

Find out more
www.thebci.org

bci
Thought
Leadership

BCI Horizon Scan Report 2023



Contents

- 7 Executive summary
- 14 Incident assessment: past twelve months
- 40 Consequences of disruptions
- 46 Risk and threat assessment: next twelve months
- 56 Benchmarking long term threat analysis
- 65 Benchmarking business continuity
- 74 Looking ahead
- 84 Annex



Foreword

We are pleased to introduce the 2023 BCI Horizon Scan Report, one of the most established annual reports in our portfolio. We extend our thanks to Noggin for their sponsorship of this year’s report.

This year’s report falls at a critical point. Organizations are facing new challenges and, even now, ‘post-COVID’ seems a term of the past. That said, organizations are still facing legacy challenges related to COVID-19 which is best exemplified by [occupational] health incidents causing more disruptions to organizations globally than any other type of incident. Organizations are still battling with the challenge of ensuring a productive, yet nurturing, working environment, while others are allowing staff to ‘work from anywhere’ with little regard for work-area risk assessments.

However, this year’s report shows more profound regional differences in the top disruptors than noted previously. In North America and Asia, extreme weather tops the list in terms of 2023 disruptions. With El Niño returning in spring 2023, coupled with the effects of climate change, China witnessed its hottest ever temperature (52.2°C), Pakistan experienced devastating floods, while Canada saw wildfires destroy three-times more land (18.5m hectares) than ever experienced previously. In Africa, however, power outages were a primary concern as blackouts continued to wreak havoc for both homes and businesses.

Looking forward, cyber security dominates the threat landscape. While the rise in the number of attacks has been slower than previous years, cyber criminals are becoming ever more skilful in their attack curation. Furthermore, given concerns over state-sponsored cyber crime as a result of continuing global conflicts, coupled with concerns around the use of artificial intelligence (AI) to generate attacks and create deepfakes, cyber security’s position at the top of the table is hardly a surprise.

However, the risk index for 2024 does show a trend that we note every year in the Horizon Scan report: that of risks which are no longer front of mind plummeting down the risk table. As an example, non-occupational disease (e.g. pandemic) has fallen to 21st position in the risk index for 2024, despite publications such as the UK National Risk Register 2023 placing it as one of the greatest risks for the year. This demonstrates the importance of maintaining awareness of those high impact risks which are, for whatever reason, put at the back of the mind but still have a high chance of happening. These are famously dubbed ‘gray rhinos’ in Michele Wucker’s 2016 book of the same name.

Our profession is becoming more dynamic but, for many organizations, this means that the use of industry standards is more important than ever. Bitten by supply chain disruptions during COVID-19, organizations are now becoming more demanding in their supplier negotiations, with adherence to ISO 22301 (the business continuity management systems standard) now a common requirement. The report also shows that demonstrable resilience not only attracts shareholders, but also customers. As a result, alignment to ISO 22301 has reached an all-time high in this year’s report.

We would like to thank our members and contacts for their time and valuable insights; and for making this report possible through filling in the survey and being available for interviews. We have once again been inspired by some of the stories we have heard, with organizations ably emerging from catastrophic crises and going on to thrive – even more so than before. We would, once again, like to offer our sincere appreciation to Noggin for the sponsorship of this report.

Rachael Elliott
Head of Thought Leadership
The BCI



Foreword

Looking back on 2023, we note the sudden rise of consecutive, concurrent, and compounding crises. Captured in the BCI Horizon Scan Report 2023, these are disruptions that are proving more complex than ever to solve yet are requiring decision makers to act more quickly than ever. Adapting to this wider range of risks as well as the increasing occurrence of multiple, major incidents at once, organizations must embrace a comprehensive and holistic approach to resilience, to facilitate collaboration and coordination in response when it matters most.

Many organizations have made great strides. Personally, it is most heartening to see the positive involvement of senior management, particularly its increasing awareness of the need to adopt benchmark standards, such as ISO 22301:19 (security and resilience/Business continuity management systems).

Learning from past experiences, organizations, under the proper stewardship, are also increasingly centralising risk scanning processes. This approach, taken up by 57.8% of respondents, serves to streamline risk assessments, data interpretation, and decision-making, enhancing risk mitigation and enabling a proactive response to evolving threats. It correlates positively with the increasing use of long-term trend analysis in BC/resilience within organizations. With 77.5% of organizations drawing on these outputs, the use of long-term trend analysis is at an unprecedented high.

