours. We can't afford to lose that much time and the impact to us is moderate to, at times, severe. We've always kept IT alert to this fact, and we now have other data centres, as well as extra servers on site. We're also building different types of environments."

Senior Business Resiliency Manager, Healthcare, United States

16. Laney, D.B. (2022). A Lesson In Flawed Metrics Design: The New Global Supply Chain Pressure Index. Forbes [online]. 6 January 2022. Available at: https://www.forbes.com/sites/douglaslaney/2022/01/06/a-lesson-in-flawed-metrics-design-the-new-global-supply-chain-pressure-index/?sh=5b61b89a2431 (accessed 15 March 2022)
17. Elliott, R. & Lea, D. (2022). BCI Emergency Communications Report 2022. The BCI. Available at: https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html (accessed 15 March 2022)

Legacy software still remains an issue within some organizations, particularly where systems had had updates delayed in recent years. One interviewee highlighted this was now an issue for them, particularly when coupled with the global shortage of silicon chips as they were now having difficulties acquiring new hardware.

> **"One of our issues is the global shortage of chips as it means that we might have to continue dealing with legacy equipment for the time being. Legacy equipment tends to cause a lot of disruption in the IT environment because technology capacity, demand from customers and demand for data storage, tends to increase. So the shortage of chips is something that will start impacting us as businesses."**
>
> Head of Continuity Management, Financial Services, Zambia

Rank	Event	Likelihood	Impact	Risk score
1	Non-occupational disease	3.9	2	7.8
2	Cyber attack & data breach	3.1	2.2	6.9
3	Travel restrictions	3.5	1.6	5.6
4	(Issues arising from) remote working/new workplace environment	3.6	1.4	5.0
5	IT and telecom outage	2.9	1.7	4.9
6	Extreme weather events (e.g. floods, storms, freeze, etc.)	3	1.6	4.8
7	Critical infrastructure failure	2.4	2	4.8
8	Regulatory changes	2.8	1.7	4.8
9	Lack of talent/key skills	2.6	1.8	4.7
10	Health incident (NOT transmissible disease such as COVID but occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	2.8	1.6	4.5
11	Supply chain disruption	2.5	1.7	4.3
12	Introduction of new technology (IoT, AI, Big data)	2.7	1.5	4.1
13	Natural disasters (earthquakes, tsunamis, etc.)	2.1	1.9	4.0
14	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	2.4	1.6	3.8
15	Lone attacker/active shooter incident	1.8	2.1	3.8
16	Interruption to utility supply	2.5	1.5	3.8
17	Enforcement by regulator	2.3	1.6	3.7
18	Exchange rate volatility	2.4	1.5	3.6
19	Political change	2.5	1.4	3.5
20	Political violence/civil unrest	2.2	1.4	3.1
21	Energy price shock	2	1.5	3.0
22	Higher cost of borrowing	2.1	1.4	2.9
23	Natural resources shortage	1.8	1.4	2.5
24	Product safety recall	1.5	1.4	2.1

Table 2. Please insert the likelihood and impact levels for each event in the following list that might occur in the next twelve months:

Risk and threat assessment: next twelve months

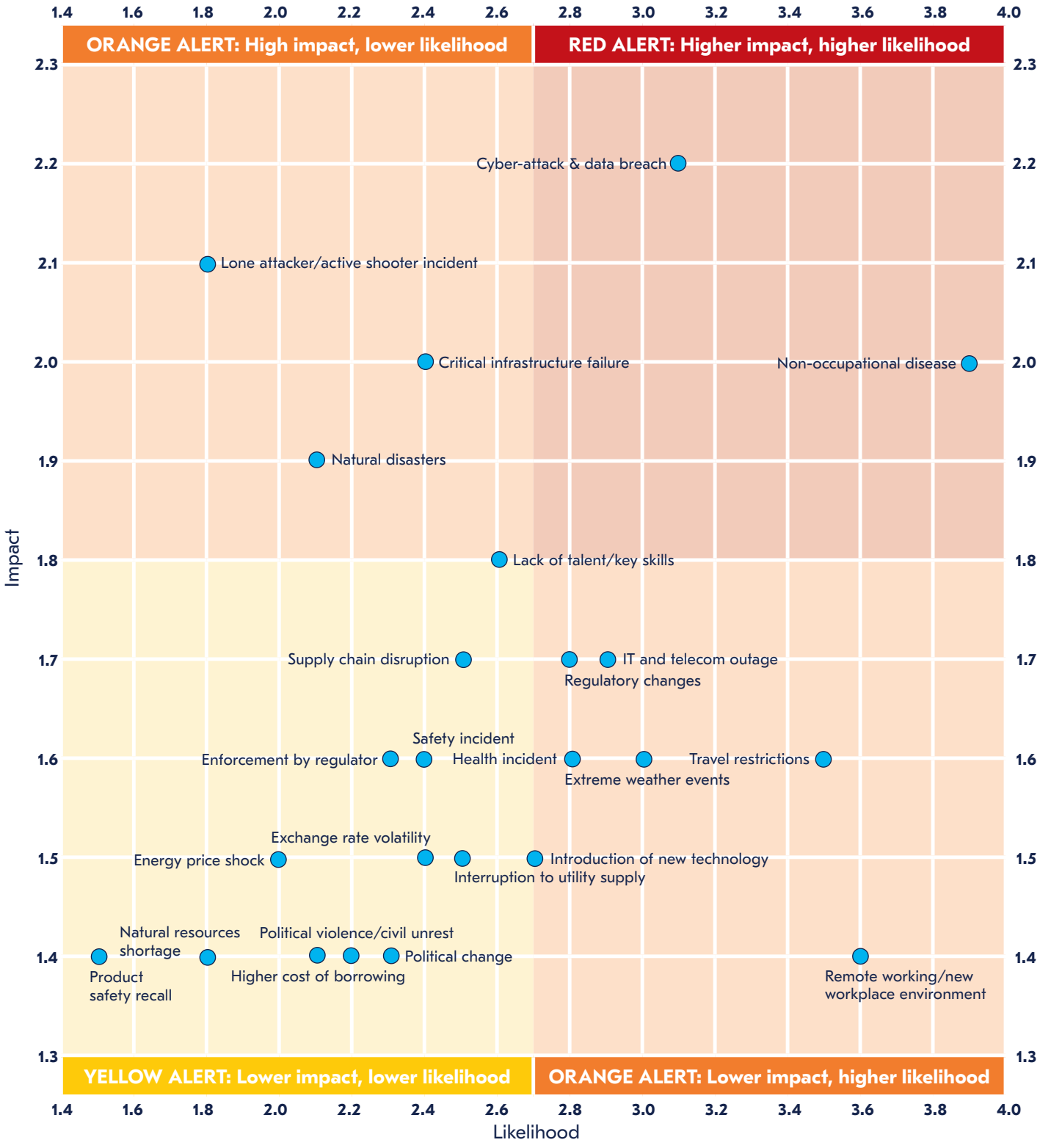


Figure 3. Risk and threat assessment: next twelve months

Consequences of disruption

Consequences of disruption

- **Staff morale, wellbeing and mental health is now the greatest consequence of disruption for organizations demonstrating the increased focus on staff wellbeing programmes exhibited in the early stages of the pandemic needs to continue.**
- **Staff loss or displacement was reported as a major concern by nearly half of respondents showing that the 'great resignation' is a reality for many organizations.**
- **The excuse of COVID-19 as a cause for poor customer service or product/service delays is now wearing thin. Respondents reported rises in customer complaints and reputational damage over the past year demonstrating customers are becoming less forgiving of bad service.**

The two main consequences of disruption for participants are negative impact on staff morale, wellbeing and mental health (68.1%), and loss of productivity (62.1%). The former has risen from second place in the 2021 report to first position in 2022, with an increase of seven percentage points.

The World Health Organization[18] reports that the global economy loses $1 trillion every year in decreased productivity due to mental health issues, which find an unfortunate fertile ground where there is widespread harassment, bullying, and other similar toxic behaviours. In many quarters, the mental health issues that arose from the pandemic - including issues such as feelings of isolation, financial apprehension, job concerns, home-schooling and medical worries - led to the mental health crisis being referred to as the second pandemic[19].

18. World Health Organization [undated]. Mental health in the workplace. WHO [online]. Available at: https://www.who.int/teams/mental-health-and-substance-use/promotion-prevention/mental-health-in-the-workplace (accessed 15 March 2022)

19. Mind (2021). Mind warns of 'second pandemic' as it reveals more people in mental health crisis than ever recorded and helpline calls soar. Mind [online]. 13 November 2021. Available at: https://www.mind.org.uk/news-campaigns/news/mind-warns-of-second-pandemic-as-it-reveals-more-people-in-mental-health-crisis-than-ever-recorded-and-helpline-calls-soar/ (accessed 15 March 2022)

On the brighter side, for every dollar invested in mental health, there is a return of $5 in terms of productivity and better health[20]. However, financial benefits should not be the primary driver in ensuring good mental health policies for staff. It is about making sure that organizations play their part in promoting a fairer and more sustainable way of doing business. Healthier employees make healthier citizens and ultimately more constructive and innovative societies; the ideal scenario for individuals, businesses, and government.

Factors that can affect mental health in the workplace range from a lack of flexible arrangements and unclear health and safety policies, to feelings of exclusion from important business activities. These unsustainable practices can lead to segregation from the rest of the team, creating a negative loop for the person affected. Zooming in on the practitioners taking part in this research, it is worth remarking that those working in high-pressure positions, such as crisis managers or first respondents are particularly vulnerable to mental health deterioration.

Employers can take action to support staff suffering from mental health issues through a series of initiatives dedicated to creating a supportive and non-judgemental workplace. Raising awareness on the topic is a good way to start. This does not have to be done as a classic seminar with a frontal lecture which is likely to lead to workers not feeling comfortable in sharing information, but by building access to confidential channels where they do feel safe. Organizations can also look at success stories and try to replicate those models that worked elsewhere. Innovative ideas to support mental health can also come from feedback from the employees themselves. Furthermore, employers should appoint skilled professionals or give employees access to initiatives such as Employee Assistance Programmes (EAPs) that can maximise the organization's efforts in supporting mental health[21]. Many organizations did start this during the pandemic but should ensure they continue to offer and promote assistance schemes, particularly as the current global instability is likely to add to mental health pressures.

On a similar note, participants reported staff loss or displacement as one of the main consequences of disruption (44.3%). This report has already touched upon the topic of attracting and retaining top talent, which has become a predominant issue in the past two years. Managing resilience also means checking in with staff and evaluating the impact on highly skilled individuals. While key employees do bring an added value to the organization, they can also represent a single point of failure or an unacceptable concentration of risk. It is good practice for managers to seek to understand what the impact on production would be of losing a specific employee or, in some cases, a whole team.

Business continuity professionals will usually evaluate critical processes and services when performing a business impact analysis (BIA). It is also key that they identify critical members of staff. Any organization should be able to survive the loss of an employee whether that be for health reasons, moving to a different region, being headhunted by a new company or retiring. Effective ways of avoiding a loss of knowledge can be ensuring training takes place to replicate skills or having someone shadow an employee so that knowledge relating to a critical role can be shared. This type of prevention would also work in countering loss of corporate knowledge which was also an issue for almost a third of all respondents to this question (31.1%).

The myriad of incidents which occurred in 2021 caused a loss of revenue for 43.0% of organizations which ranks it fourth in the list of consequences. COVID continued to weigh on many organizations' profitability in 2021 as spending patterns changed and supply chain issues impacted organizations' ability to get products to market.

Supply chain disruption itself rounds up the top five with a 41.3% consensus among participants. Customer complaints in sixth place (39.2%) also prove to be quite a hindrance to business continuity. They rank one place higher with a seven-percentage point increase from the previous year. It seems that the difficulties organizations have been enduring for the last two years do not serve as an excuse in the eyes of the public who still expect products and services to be available. Whilst consumers and businesses were more sympathetic to poor service and a lack of availability of supplies in 2020, the mood turned more to aggravation in 2021 as people believed that organizations should, by now, have addressed any poor service or supply issues which emerged at the beginning of the pandemic.