These positive trends are counterbalanced, though, by the vicissitudes inherent in the present risk environment. As the report also notes that new disruptions, such as the cost-of-living crisis, have burst onto the scene, only to interact with longer standing disruptions (e.g., supply-chain and wellbeing crises), exacerbating the effects of each.



One practitioner in public administration sums up this push-and-pull best: "From a resilience perspective, COVID-19 has really shone a light on some of our practices. Each time we have a disruptive event, we realise that perhaps we are not as prepared as we thought we were."

As a result, I come away from this admirable report with a sense of the work that remains to be done to achieve and maintain resilience. Although 48.3% of respondents plan to maintain investment levels in BC/resilience in 2024 and another 24.6% to increase, I worry about the preparations that are needed to face multiple simultaneous events. Add to that, the uptake of technology to help with risk scanning activities remains frustratingly low, as most organizations still do not have a formalised electronic system to manage disruptive incidents.

Reviewing the BCI Horizon Scan Report 2023, I therefore remain ever more committed to the Noggin company mission to work hand in glove with customers to facilitate and enable their resilience journey with Noggin's thoughtful, integrated software solutions. I must also thank our great partner, the BCI, for allowing us to be a part of this latest resilience-enhancing resource for, as the survey itself notes, such resources are invaluable for practitioners to maintain a comprehensive perspective of the risk landscape.

Finally, to survey readers directly, I hope you take to heart and to practice the many valuable insights that are contained within it to build a solid culture of resilience.



James Boddam-Whetham
Chief Executive Officer, Noggin

Executive summary





The consequences of the pandemic continue to dominate organizations’ agendas in 2023 in the form of health incidents such as stress and/or mental health. The cost-of-living crisis features for the first time as a top threat for organizations.

While the height of the COVID-19 pandemic has passed for all countries, the effects and impacts of the last three years on organizations’ workforces cannot be ignored. Organizations report a considerable increase in sickness absence due to health incidents such as stress, depression, and anxiety within employees.

Top five incidents for organizations over the past 12 months

- 1  Health incident
- 2  Safety incident
- 3  Increased cost of living
- 4  Supply chain disruption
- 5  Non-occupational disease

COVID-19 related disruptions have lessened throughout 2023, but primary disruptions in the last three years have all related to the human factor.

In the period 2020 to 2023, key threats identified by organizations were related to employee’s health incidents such as occupational disease, and infectious disease (pandemic); while the primary risks to organizations between 2013 and 2019 were cyber-attacks or IT/telecom outages.

The greatest single disruption for organizations in the past twelve months has been IT and telecom outages.

The move to remote and hybrid work models has emphasised the need to deal with IT and telecom outages. 20.4% of respondents reported that an IT/telecom outage was their organization’s most disruptive event in the last 12 months.

Top five most disruptive events for organizations in the past 12 months

- 1  20.4% IT or telecom outage
- 2  10.9% Critical infrastructure failure
- 3  10.2% Extreme weather events
- 4  6.1% Cyber-attack
- 5  5.4% Lack/loss of talent/key skills

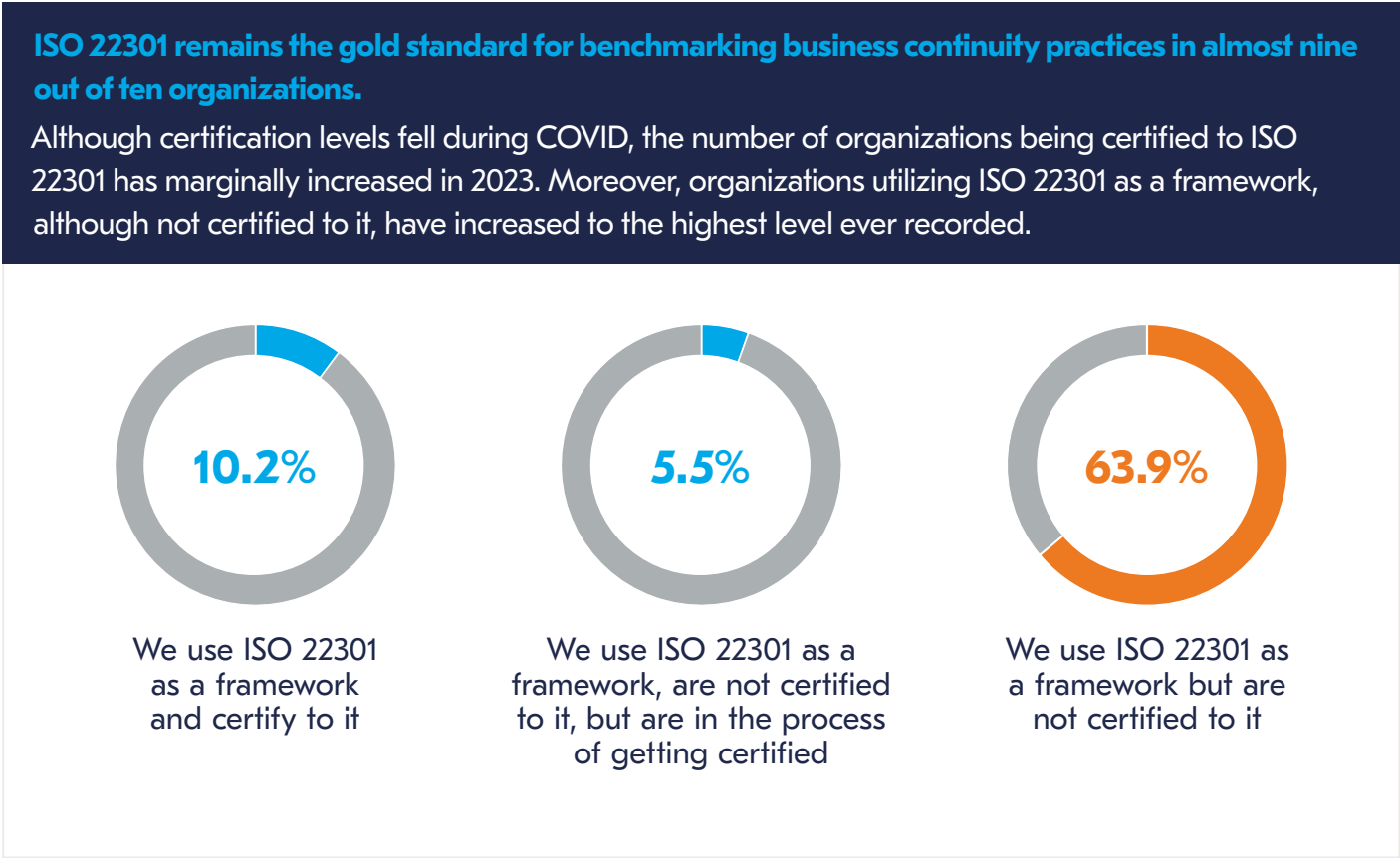
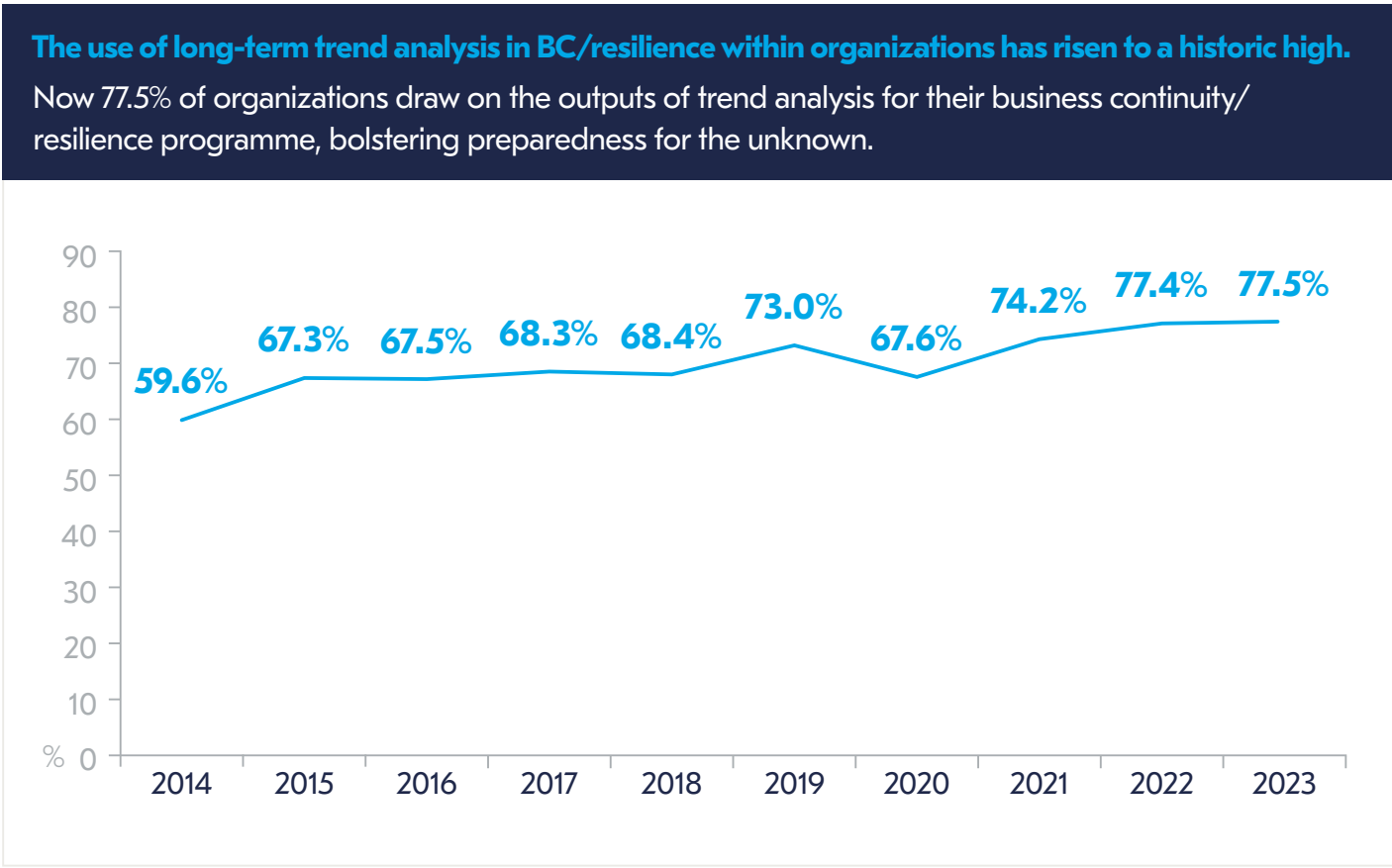