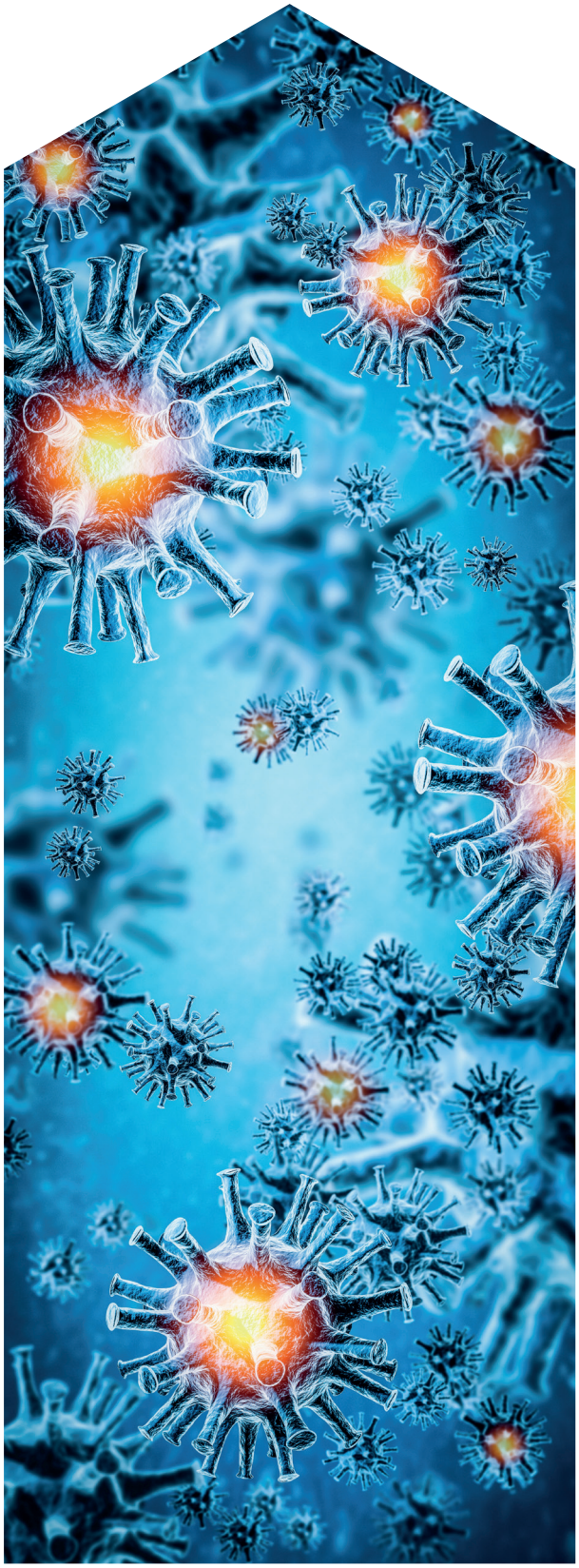
20. World Health Organization [2020]. World Mental Health Day: an opportunity to kick-start a massive scale-up in investment in mental health. WHO [online]. 27 August 2020. Available at: https://www.who.int/news/item/27-08-2020-world-mental-health-day-an-opportunity-to-kick-start-a-massive-scale-up-in-investment-in-mental-health (accessed 15 March 2022)
21. World Health Organization [undated]. Mental health in the workplace. WHO [online]. Available at: https://www.who.int/teams/mental-health-and-substance-use/promotion-prevention/mental-health-in-the-workplace (accessed 15 March 2022)

A survey by the Institute of Customer Service[22] found that complaints have reached a record high during the pandemic, with the 'COVID-19 excuse' becoming tiresome amongst the consumer audience[23]. From the customers' perspective, this shows that continuity is not a nice-to-have but a must-have. Perhaps even more importantly, the survey revealed that participants were willing to pay higher prices for a reliable delivery. This sheds light on a very important aspect of resilience and business continuity, that of competitive advantage. Top management often considers such efforts too costly and mainly reactive, whereas the public is explicitly telling the opposite. Those who can deliver — no matter the conditions — will stay in the market, the others will struggle.

This is further confirmed by the fact that one in five respondents (22.1%) experienced reputational damage in the last twelve months. This highlights the usefulness of implementing a business continuity management system, which includes the formation of a crisis management committee or an incident response structure with crisis communications an integral part of the structure. The way management respond and communicate during an incident or a crisis has a significant impact on reputation. Therefore, it is important that executives are ready to speak in a consistent and structured way, avoiding conflicting or false statements.

"During times of disruption, there's normally a time when the customer doesn't receive a service. So during COVID was a period where you find some customers complaining. We had two alternating teams that quickly came in and started sending communications to various levels of customers, so it was individualized communications. As a bank, we've got a certain customer that they're segmented. So you can't just send a one size fits all kind of various customer segmentations so you have to send out different communications depending on the profile of customer. If it is done right, the customers become your ambassadors in championing your response and supporting you during disruption, so that's the one area we have worked on heavily. As a result, we saw a number of customers supporting us, helping us, and lobbying for us on that space."

Head of Continuity Management, Financial Services, Zambia



22. Sky News (2022). Consumer complaints about business reach record high in UK due to COVID shortages. Sky News [online]. 25 January 2022. Available at: https://news.sky.com/story/consumer-complaints-about-business-reach-record-high-in-uk-due-to-covid-shortages-12524477 (accessed 15 March 2022)
23. Peachey, K (2021). Customers fed up with Covid excuse for bad service. BBC News [online]. 7 July 2021. Available at: https://www.bbc.co.uk/news/business-57734808 (accessed 15 March 2022)

In seventh position, increased cost of working ranks lower than last year with a score of 37.9%. Last year, this was in fourth position, and was seven percentage points higher. This is likely to have been down to the higher adoption of remote work, the initial outlay associated with new hardware and software, as well as investment in staff health and wellbeing. The rest of the top ten is completed by two impacts, namely impaired service outcome (30.6%) and increased regulatory scrutiny (22.6%) that both affected a larger number of organizations in 2021, albeit by small margins. Indeed, the interviews carried out for this year's report also show that regulatory concerns were elevated this year, particularly within financial services organizations worldwide.

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

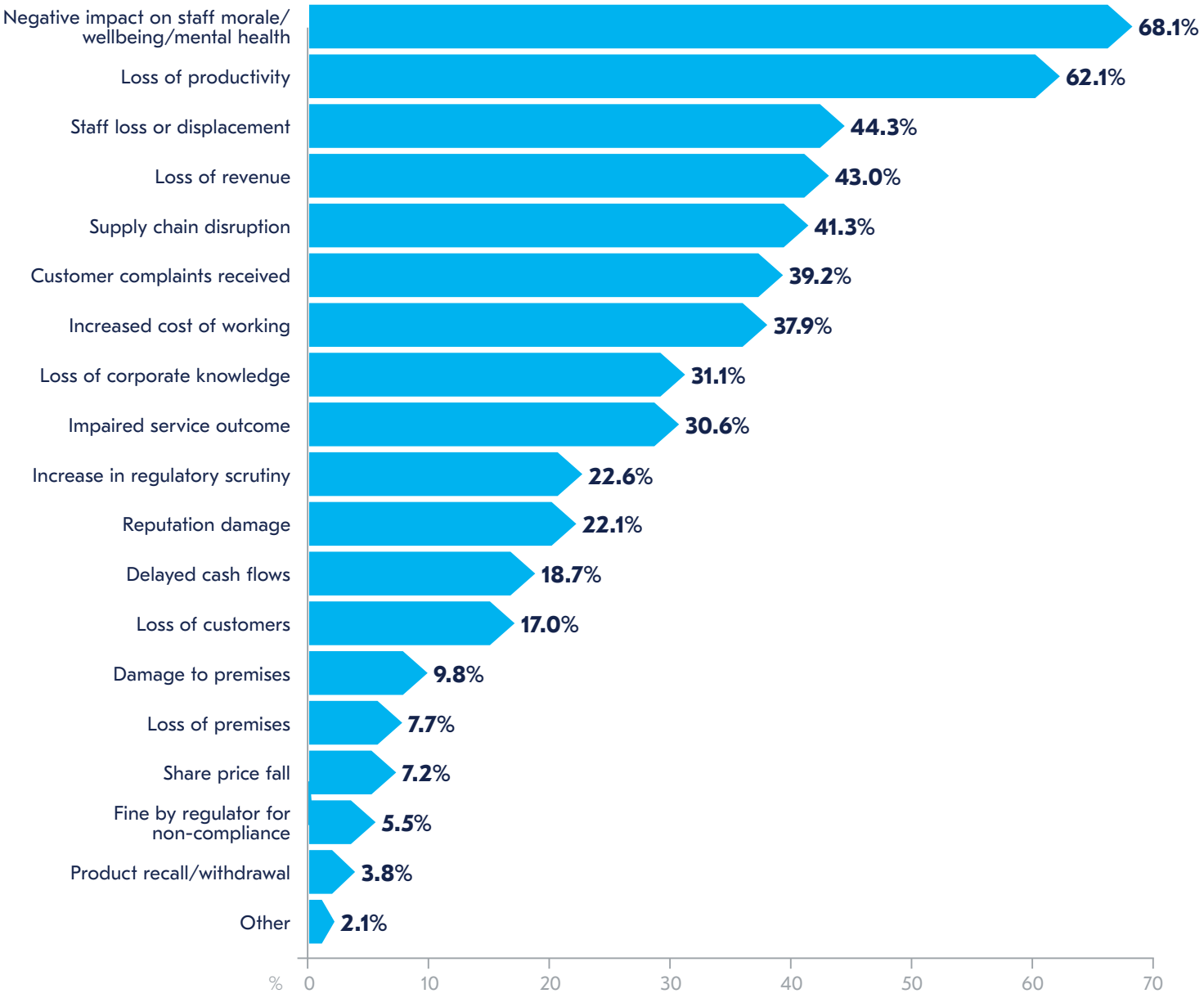


Figure 4. Which of the following impacts or consequences arose from the disruptions experienced in the last 12 months?

Benchmarking business continuity

Benchmarking business continuity

- **ISO 22301 remains the business continuity benchmark for nine out of ten organizations.**
- **Although certification levels fell slightly during 2021, the number of organizations using ISO 22301 as a framework increased by 11 percentage points over the year.**
- **Although organizations report ISO 22301 helps increase organizational resilience and better manage incidents, many cite that it benefits their organization externally: it allows them to demonstrate the effectiveness of their business continuity programme, aids relationships within supply chains and helps to align with industry peers.**
- **Cost remains a deterrent to certification for many companies, although interviewees reported that with the experiences of the pandemic, management teams were pressing for certification for the first time.**

Despite many organizations looking to move beyond business continuity towards overall organizational resilience, the main standard of reference for business continuity professionals remains ISO 22301. 91.3% of professionals say that over the past two years they have not moved away from the standard in favour of another resilience standard (such as ISO 22316). However, types of alignment tend to vary across organizations. Although some interviewees cited that ISO 22301 was becoming less relevant for their own organization, there is a notable increase in the number of organizations who are using the standard as a framework, even if the number who certify has fallen slightly. 63.6% of respondents are using ISO 22301 as a framework (2021: 52.7%) even though they have no formal certification and, of those, 13.5% are currently in the process of getting certified. Additionally, some 7.6% of organizations who currently do not use the standard as a framework, admitted that they plan to move towards it in 2022. Despite the fall in certification this year, nearly one in six organizations are still certified: 15.1% are either certified or in the process of becoming certified (2021: 18.9%).

Although certifications are down slightly in 2021, the appetite for certification does still very much remain. Interviewees explained how their organizations had aligned to the certification for the first time in 2021 after management realised the importance of having a solid and demonstrable business continuity programme in place. Practitioners themselves could see the value, but explained how there was no budget to certify, particularly when the organization had already certified towards another standard(s).

Interestingly, one in five organizations (21%) have no plans at all to align to ISO 22301, revealing there is a significant minority of organizations that still prefer to run their business continuity management programs independently. Indeed, one interviewee highlighted that whilst they value the framework of ISO 22301, they felt that building their own programme which went above and beyond that stipulated by ISO 22301 worked best for their own organization.

It is worth noting that not adopting ISO 22301 does not necessarily mean not relying on standards at all. Several practitioners revealed they use a wealth of guidelines to improve resilience levels within their organization. ISO 27001 is one of the most popular documents for resilience professionals as it helps them set up information security management arrangements, focusing not only on the technology, but also on those organizational processes that can boost protection of key data and information. On the same note, respondents report using other frameworks on information security such as NIST, from the US National Institute of Standards and Technology, and COBIT, which is issued by ISACA.

Similarly, the main risk management standard ISO 31000 is another major player in the resilience industry. The 2018 update attempts to make risk management more strategic and embedded within internal processes which makes it possible to use for objectives too: another driver for this standard's popularity. Another takeaway from the update is to dedicate enough resources to risk management and establish clear roles and responsibilities. Following this line of thought, these principles are also very much applicable to business continuity management, particularly as many organizations are moving towards overall resilience.