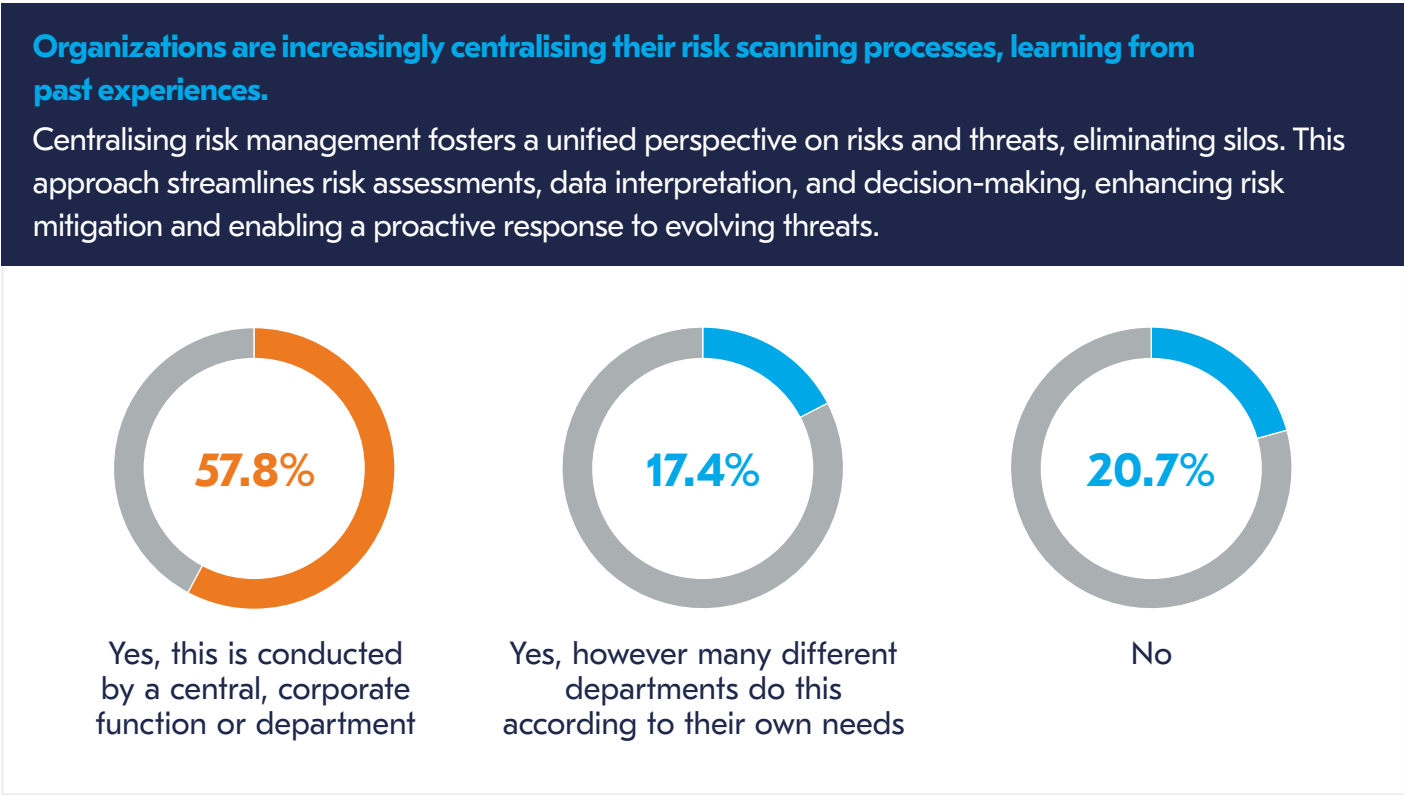
Loss of productivity was the greatest consequence of disruption to organizations in 2023.