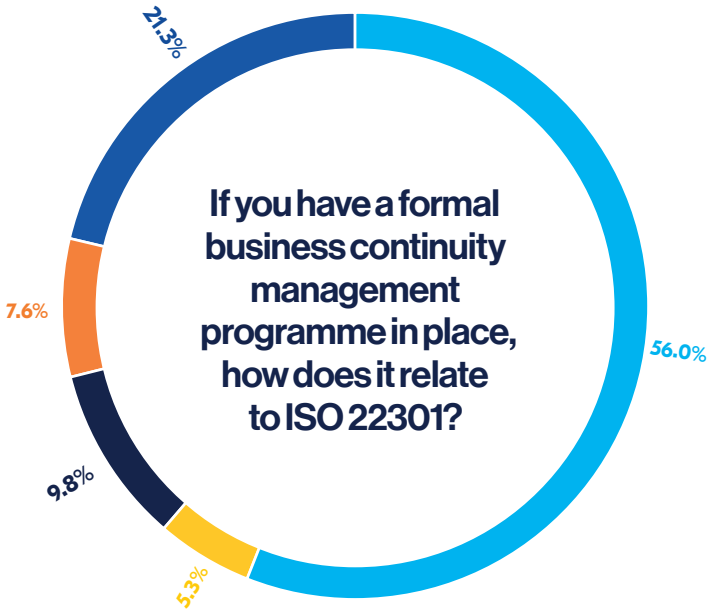
Moving forward, ISO 22316 tries to tie a variety of management disciplines together to establish organizational resilience. The standard does not emphasize any specific unit or division responsible for this, but it stresses the importance of cooperation and the removal of internal silos. The principles to get to true organizational resilience are somewhat similar to those present in ISO 22301 or ISO 31000, especially with regards to investment levels, raising awareness, and top management commitment. The general trend seems to be to align resilience functions with strategic objectives as much as possible, to avoid perceiving it only as a cost. The findings of this report support this notion, as participants revealed that in the last year, being resilient brought a series of advantages including a more prominent position in the market. Despite this concerted move towards resilience, most organizations are not yet ready to retire their use of ISO 22301 in favour of ISO 22316: just 3.5% of organizations are planning to move towards ISO 22316 as their preferential resilience standard.

Despite the ISO 22301 standard still prevailing in popularity amongst resilience professionals, some organizations are going beyond standards within their organizations to demonstrate exemplary organizational resilience. One interviewee spoke about how they had instigated a joint project with peers, other industries and governing bodies to 'future proof' the resilience of the sector.

"I'm doing a collaborative project with the utility companies to ensure continuity of supply. I'm working with Telstra — the telecommunications company, NBN, internet, water, and all the energy providers. This collaborative groups aim is to undertake tactical planning together. I'm finding that during an actual emergency, the different parts of the cog need to collaborate. This is where the incident management part of my role, and business continuity work quite well together because I'm able to instantly see and then plan exactly what is critical. Bringing the whole utility sector together. It's instigated off the back of a power outage incident in November last year where I realised half the people during the incident didn't know each other and it was a perfect opportunity to collaborate and actually share."

Business Resilience Advisor, Utilities, Australia

In the past year, other standards that turned useful for organizations touch upon different topics, mirroring the risks highlighted in this report, such as health and safety (ISO 45001), environmental management (ISO 14001), incident response (ISO22320), and quality management (ISO 9001).



56.0%
We use ISO 22301 as a framework but are not certified to it.

5.3%
We use ISO 22301 as a framework, are not certified to it, but are in the process of getting certified.

9.8%
We use ISO 22301 as a framework and certify to it.

7.6%
We don't currently use ISO 22301 as a framework but we intend to move towards this during 2022.

21.3%
We don't use ISO 22301 as a framework and have no plans to move towards this during 2022.

Figure 5. If you have a formal business continuity management programme in place, how does it relate to ISO 22301?

Top 10 standards used within organizations (aside from ISO 22301)		
1	**ISO 27001**	Information security management
2	**ISO 31000**	Risk Management
3	**ISO 9001**	Quality
4	**ISO 22316**	Organizational Resilience
5	**NIST Framework**	Information Security
6	**COSO Framework**	Internal Control
7	**ISO 45001**	Health and Safety
8	**ISO 14001**	Environmental Management
9	**ISO 22320**	Incident Response
10	**COBIT**	Information Technology

Figure 3. Do you use any other management system standards to manage risk and/or resilience? If yes, please specify which.

Figure 6. Have you moved away from using ISO 22301 in place of another resilience standard (such as ISO 22316) over the past two years?

An increasing focus on organizational resilience (74.0%) remains the main reason to certify towards ISO 22301. However, this year it shares the top of the chart with being able to demonstrate the effectiveness of the business continuity management programme (74.0%). An interesting point about these results is that the main reason to align to the standard appears to be very practical and rooted in the needs of 'the real world'. However, one interviewee raised a concern that they were frequently asked to 'tick a box' to show they certified to ISO 22301 when they were entering into a contract with a new buyer. They felt that more was needed than just a 'tick box' exercise to improve resilience levels and to prove this to their business partners. The same interviewee further affirmed this by claiming it was 'too easy' to not lose a standard, even if errors had been made.

Nevertheless, the importance of demonstrating that the BCM programme is effective is another consequence that has risen out of the pandemic: being able to guarantee continuity of service has earned a more visible role in commercial partnerships.

The third and fourth benefits — which share the same consensus — are also deeply rooted in practical business needs, as 60.0% of participants acknowledge the 'importance of enabling the management of disruptions' and 'consistent BCM measurement and monitoring'. Enabling faster recovery (54.0%) rounds up the top five, with a slightly greater preference than last year (52.1%). However, there is certainly less concern for benefits which relate to organizations outside their own: alignment with industry peers (46.0%) and helping stakeholders manage risk (46.0%) receive less attention from respondents and both lose three positions this year.

Further down the chart, it is worth noting that a significant minority of the respondents report two impacts of ISO 22301 certification: 'improved communications' and employee engagement' (46.0%), and 'better customer satisfaction' (38.0%). Both benefits are pivotal to a successful organization, particularly since the start of the pandemic as they positively affect the people within the organization and the customer base. This report has already demonstrated how some of the main challenges in the past and upcoming year circle around staff morale and reputation; therefore, it is important to understand how BCM supports the organization in this sense.

What benefits does certification provide to you and your organization?

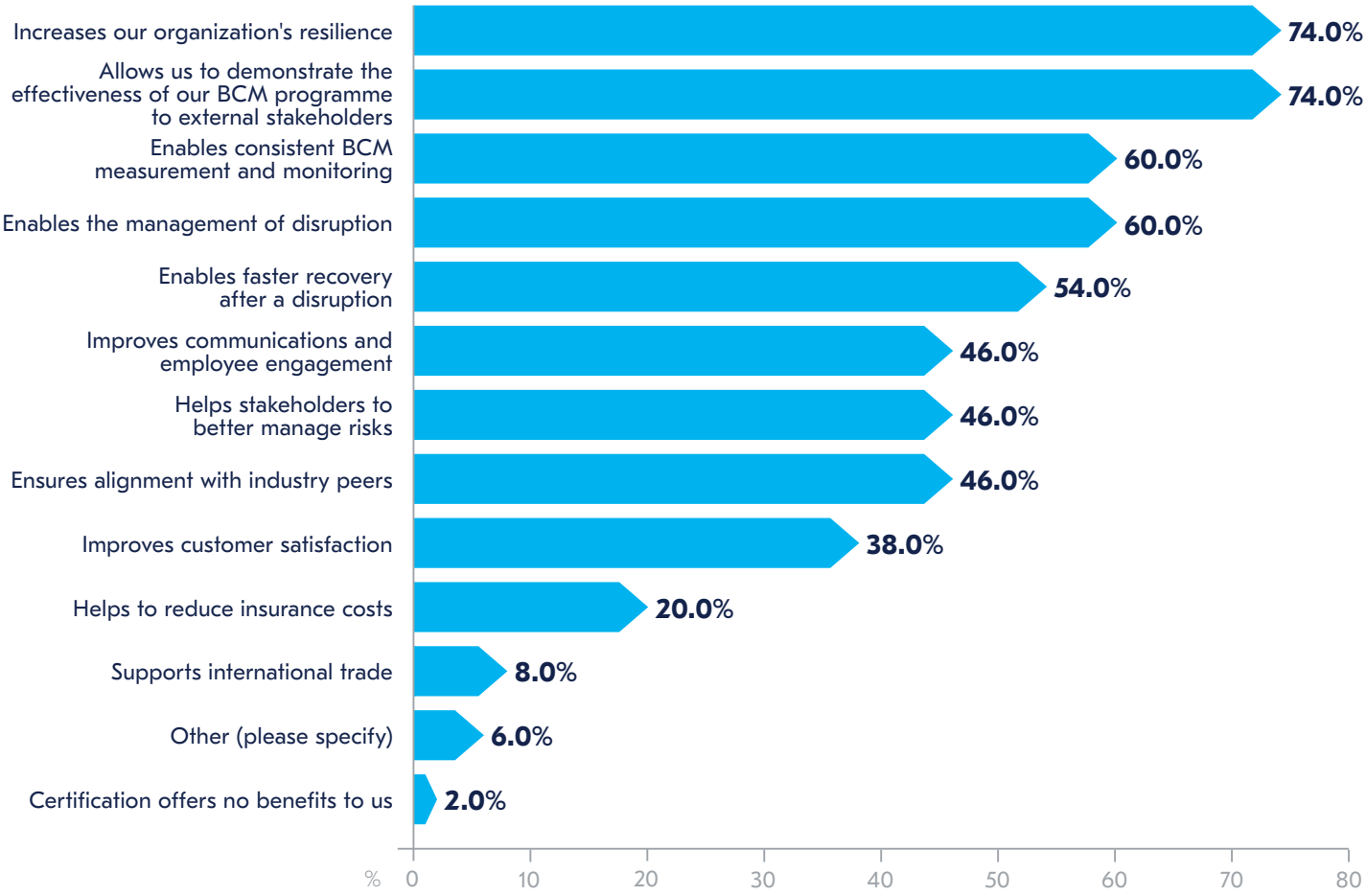


Figure 7. What benefits does certification provide to you and your organization?

Just as last year, 60.2% of respondents did not feel the need to certify due to the lack of business requirements. However, 48.0% state that whilst they are not certified to ISO 22301, they felt very strongly that using it as a framework was important. For some organizations, this is often the first step towards actual certification and, for others, it enables them to build their own resilience models using ISO 22301 as that core part of their skeleton.

On a different note, a significant section of participants admit certification is not relevant to their organization. 29.2% claim there are no external drivers, 26.3% do not see a real value, and a further quarter (24.6%) have no commitment from top management — even though many are working hard to convince management of the importance of certifying.

Nearly a third of organizations (29.3%) also report lack of budget to dedicate to the alignment towards the ISO 22301 standard. This is a similar figure to last year and shows that those professionals who had hope in last year's report of acquiring budget to certify may not have been successful in their approaches to management.

For some countries and/or sectors, ISO 22301 is also less relevant. An interviewee from Ireland explained that ISO 22301 was not widely used in Ireland and, whilst they did use ISO 31000 for some guidance, the business continuity standard was not widely followed at all. They explained how they used the National Framework for Emergency Management instead. Indeed, there are local preferences witnessed globally: in Australasia and the United States, for example, organizations often use locally issued standards in preference to global ones.

"The ISO 22301 standard for Business Continuity does not seem to be in use in Irish higher education. On the emergency management side, we follow the National Framework for Emergency Management, which is similar to the gold-silver-bronze system in the UK. We do not use a standard for business continuity. For Risk Management we follow the ISO 31000 standard for principals and guidelines, I'd like if ISO 31000 was further developed for accreditation and certification."
Business Continuity Professional, Higher Education, Ireland

Another interviewee explained how although the ISO 22301 standard was used as a framework, they did not have time to go through the process of certification due to the good processes they already had in place in the organization around business continuity.

"When we first started our business resiliency plan, it was like most, in Word and Excel, but that was 2015. Trying to be ISO compliant on Word and Excel is nearly impossible. As a result, we've vetted quite a few business continuity software applications and came across a company that had the same ideals that we did. They made sure that their software application was ISO compliant, and it really helped somebody new like me. And so using that application, I believe we are using a great framework. My goal is to get our plans ISO certified one day, but with all the departments that I have — I have to approve 50 different business continuity plans in total — there's just no time to do it at the moment."
Senior Business Resiliency Manager,
Healthcare, United States

In fact, all these issues — albeit with some small variation — were also present and relevant last year, showing that there are still many organizations for whom certification is not a viable option now, or in the near future. However, whilst certification is down, we must remember that there is an eleven-percentage point increase in the number who use the standard as a framework, demonstrating that the standard's principles are being adhered to more than ever within organizations.

The conversation around standards and their applicability in the 'real world' is not easy and sometimes quite controversial. The data suggests that there is not a clear division between those who find ISO 22301 and other standards useful, and those who dismiss it completely. Rather, there are different shades of alignment towards international guidelines, that vary due to personal and organizational convictions, budget, awareness, and industry alignment. Alignment and certification should be viewed as a path made of different steps and not with an 'in-or-out' perspective.

At the same time, in the interest of raising awareness, it is important to acknowledge that this report highlights several instances where the practices that are present and recommended by ISO 22301 proved useful during the pandemic. These findings do not rely on speculation or estimates, but they are a direct account of the positive impact of the practices present in documents such as ISO 22301 and the *BCI's Good Practice Guidelines*[24] on the benefits of employing improved resilience tactics.