This demonstrates the importance of the human factor within organizations and the need to focus on staff wellbeing programmes to support employees and build stronger organizations.

Top five consequences of disruptions for organizations

- 1  63.7% Loss of productivity
- 2  37.0% Customer complaints received
- 3  34.9% Negative impact on staff morale/wellbeing/mental health
- 4  33.5% Reputation damage
- 5  29.4% Loss of revenue

Top five risks for organizations in the future.			
Short-term: over the next 12 months (2024)		Mid to long-term: over the next 5 to 10 years (2029-2034)	
1	Cyber-attacks	1	Cyber-attack
2	Extreme weather events	2	Climate risk
3	IT or telecom outage	3	Supply chain issues
4	Increased cost of living	4	Technology or telecoms outage
5	Interruption to energy supply	5	Geopolitical changes



Top three benefits of certification.

1

88.2%
Allows us to demonstrate the effectiveness of our BCM programme to external stakeholders

2

82.3%
Increases our organization's resilience

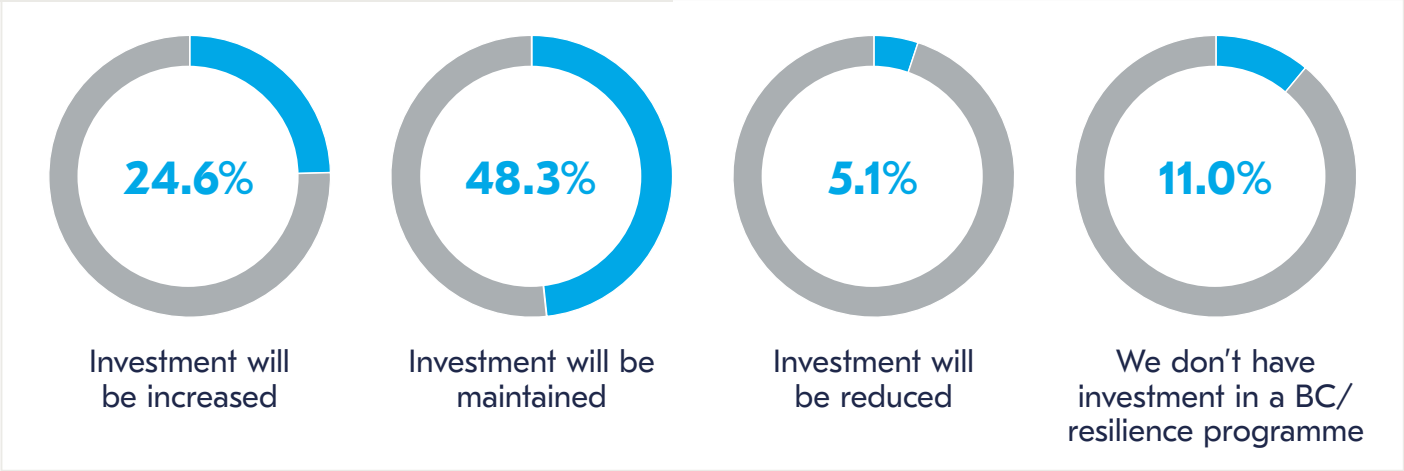
3

58.8%
Enables faster recovery after a disruption

Investment in BC/resilience is likely to remain at current levels in 2024.

Two in four practitioners expect business continuity and/or resilience funding to stay the same in 2024 as in 2023, as a result of economic downturn. However, one in four practitioners expect investment levels to increase in 2024, in order to meet the needs of a growing programme or new requirements.

How will investment levels in 2024 compare to the current year in order to better prepare for the challenges/threats identified in horizon scanning?



There is a low uptake within organizations of the use of technology within risk analysis functions.

Most risk analysis work is done manually, via public sources and through peer collaboration. Moreover, most organizations don't have a formalised electronic system to manage disruptive incidents.

Top five tools for conducting trend analysis/horizon scanning within organizations

1

87.9%
Internal risk and threat assessment

2

77.6%
Social media monitoring

3

77.6%
External reports/industry insight

4

61.2%
Participation in industry events/conferences

5

60.3%
Collaboration with peers



Overview

The previous edition of this report depicted a risk landscape defined by issues related to the pandemic, such as supply chain issues and adapting business continuity practices to the new working environment. As the world adapted to functioning in new workplace environments, employers worked to ensure that their workforce had the necessary equipment and suitable IT infrastructures to adapt to remote or hybrid environments. At the time there was also an initial awareness of geopolitical events and their influence within the risk landscape, due to the escalating conflict in Ukraine.

In this new edition of Horizon Scan, organizations are facing a wider range of risks, as well as increasing occurrences of multiple, major incidents happening at the same time. In 2023, the incidents organizations have faced has evolved since in 2022, with non-occupational disease falling from first to fifth place in terms of disruptions faced over the past year. Over the year, organizations' have seen stress/mental health issues, safety incidents, and the cost-of-living crisis/inflation as the primary cumulative events causing disruption. Alongside these events, supply chain disruptions, interruption of energy supply, and weather-related events have also caused significant disruption to organizations' operations.

Meanwhile, the events which caused the largest singular disruption tended to focus more on acute impacts, typically related to technology disruption or natural disasters. The singular disruptions that caused the most impact were IT and telecom outages, critical infrastructure failures, extreme weather events, cyber-attacks, and the lack/loss of talent.

Also, the effects of geopolitical events, such as the Ukraine conflict, have had a major impact around the world: global supply chains and financial/energy markets have exhibited high degrees of volatility. These issues highlight the need to increase organizational awareness of the wider implications of political changes and/or political conflict when assessing the threat landscape.

For some organizations, certifying to national or international standards can help them to become more able to plan and respond effectively to disruptions. It is therefore positive to note a trend noted in the previous edition of this report has continued to consolidate in 2023: there is a growing awareness among management regarding the adoption of standards, leading to an increase in the number of organizations opting to align themselves with the ISO 22301:2019 (Security and resilience/Business continuity management systems) standard. This is regarded as one of the gold standards within the business continuity and resilience industry, and helps not only to combat disruption, but also showcase to potential suppliers and customers the strength of their resilience programme.

Once more, this report demonstrates that resilience professionals' minds still deviate towards the incidences that have occurred over the past year when considering their risk mapping for the coming year. However, there is a notable reduction in this trend in this year's report, testament to the better resourced and improved centralisation of horizon scanning processes.

Incident assessment: the past twelve months



Incident assessment: the past twelve months

- The consequences of the pandemic continue to dominate organizational agendas in 2023. There has been an uptick in sickness absence due to health incidents such as stress/mental health; and continued pandemic-linked supply chain disruptions.
- The cost-of-living crisis features for the first time within the top three disruptions for organizations in 2023.
- Technology has been the most disruptive element that organizations have suffered over the last seven years. This continues in 2023, with IT and telecom outages being the biggest disruptor for organizations.
- The need to consider and plan for simultaneous multiple events increases, as the variety of threats organizations are facing multiply and interact with each other, deepening the impact of events.

On 5 May 2023, the World Health Organization announced that COVID-19 would no longer be classified as a Public Health Emergency of International Concern (PHEIC). While COVID-19 infections are still occurring around the world and new variants continue to develop, the immediate threat has been effectively mitigated¹. As a reflection of this, non-occupational disease (pandemic) has gone down from the number one impact to organizations in 2021 and 2022 to the fifth place in 2023: and the risk score² has nearly halved from 24.5 in 2022 to just 13.3 in 2023.

Currently, the top disruption for organizations is health incident, defined as occupational disease, stress/mental health, and increased sickness absence. It has a risk score of 16.1. The impact score of this threat is lower than the other top ten threats in 2023, but the frequency (8.4) is considerably higher, positioning it as the incident which organizations have seen the most disruption from in 2023.

While the height of the COVID-19 pandemic has passed, the effects and impacts of the last three years on organizations' workforces cannot be ignored³. A recent examination of the worldwide mental health consequences stemming from the COVID-19 pandemic substantiates concerns about the surge in depression and anxiety. Indeed, the results of a survey by KFF/CNN in May 2023 showed that 90% of Americans believe that the country is still facing a mental health crisis which, in turn, is leading to increased substance abuse⁴. Moreover, research carried out by the organization PwC within its UK personnel shows that poor mental health is the main cause of long-term sickness in its workforce.⁵ Corroborating this further, an interviewee explained how, in the health sector, people are leaving as they cannot stand the pressure any longer.

"I spoke to someone probably about six weeks ago and they said it was their last day. I asked them where they were off to, and they replied with: 'I haven't got another job. I'm just leaving because I can't take it anymore'."

Resilience and response manager, health & social care, UK

The number of work-related health issues has also been influenced by the consequences of the COVID-19 pandemic. Firstly, through cases of COVID-19 believed to be from exposure to COVID at work and, secondly, by playing a role as a contributing factor to other health concerns, with a particular emphasis on stress, depression, and anxiety. Two to five years prior to the pandemic, the trend in self-reported work-related health problems was in decline. However, in the two years immediately preceding the pandemic, this decline levelled off, indicating a stabilisation in the rates. Now, the rate of work-related health issues is higher than the levels observed in the pre-COVID period of 2018/19, highlighting the profound impact of the pandemic on workplace health. According to the Health and Safety Executive (HSE)⁶, 1.8 million of workers in the UK suffered from work related ill health in 2021/2022. Over half of these cases (51%) were due to stress, depression, or anxiety. Another 27% were due to musculoskeletal disorders which could be attributed to higher levels of homeworking.

"Most of my workforce is an average age of 35-45, with 15-20 years of administrative working experience. Occupational diseases, especially ergonomic ones, are appearing which is also being fuelled by consumer habits."

Business continuity coordinator, support services, Portugal

"There are issues arising from remote and hybrid working; it suits a lot of people. However, it does not suit everyone, resulting in some mental health issues. We also need to make sure employees have the correct workstation equipment to prevent musculoskeletal issues arising."

Business continuity manager, public sector, UK

"Working from home has a big impact on the health and wellbeing of our staff. This is paramount to us and as part of our strategic risk review, we are monitoring and managing this closely."

Business continuity manager, public sector, UK

When it comes to any form of business disruption, determining the cost of readiness and impact mitigation can be guided by cost-benefit analyses. However, the positive effect of extra resources for mental health and wellbeing is not eminently quantifiable. COVID-19 was the most rigorous test of employee wellbeing than many companies had ever faced and mutual support became essential during this period to avoid employee attrition.⁷ Furthermore, with new crises having the potential to cause further emotional upheaval (e.g. civil unrest and global conflicts) organizations should take this into consideration and ensure that measures to support the wellbeing of employees remain in place.