24. BCI, The. Good Practice Guidelines (2018 edition). The BCI. Available at https://www.thebci.org/resource/good-practice-guidelines--2018-edition-.html. (accessed 15 March 2022)

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

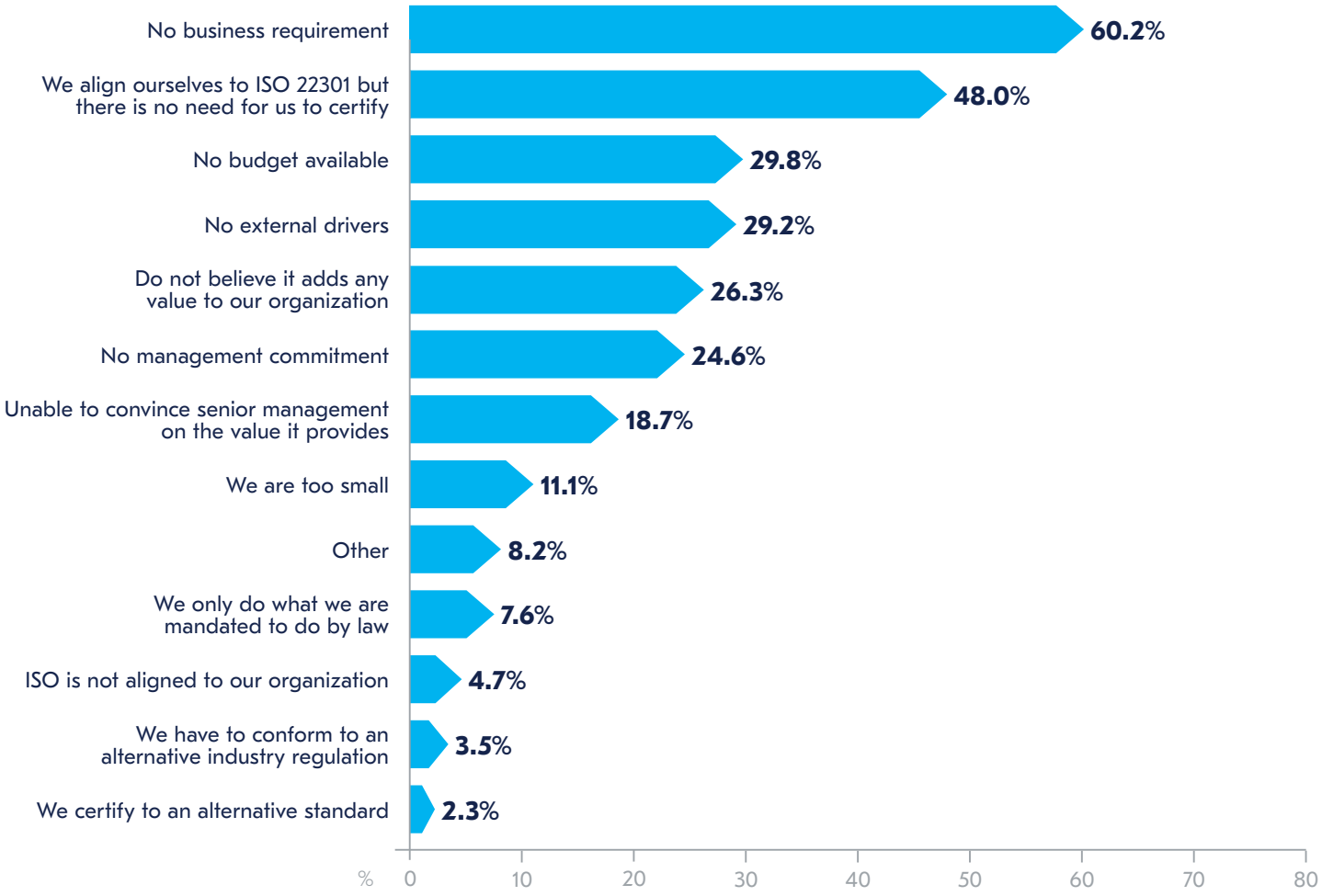


Figure 8. What are your reasons for not being certified or having no plans to be certified to ISO 22301?

Benchmarking longer term trend analysis

Benchmarking longer term trend analysis

- **In the mid- to long-term, cyber-security was cited as a top concern by 85% of practitioners.**
- **Climate risk is an emerging risk, with worsening extreme weather and elevated concerns arising from COP26 encouraging practitioners to consider how climate change will affect their organization in the long term (chronic) rather than short term (acute).**
- **Less than half of organizations have centralized their risk scanning processes, with many labelling it as an 'area cited for improvement' during 2022.**

For the first time in this report, we asked practitioners what their greatest concerns were for the medium- to long-term (the next 5-10 years). Cyber-security was the most prevalent concern, with 85.0% of respondents believing this is the biggest long-term threat to their organization. This concern may have been ranked even higher had the survey period for this report been later: interviewees highlighted how the current situation in eastern Europe had elevated the risk of cybercrime for their organization.

The sheer volume of digitization concerns practitioners, who see the attack surface getting constantly broader as the opportunities for cybercriminals multiply. Current global investment levels in cybersecurity stand at $217 billion, and by 2026 they are projected to experience roughly a 60% growth, reaching over $350 billion[25]. As experts often underline the importance of the human aspect of cybersecurity, the success of a cyber security strategy can be more down to increased training, raising awareness, and promoting best practices in the field than it is to having the most advanced antivirus technologies installed. Indeed, business continuity management is an effective ally in preventing, responding and recovering from cyber-attacks, and it would be wise for organizations to dedicate it part of their budget to training and exercising — as well as technology - if they want to build a truly resilient cyber strategy.

25. Statista (2022). Size of the cybersecurity market worldwide from 2021 to 2026. Statista [online]. 14 February 2022. Available at: https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/ (accessed 15 March 2022)

One interviewee expressed how their primary long-term concern for cyber security was the increasing use of social engineering within cyber-attacks — and how criminals were becoming ever more deceiving with their attacks.

> **"Attackers are now taking more of a spearphishing approach to target individuals. So the old school phish from a foreign Prince is now dying as everyone is more educated with them, we're seeing a lot more social engineering and targeted phishes. They'll look at your LinkedIn account. They'll look at your social media account. They'll make a speculative intervention with you. At no point will malicious links be shared or anything like that. But they'll build up that knowledge base or the individual. They'll build up that trust, and then deliver the payload when consistent communications and trust is achieved."**
>
> Resilience Professional, Utilities, United Kingdom

In joint second place, non-occupational disease and climate risk both received a 50.0% consensus from participants. These are both threats that belong to environmental and biological realm, which is once more a wake-up call to rethink the impact of organizations on the ecosystems where they operate. The Harvard Centre for Climate, Health, and the Global Environment[26] highlights how the same factors that increase climate risk are also likely to be risk factors in the spread of new viruses. Actions such as deforestation can destroy natural habitats and lead animal species to migrate, carrying with them germs and infective agents that can spread to other species including humans. Furthermore, research has shown that living in areas contaminated by extreme pollution increases the chance of respiratory complications from viruses such as COVID-19 and SARS.

The Climate Action Tracker, a research group that keeps tabs on countries' efforts towards climate change, also reports there is still a substantial gap between current achievements and the established targets. Out of the 35 countries that produce 80% of total pollution, there are still 12 — including large ones such as Brazil, Australia, and Russia — that did not show any real change with emissions that are still above target.

Whilst many organizations are adopting changes into their practice as part of their environmental, social and governmental (ESG) or corporate social responsibility (CSR) strategies, many practitioners admit to viewing events caused by incidents such as extreme weather as 'acute' risks. This means that a well-practiced and rehearsed plan is invoked in the case of a building being destroyed by a flood, for example. In the long term, however, organizations should start to consider severe weather events as 'chronic' risks (e.g. moving a factory if it is on a floodplain, moving offices if they are located in an area prone to wildfires). Some practitioners are already considering this in their own organizations, but interviews for this report suggest that the practice is rare. One interviewee discussed how the questions around chronic climate risk were serving as a prompt to take the case to senior management.

> **"We are definitely looking at sustainability, but I think that's just part of being a good company with strong ethical values. Our location strategy to mitigate against longer term climate change is a really interesting point though. It's not something we've discussed, but I think I will now raise this as an issue. When we are looking for long term, you want a company that can continue, and as these environmental impacts start, you need to be prepared and think about things like office locations in advance."**
>
> Senior Business Continuity Manager, Electronics, United Kingdom

26. Harvard TH Chan School of Public Health (2020). Coronavirus, Climate Change, and the Environment. A Conversation on COVID-19 with Dr. Aaron Bernstein, Director of Harvard Chan C-CHANGE.Harvard TH Chan. Available at: https://www.hsph.harvard.edu/c-change/subtopics/coronavirus-and-climate-change/ (accessed 15 March 2022)

Technology and telecoms failure (35.8%) is the fourth main longer-term risk for practitioners, which is in line with the critical role of IT infrastructure in current times, especially as new hybrid work environments become more popular. Furthermore, new technologies are entering onto the scene at pace and, for each introduction of a new technology into an organization, new training programmes will need to be set up and initial teething issues could lead to failure. There is also the issue which was raised at the start of the report: that of an overreliance on the internet for communications. VoIP might be a cost efficient and convenient solution, but what will happen if the internet goes down or an entire platform, such as Microsoft, is hit by a cyber- attack and all applications — including tools such as Teams — go offline? Such scenarios require considerable planning and back-up processes need to be built in, particularly with copper telephone wires due to be grandfathered globally by 2030.

Moving further down the table, talent concerns (31.4%) and supply chain risk (30.1%) jointly occupy the fifth and sixth place in the table respectively. Both have recurred through the findings of this report and they appear to be here to stay, especially if coupled with other challenges such as regulatory changes (28.3%), adapting to new way of working (21.7%), and geopolitical violence (21.7%).

Some organizations were considering the far broader risk landscape when it came to understanding mid- to long-term risks. An interviewee from the education industry told how they were trying to understand how the industry would evolve over the years, and the challenges they would face on that journey rather than tackle the long-term landscape segmented risk approach. Another interviewee discussed how they prefer to look at the impact of incidents, rather than the cause.

"The major threat on the horizon for us is around the broader picture of academia. What is the future of academia? We also make sure that people are actually thinking about that at the right levels as well. This means I am immersing myself in all levels in the organization, right from the board all the way down to lower grade manual staff. When I started this role, it was about me coming in and going, 'Let me look at everything and understand what it looks like, and then target specifically what the risks are."

Risk & Compliance Officer, Education, Australia

"One thing we always look at is the impact rather than the cause. So the biggest impact for us at the moment is trade compliance and being able to trade freely across the globe. I don't think it matters if it's political change, a war or conflict or something else that's causing it. That's what we're seeing at the moment in Russia. At the moment, it's going to stop us being able to trade with other companies in other parts of the world. That, to me, is an impact."

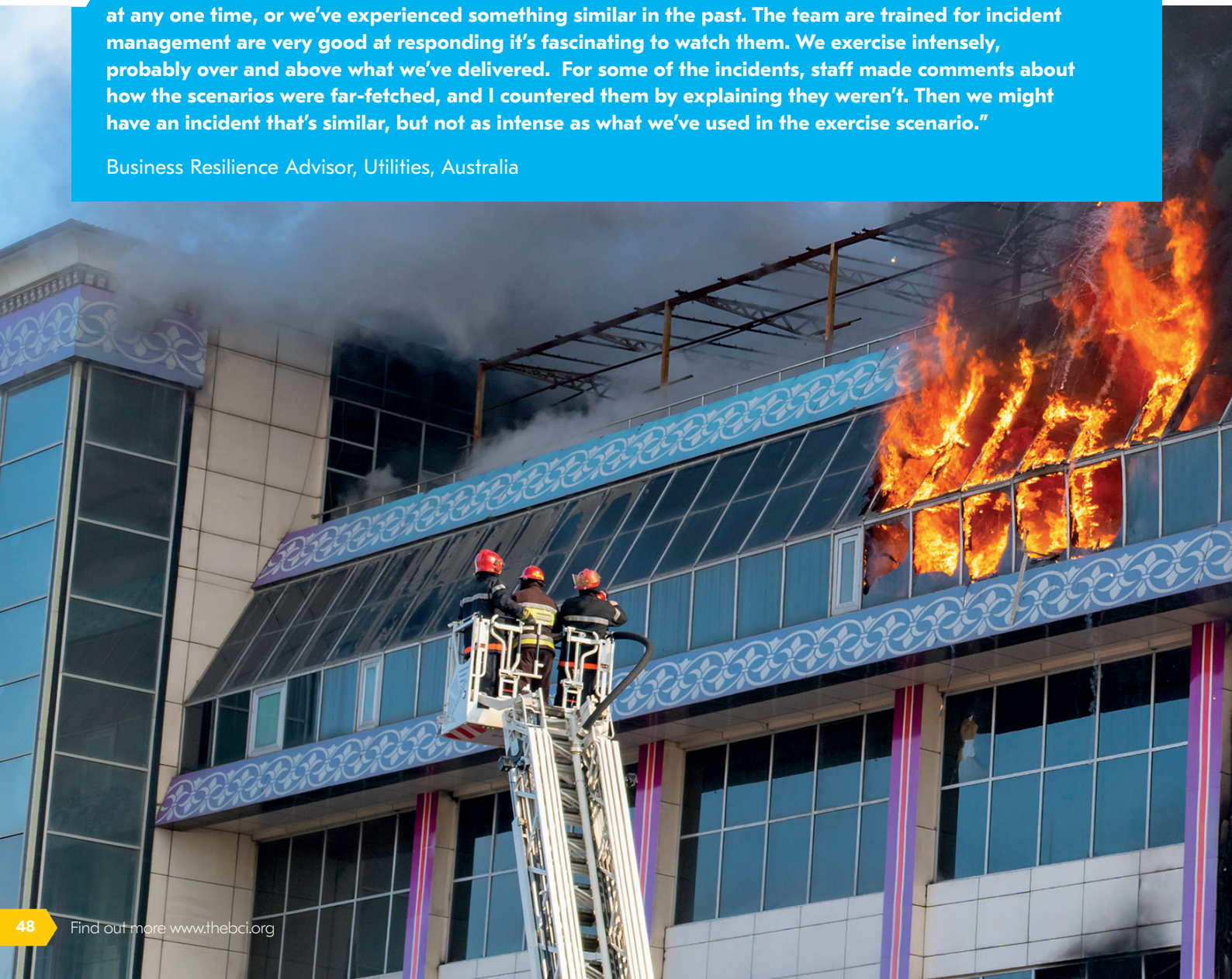
Senior Business Continuity Manager, Electronics, UK

Comparing the list of risks and threats across different time spans, issues concerning the pandemic (e.g., non-occupational disease, travel restrictions) and the management of human resources (e.g., remote work, lack of talent) are consistently present in the charts for the past twelve months, next twelve months, and next five years. Differently, cyber threats, IT failure, and climate risk become more prominent moving forward. Overall, it is fair to argue that the challenges for organizations in the medium to longer term will fall under three main domains, namely human resources, digital assets, and environmental impact.

However, it is worth highlighting the importance of 'preparing for the unexpected'. Both the 2020 and 2021 Horizon Scan Reports demonstrated that practitioners' concerns for future risks divert to those that they are currently experiencing. This year, this was exemplified in interviews where practitioners admitted that if they were to complete the survey now, cyber security would be rated as a greater long-term risk, due to the escalating situation in Ukraine. Practitioners therefore need to continue to keep a broad view of the risk landscape. Those that use all the intelligence they can to help plan their own risk landscapes will ultimately be better prepared for previously unforeseen incidents that can cause challenges to their organizations. One interviewee was keen to point out that they felt their organization was 'prepared for anything'. When considering future risks, the interviewee had ticked every incident type as 'imminent' such was their preparedness for all types of event.

"Realistically, we are always prepared for unknown incidents. We've got that many incidents going on at any one time, or we've experienced something similar in the past. The team are trained for incident management are very good at responding it's fascinating to watch them. We exercise intensely, probably over and above what we've delivered. For some of the incidents, staff made comments about how the scenarios were far-fetched, and I countered them by explaining they weren't. Then we might have an incident that's similar, but not as intense as what we've used in the exercise scenario."

Business Resilience Advisor, Utilities, Australia



One of the problems is that organizations continue to have a 'reactive' strategy to incidents, rather than being 'proactive' with their approach to planning and thinking longer-term. An interviewee highlighted how management within their organization still preferred to take the former approach, and the resilience manager was trying to get them to move their thinking towards the latter.

"There's a culture within the company around what risks really need looking at and whether there needs to be analysis and communication around it. Currently, they are just at the point where they don't want to be proactive. They're very reactive about incidents. This means, right now, it is really hard to properly plan. So, one of the things I'm working on is trying to get management to be more proactive. They need to be ready for a situation rather than reacting when it happens."

Senior Business Resiliency Manager, Healthcare, United States

However, sometimes a reactive strategy does need to be deployed, particularly in the case of an incident for which intricacies could not be seen in advance. COVID-19 was an example of this, and to some extent, the escalating situation in the Ukraine as well. One interviewee explained how they were already dealing with issues relating to the Ukraine crisis within their own organization.

"We did an assessment of our people and we've had a couple of contractors who are from the Ukraine, so we had to ensure that they are okay. We also have people who work with us from different countries and check that they were not in the region. Similar with Russia and people working in surrounding countries. There's also the internal communication piece and managing what our colleagues are saying to one another and making sure that, whilst people can speak freely, the right things are being said. We also did a full assessment on all our critical vendors to make sure that they're able to deliver to us and what are the impacts to them. We also have to consider our political stance."

Senior Business Continuity Manager, Electronics, United Kingdom

Other organizations stressed the importance of regular after-action or post-incident reviews to ensure learnings made from incidents are quickly embodied into operational plans. An interviewee spoke how they were ensuring there were solar-powered remote terminal unit (RTU) batteries installed in an area which was devastated by a recent earthquake thanks to learnings made from the post-incident investigation.

> **"To mitigate these happening further, we have a post-incident investigation for each incident where we go through what went well, what didn't go well and what we can improve. The endless improvements are then itemized either by documentation updates, further training for people or purchasing products and services. As you can imagine, all the planning we've done in the last couple of years, especially around the power outage planning and comms outage planning, assists us in a lot of the response. We can't mitigate incidents completely from occurring we can just plan for the worst and hope for the best."**
>
> Business Resilience Advisor, Utilities, Australia

Thinking about the next 5-10 years, which are your top three concerns for the mid- to long-term risks?

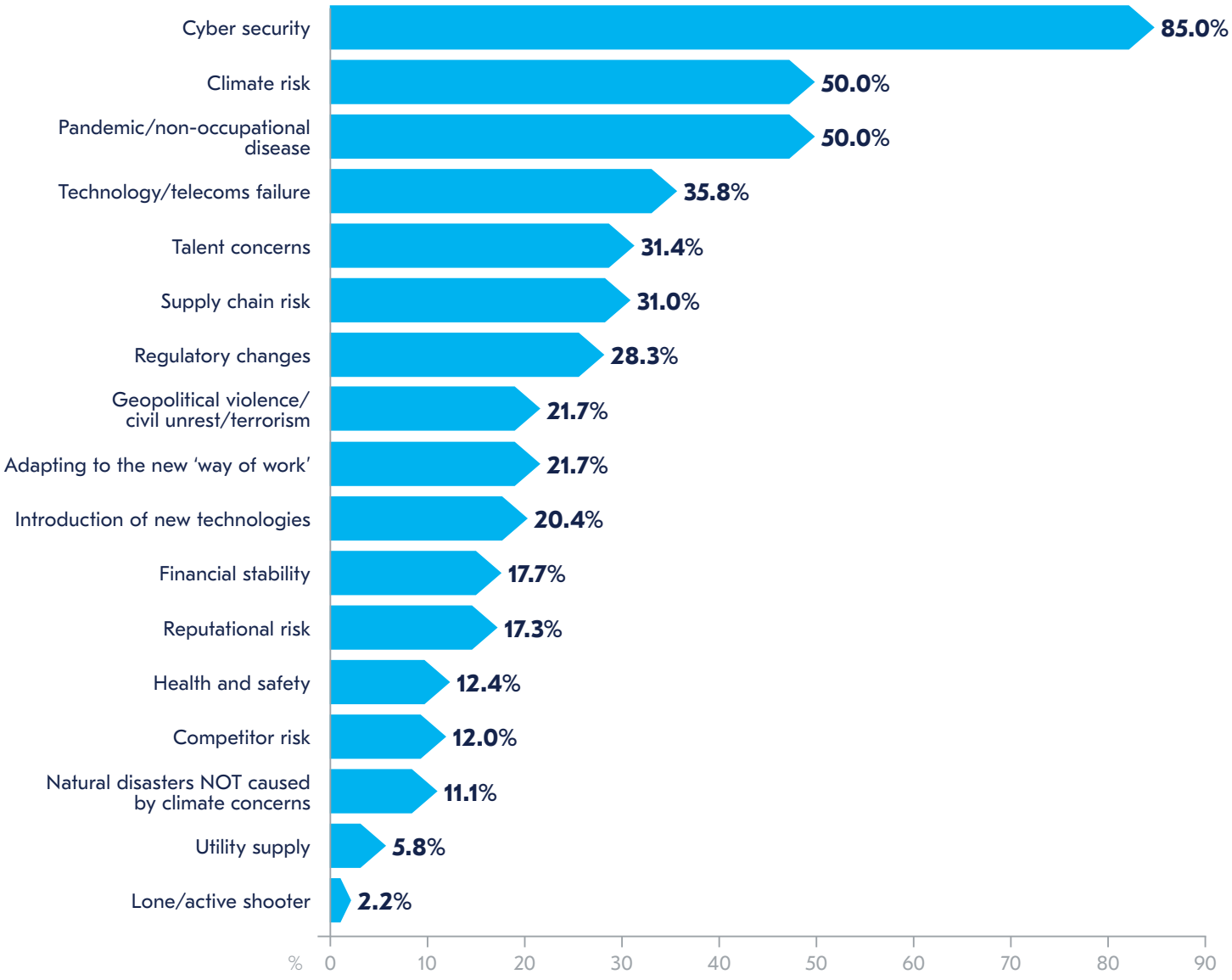


Figure 9. Thinking about the next 5-10 years, which are your top three concerns for the mid- to long-term risks?

Past twelve months	Next twelve months	Next 5 years
Non-occupational disease	Non-occupational disease	Cyber attack & data breach
Remote work	Cyber attack & data breach	Non-occupational disease
Travel restrictions	Travel restrictions	Climate risk
Health incident	Remote work	Technology/ telecoms failure
Lack of talent	IT and telecom outage	Talent concerns

Nearly half of respondents (46.9%) conduct a longer-term trend analysis through a central corporate function or department, while an additional 27.4% do so with the support of many different departments based on specific needs. Disappointingly, both these figures are down compared to the previous year (the 2021 report showed that 52.8% of organizations were now organizing longer-term trend analysis via a centralized function). For many organizations, COVID-19 has been the precipitator for acquiring more data for risk planning processes, centralising these processes and, where possible, investing in data mining processes to help sieve through the information. Although nearly three-quarters of organizations do this, there is still clear room for improvement, particularly given that one in five organizations (20.4%) do not perform this type of analysis at all. Interviews carried out for this report do, however, point to an improving picture. There were several interviewees who commented that they now had a Chief Resilience Officer within their organizations who was looking to drive this kind of process, whilst others had had new senior risk managers employed who had been charged with improving data resources, as well as the mining and management of those resources.

"We are moving forward in terms of resiliency. Resiliency in the organization is very much on trend. We've got a new Chief Resiliency Officer, which we never had before. There's now a more holistic approach to resilience than we've ever had previously. So we're moving in the right direction, but not explicitly aligned to it in any shape yet."

Resilience Professional, Utilities, United Kingdom

"One of the stated aims of our recent departmental organization was to enable a more centralized threat risk and scenario contingency planning. So, for example, when the treasury are looking into liquidity or market funding issues they're working off a consistent view of what the organization sees as the future, as opposed to one department looking at it one way and another department looking at it another way. So, our plans are to centralize that and improve that area within the organization as a whole."

Group Business Resilience Manager, Financial Services, Australia

Whilst organizations may not be as efficient as collecting and analysing data, practitioners are now using the outputs from trend analyses more readily. 52.5% of practitioners state that they draw on the inputs of this trend analysis - an 11-percentage point increase from 2020 — with a further 24.9% who help develop the analysis in the first place. However, there is still a minority (19.1%) of practitioners who do not have access to outputs from trend analyses, albeit down from last year's figure of 24.0%. Not having access does not mean that practitioners are not doing their own analysis. There are a number of free resources available that can help with risk mapping such as the *BCI Horizon Scan*, national risk registers and reports such as the OECD cross-country perspectives on global risk[27].

External forums, conferences and opening up information channels between peers, customers and suppliers can also help to provide useful sources of information.

27. OECD (2022). Risk Governance. OECD [online]. Available at: https://www.oecd.org/gov/risk/ (last accessed 15 March 2022)

46.9%
Yes, this is conducted by a central, corporate function or department (e.g. Business Continuity, Strategy or Risk).

27.4%
Yes, but many different departments do this according to their own needs.

20.4%
No, we don't do this.

5.3%
I don't know.

Figure 10. Does your organization conduct longer term trend analysis to better understand the threat landscape?

52.5%
Yes, I'm aware of the outputs and use them.

24.9%
Yes, I help develop the analysis in the first place.

19.9%
No, I do not have access to this information.

2.7%
No, I don't see the value of this information.

Figure 11. As a business continuity practitioner, do you draw on the outputs of this trend analysis for your programme?

Looking at how organizations perform their longer-term risk analysis, there seems to be a preference to rely on traditional processes more than automated systems. This is not surprising considering that the main tool to gather intelligence remains the internal risk and threat assessment (88.2%) for the second year running. This is the stalwart for risk analysis and it will take years before automated processes replace its effectiveness. The use of external reports and industry insights jumps up in second place - 77.7% of participants include these types of resources in their analysis, compared to 72% last year. This suggests that practitioners are becoming more resourceful in their search for reliable information. Industry research offers remarkable support to professionals in several aspects, such as helping them glimpse the bigger picture while also benchmarking their practices against their industry peers. Being able to access information on what other organizations are doing is a highly effective way to understand the organization's resilience posture and adjust if necessary.

Further down the chart, the duality in the type of information used for the analysis can be noted as risk registers (71.4%) — an internal resource — rank third and the participation to industry conferences and events (62.3%) — which rely on peer-to-peer discussions — are in fourth place. As anticipated, at the bottom of the chart are those solutions that are usually software-based, rely on automation and are more specialist in their application such as social media monitoring (39.6%), automated systems for cyber security (34.6%), and risk assessment software (18.6%).

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

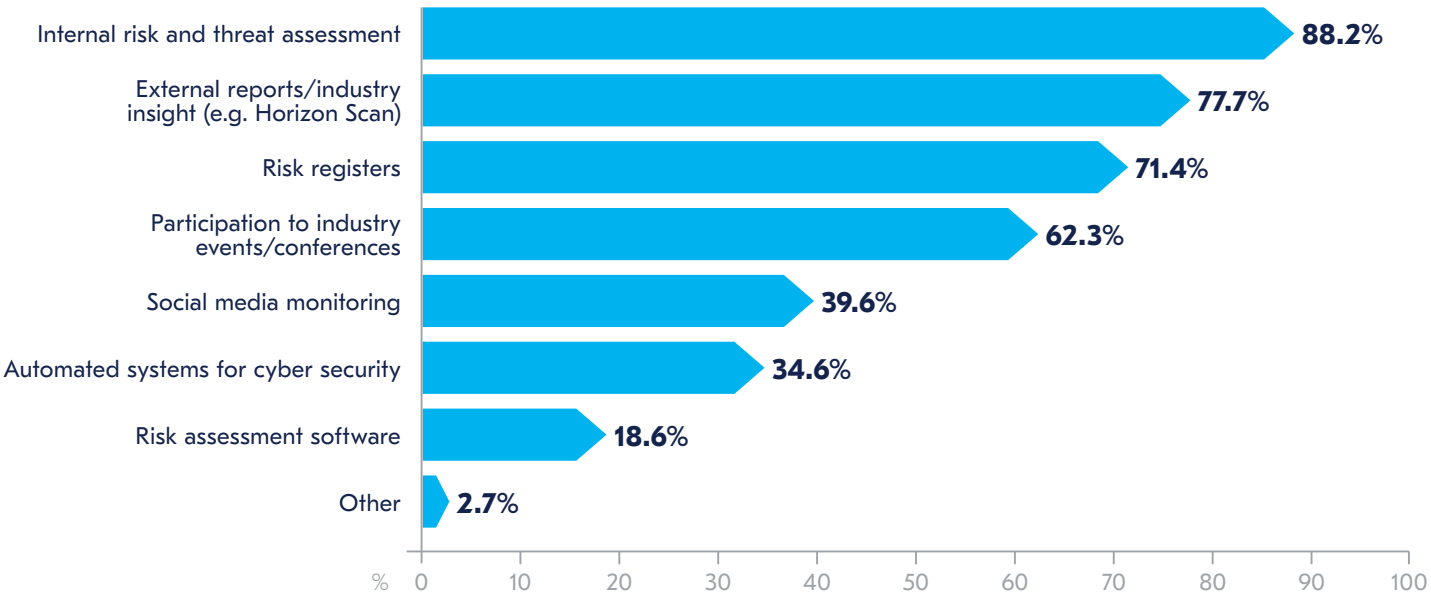


Figure 12. How do you conduct a trend analysis of the risks and threats to your organization?

When it comes to the maturity of respondents' Business Continuity Programmes (BCP), 54.2% report having a mature Business Continuity Management (BCM) programme which has been in place for more than five years, while an additional 39.5% have been engaging in BCM for 2 to 5 years. Only a small minority of them (6.2%) state that this is still new for the business. Compared to last year, fewer participants fall into the 1-year bracket, in favour of more consolidated programmes of 2-3 years. Respondents who report having new programmes is always a positive sign as it demonstrates an increase in the number of organizations who are deciding to employ BCM programmes within their organizations. Furthermore, this group of respondents are not limited to small businesses: some 80% of respondents who report new programmes (<1 year old) are from larger organizations.

A similar trend emerges from levels of investment into BC as more respondents are expecting to have increased budgets this year (33.9% compared to last year's 30.9%). Nearly half of organizations (46.6%) will maintain the same investment levels as last year and only 8.1% say they will cut financial resources for business continuity. While dedicating budget is paramount to a successful programme and a resilience organization, it is also important to remember the other key resource for BCM: people. The *BCI's Business Continuity Resources Benchmarking Report*[28] shows how the most effective BCM functions rely on allies and facilitators throughout the organization, highlighting the importance of embracing a resilience culture and raising awareness.

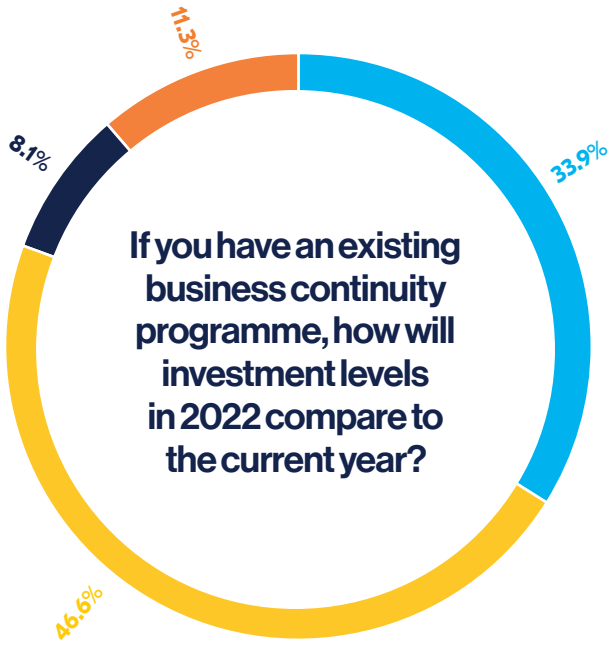
6.2%
1 year — this is still new for the business

21.3%
2-3 years — this has been recently established

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

54.2%
5+ years — this is a mature programme

Figure 13. How long have you been engaging in business continuity management planning for?



33.9%
Investment will be increased to meet the needs of a growing programme or new requirements.

46.6%
Investment will be maintained at appropriate levels for the programme scope and position in the lifecycle.

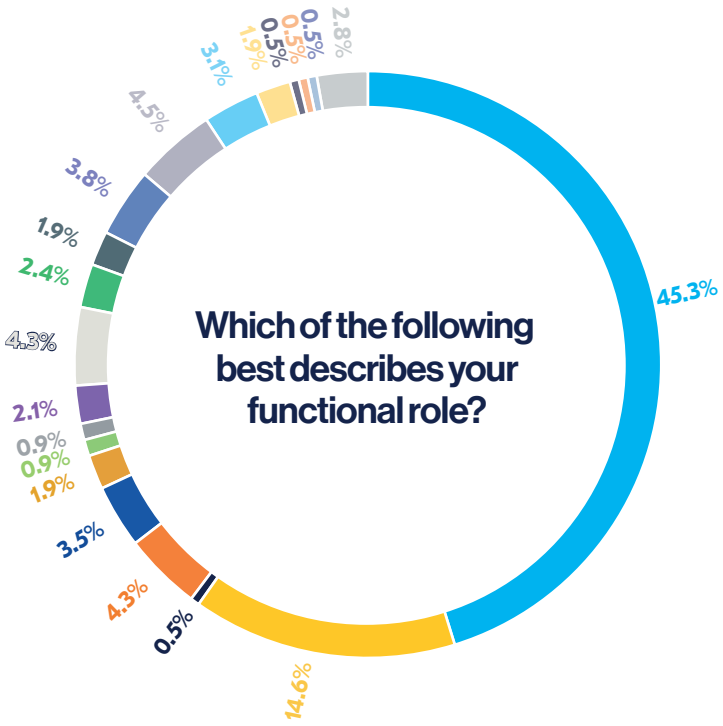
8.1%
Investment will be cut, limiting the scope or effectiveness of the programme.

11.3%
I don't know.

Figure 14. If you have an existing business continuity programme, how will investment levels in 2022 compare to the current year?

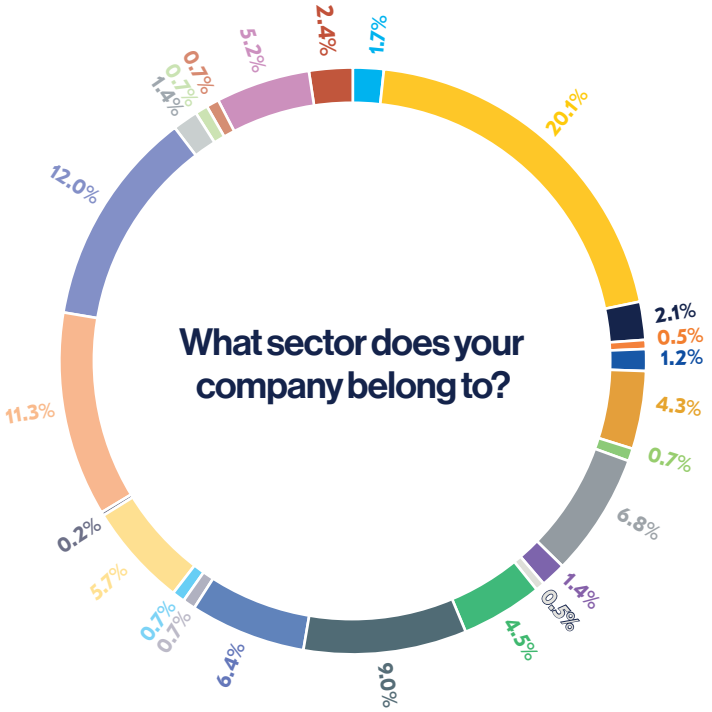
28. BCI, The (2022). BCI Business Continuity Resources Benchmarking Report 2022. The BCI. Available at: https://www.thebci.org/resource/bci-business-continuity-resources-benchmarking-report-2022.html (last accessed 15 March 2022)

Annex



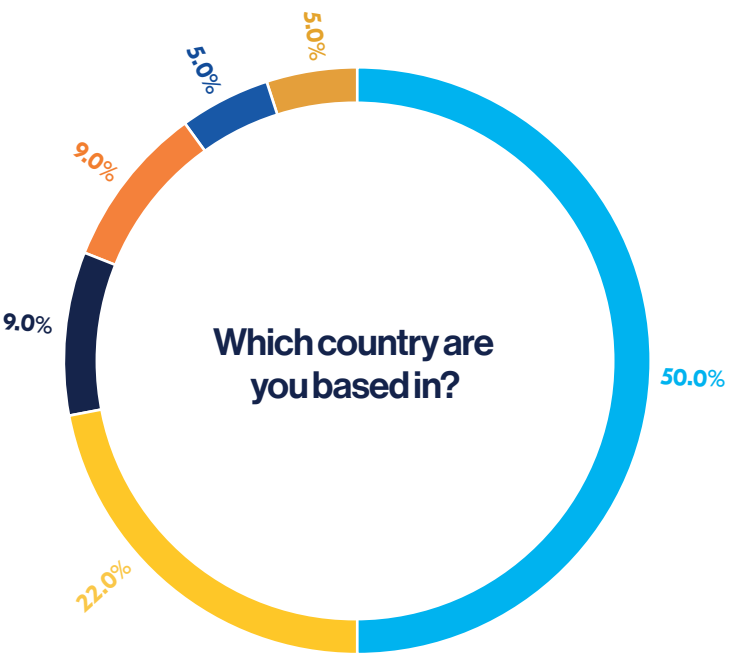
45.3% Business Continuity
14.6% Risk Management
0.5% Supply chain/logistics/ procurement/purchasing
4.3% Operational Resilience
3.5% Organizational Resilience
1.9% Internal Audit
0.9% Line of Business/ Service Directorate
0.9% Quality/Business Improvement
2.1% Health & Safety management
4.3% Emergency Planning
2.4% Security (physical)
1.9% Cyber/information security
3.8% IT Disaster Recovery/ IT Service Continuity
4.5% Crisis management
3.1% Top management
1.9% Operations
0.5% Human Resources
0.5% Marketing
0.5% Sustainability
2.8% Other

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



1.7% Aviation
20.1% Banking and finance
2.1% Charity/Not for profit
0.5% Consumer goods
1.2% Creative industries
4.3% Education and training
0.7% Emergency services
6.8% Energy and utilities
1.4% Engineering and infrastructure
0.5% Environment and agriculture
4.5% Healthcare
9.0% Information technology
6.4% Insurance
0.7% Law enforcement and security
0.7% Leisure and hospitality
5.7% Manufacturing
0.2% Medical devices
11.3% Professional services (including consuting)
12.0% Public services, government and administration
1.4% Real estate and construction
0.7% Retail and wholesale
0.7% Science and pharmaceuticals
5.2% Telecommunications
2.4% Transport and logistics

Figure 16. What sector does your company belong to?



50.0% Europe
22.0% Americas
9.0% Asia
9.0% Australasia
5.0% Africa
5.0% Middle East

Figure 17. Which country are you based in?

7.1% 1-10	**2.6%** 11-20
1.9% 21-50	**1.7%** 51-100
2.8% 101-250	**5.2%** 251 - 500
8.0% 501 - 1,000	**21.9%** 1,001 - 5,000
13.7% 5,001 - 10,000	**19.8%** 10,001 - 50,000
9.4% 50,001 - 100,000	**5.9%** More than 100,000

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

7.3% Less than €1 million	**7.1%** €1-10 million
4.5% €11-25 million	**3.5%** €26-50 million
5.2% €51-100 million	**4.7%** €101-250 million
5.7% €251-500 million	**5.9%** €501 million-€1 billion
13.4% €1-10 billion	**8.5%** €11-50 billion
5.0% Greater than €50 billion	**29.3%** I don't know

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

Asia Pacific: past twelve months

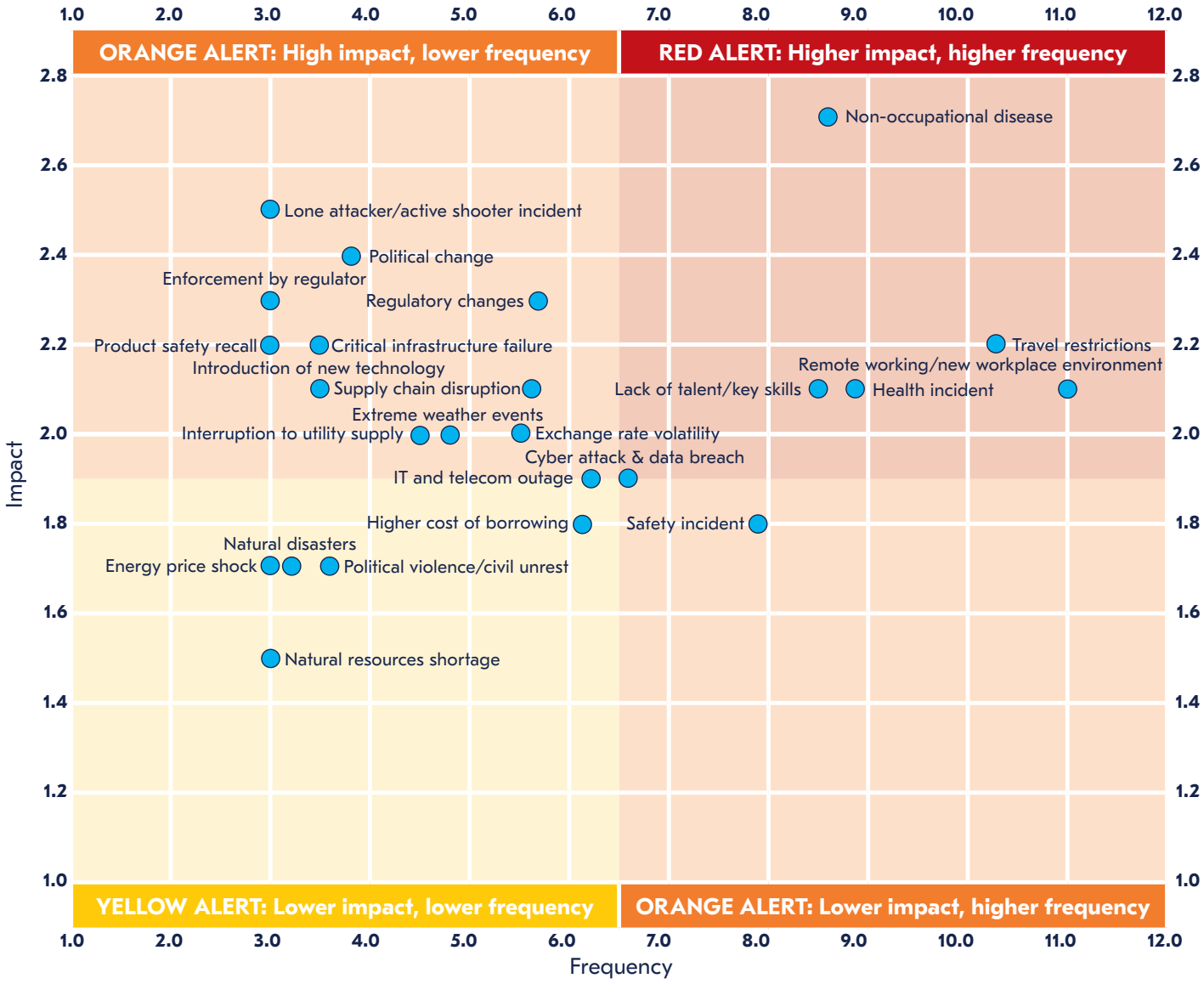


Figure 20. Risk and threat assessment: past twelve months (Asia Pacific)

Europe, Middle East and Africa: past twelve months

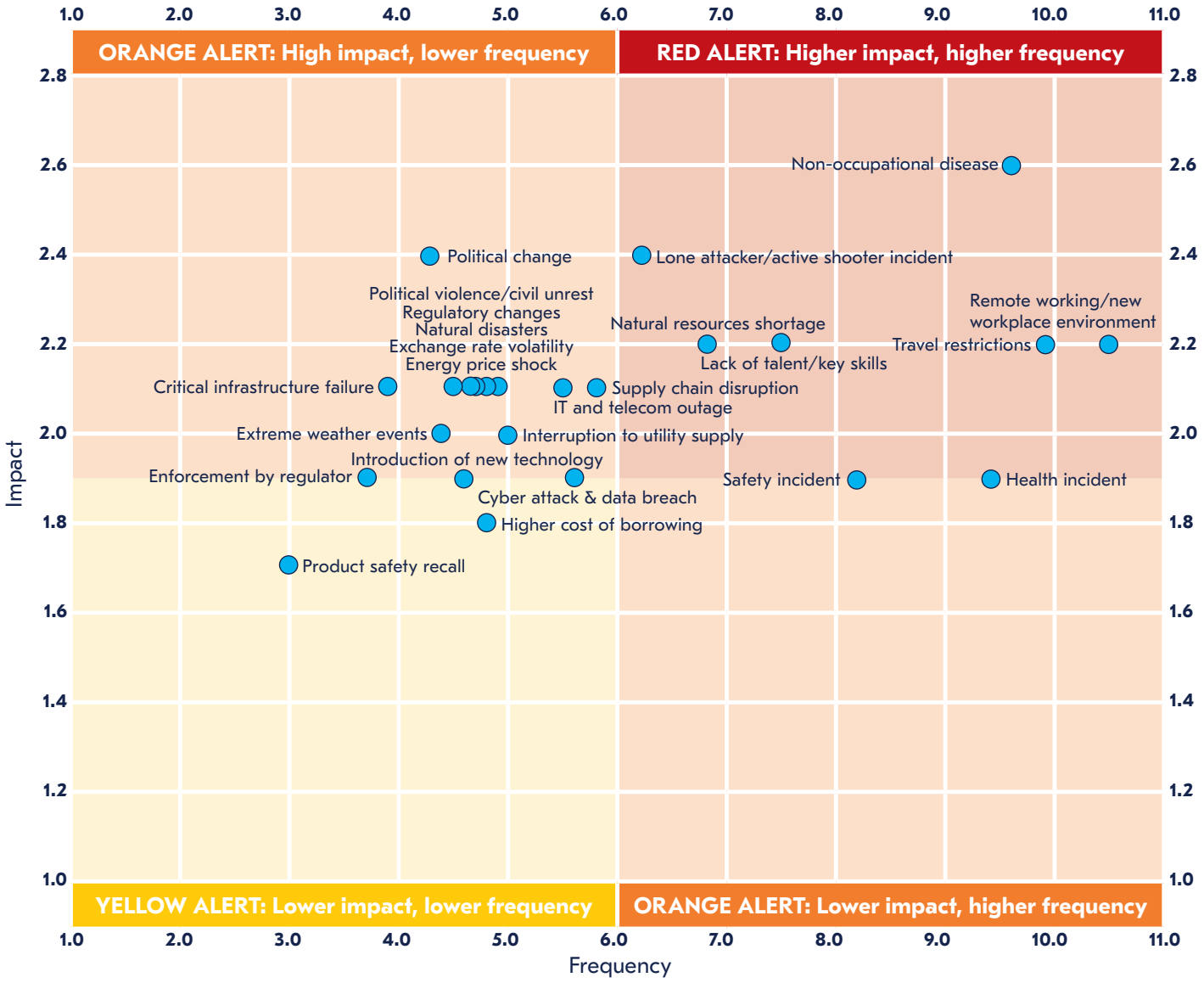


Figure 21. Risk and threat assessment: past twelve months (Europe, Middle East and Africa)

Americas: past twelve months

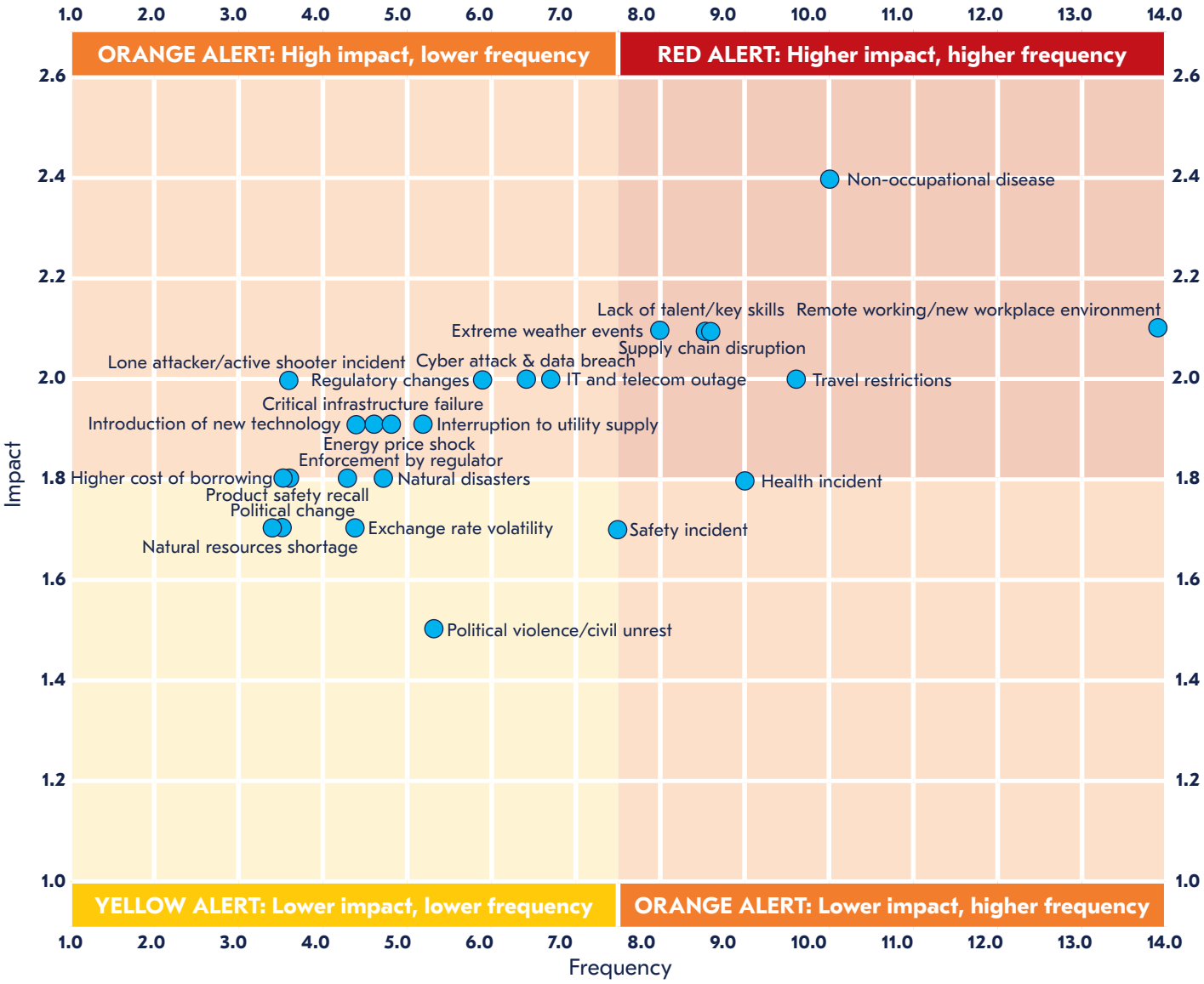


Figure 22. Risk and threat assessment: past twelve months (Americas)

Asia Pacific: next twelve months

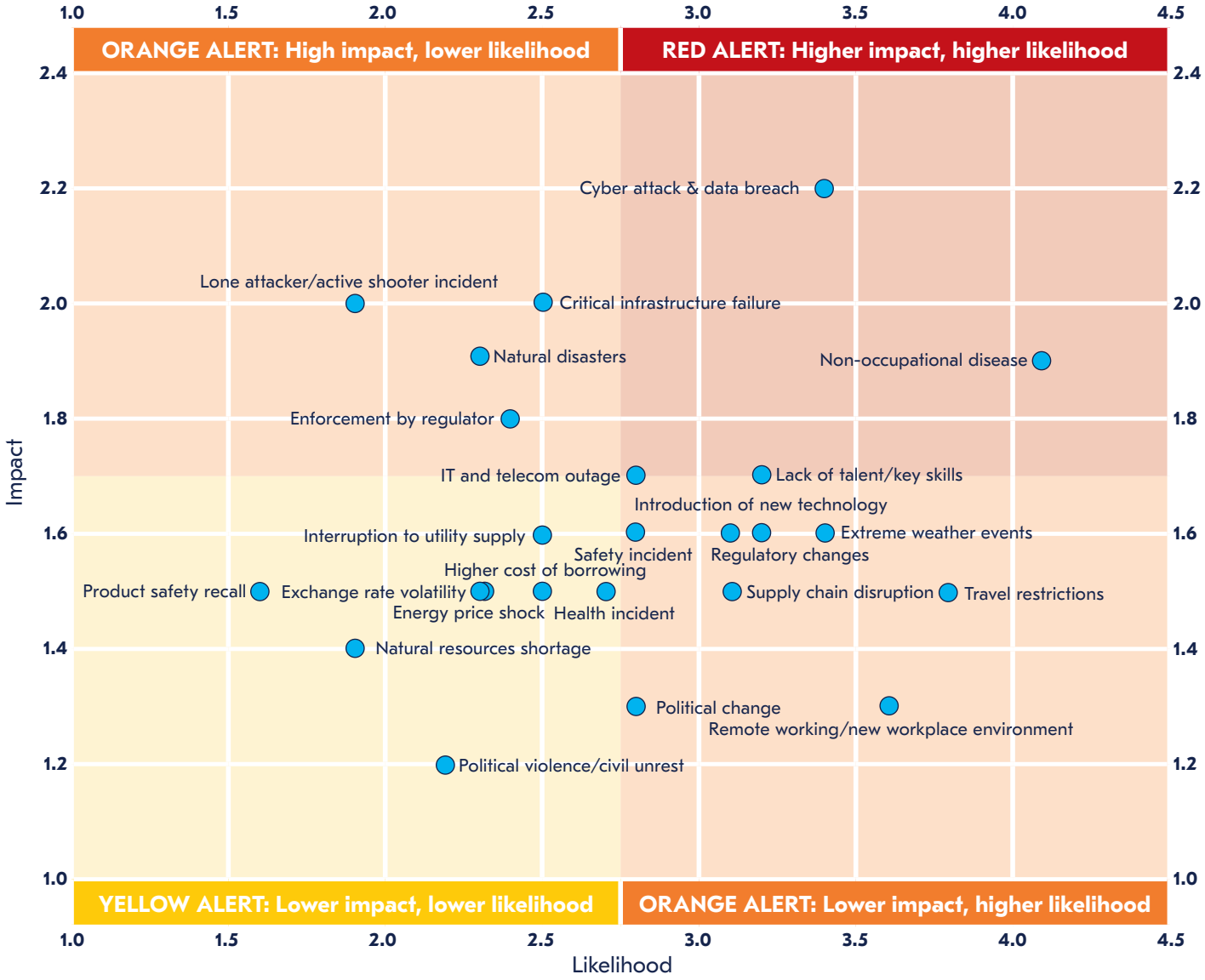


Figure 23. Risk and threat assessment: next twelve months (Asia Pacific)

Europe, Middle East and Africa: next twelve months

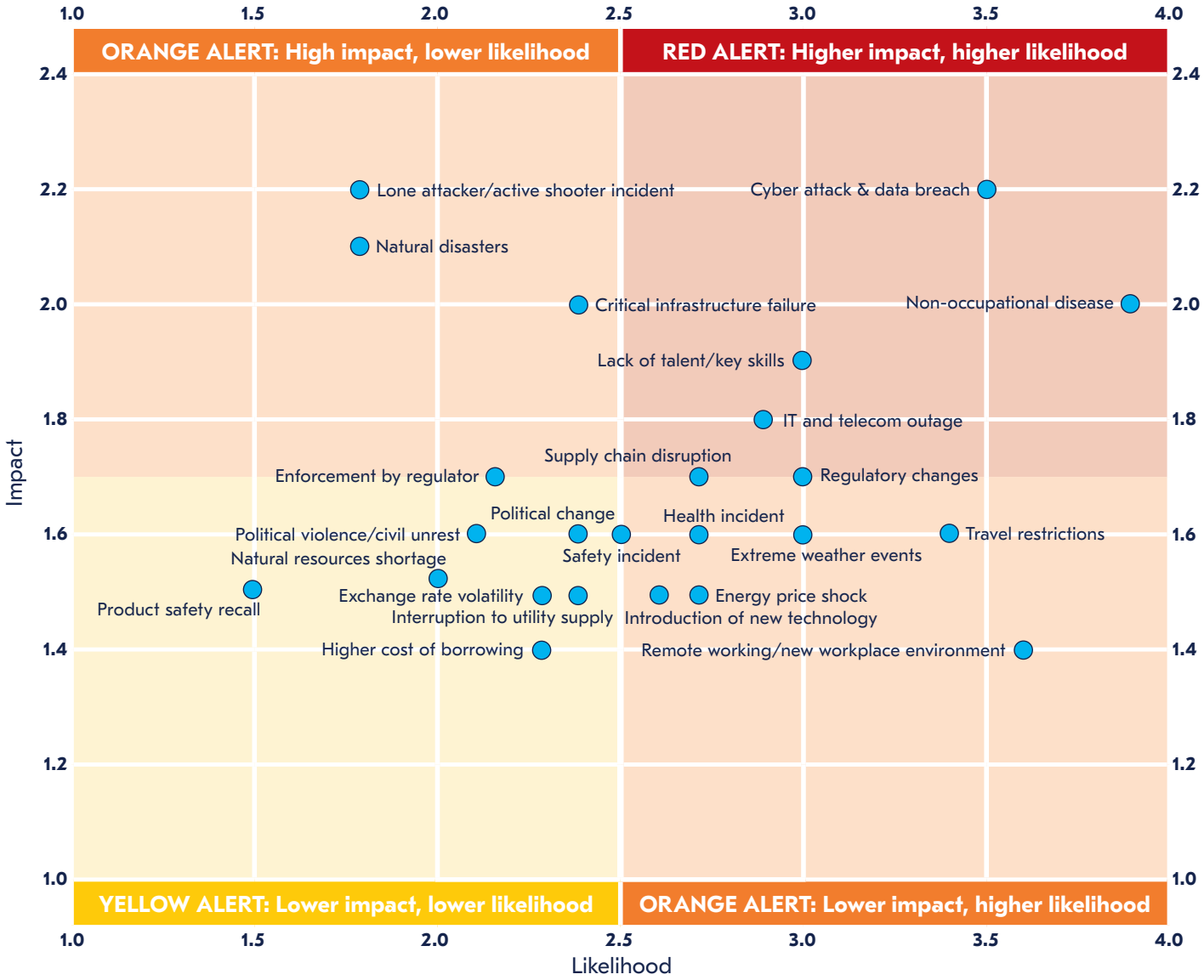


Figure 24. Risk and threat assessment: next twelve months (Europe, Middle East and Africa)

Americas: next twelve months

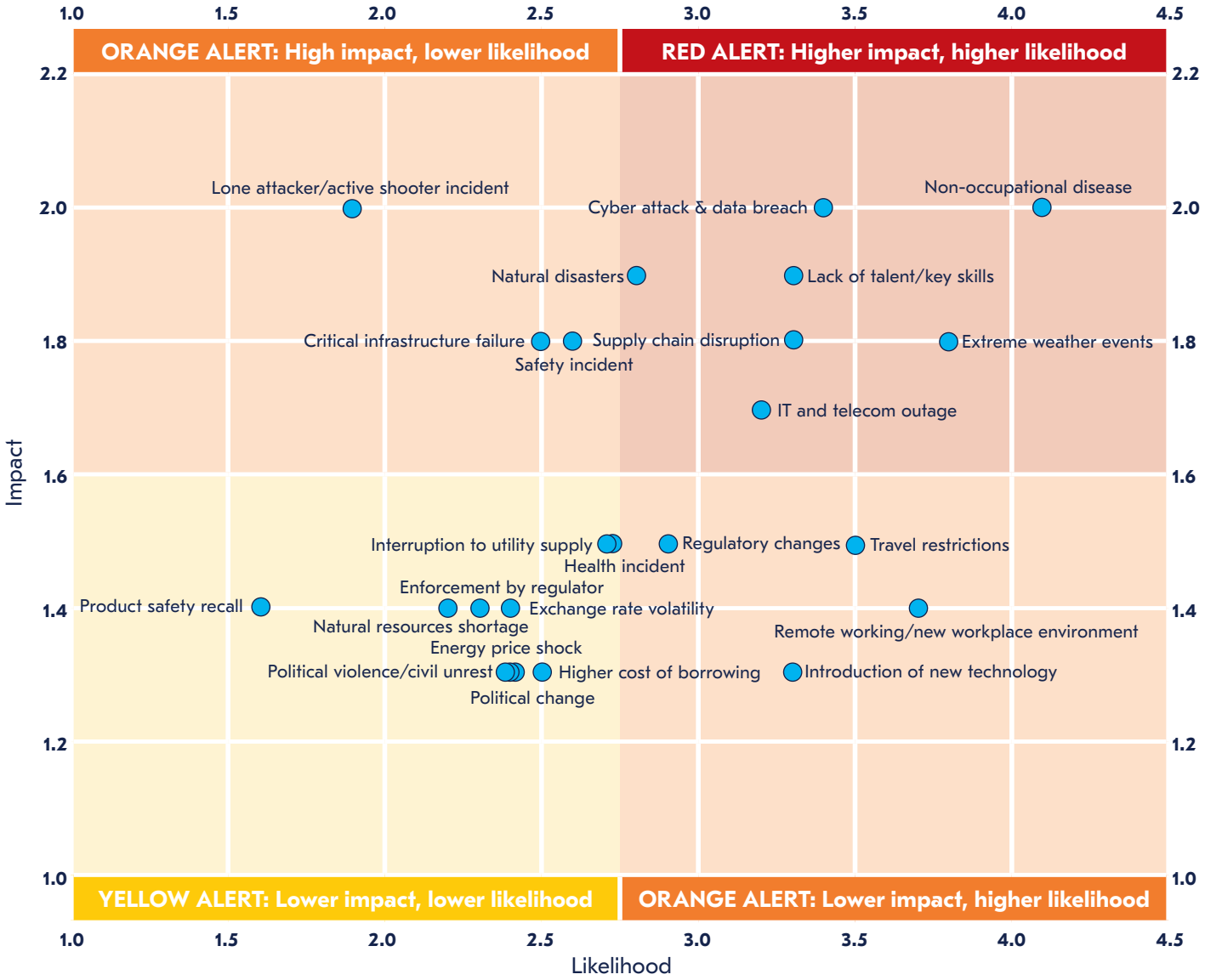


Figure 25. Risk and threat assessment: next twelve months (Americas)

About the Authors

Rachael Elliott

(Head of Thought Leadership)

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

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

Gianluca Riglietti

(Content Specialist in Business Continuity and Resilience)

Gianluca is a researcher and a freelance content creator interested in the development of resilient and safe societies. He has experience managing international research projects for companies such as BSI, Zurich, Everbridge and SAP. He works regularly with a number of organizations in the field of organizational resilience, such as the Business Continuity Institute. In his publications he has addressed a wealth of topics, such as climate change, cybersecurity, supply chain management and business continuity. He is also a PhD Candidate at Politecnico di Milano, where he investigates the impact of business continuity management on supply chain resilience.

He can be contacted at SCWF@protonmail.com.

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 2022

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