Safety incidents take second place in the 2023 table of disruptions despite, or because of, the move to remote/hybrid environments?

Safety incidents (personal injury, fatality, asset damage, dangerous occurrence, and reportable incident) is in second place in this year's risk index with a score of 14.2. This has featured in the top three risks for organizations since 2019.

According to the International Labor Organization (ILO), around 2.3 million people globally lose their lives due to work-related accidents or diseases annually, equating to more than 6,000 fatalities daily. Furthermore, there are 340 million occupational accidents each year, leading to 160 million individuals suffering from work-related illnesses.⁸ The ILO periodically revises these statistics and the revisions reveal a consistent rise in both the number of accidents and the prevalence of work-related health issues.

Furthermore, the number of incidents reported globally is likely to be lower than the number of actual incidents that have taken place. In the UK, for example, there were 61,713 injuries to employees reported under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) in 2021-2. However, given the decline in the number of investigations that the HSE has been carrying out, it is likely that the true number of incidents is not publicised.⁹ The same phenomenon is noted globally: in the United States, for example, as many as 69% of workplace injuries, illnesses, and deaths are never reported¹⁰ while in Australia, the figure may also be as high as 66%¹¹.

“The major safety incidents or accidents that occur are when people are coming in and out of the site, which is usually a fall or a car accident. When these accidents happen in a small team, and one person is out for two months that can be a big deal.”

Business continuity coordinator, support services, Portugal

Given the high degree of underreporting to national and regional governments, coupled with the lack of spot-check investigations, organizations should conduct their own internal enquiries to understand the underlying factors behind incidents as a matter of course; and then should implement measures to prevent or minimise the likelihood of a recurrence. These measures need to be well-documented to provide evidence of the organization’s commitment to ensuring workplace safety.

The final disruption in the top three is the increased cost of living with a risk score of 13.6. The cost of living, together with inflationary pressures, has a substantial impact on individuals, families, organizations, and economies.

Most economies around the world have noted a rise in the cost of living in 2023 and research from the Economist Intelligence Unit (EIU) notes that while New York and Singapore have the highest cost of living globally, Istanbul (Turkey), Buenos Aires (Argentina), and Tehran (Iran) noted increases of 86%, 64%, and 57% respectively between 2021-2022¹². Given differing tensions in 2023, the EIU predicts that inflation will continue well into 2024, which could result in a global recession¹³.

As a result of the increased cost-of-living, staff may need to allocate a larger portion of their income to meet basic needs, leaving less for discretionary spending or savings. For some staff, it could even push them into poverty. This stress can negatively affect mental and physical well-being, ultimately impacting organizations as employees fail to perform and impacting on an organization’s overall resilience.

“The current condition of the economy puts a strain on the mental health of employees; this is not something that has been reported but it has been noticed. I think in the long run it’ll ultimately show its head because a lot of staff are under strain in terms of finances, and the economic conditions are not that great. Ultimately, they will have increased pressure at work, but if the economic conditions are not also helping, the pressure will ultimately get to you, and it’ll impact on your mental health.”

Business continuity manager, financial services, South Africa

The increased cost-of-living, together with inflationary pressures, weigh on organizations and staff alike

Increased cost-of-living can lead to wage pressure on employers and organizations in regions most affected are likely to face increased competition for talent. This can drive up labour costs and necessitate more robust employee retention and attraction strategies, such as offering competitive salaries, benefits, or remote work options. In areas where costs are high, such measures will be difficult — or even impossible — to implement. In addition to this, organizations may also face higher costs for inputs and services as their providers respond to rising operational expenses. Providers may also seek to renegotiate contracts or increase prices to offset their own rising costs. While this may be unavoidable for some organizations, it highlights the importance of forging deep relationships with providers in order to receive early warning of potential supplier price increases.

To demonstrate the supplier problem further, BDO conducted a survey in April 2022 to determine how the cost-of-living crisis was affecting organizations¹⁴. Rising costs posed the most significant challenge for businesses and nearly a third of respondents were looking for additional financing in response to inflationary pressures. To mitigate the impacts, a third of organizations were raising the prices of their goods and services. A similar percentage also planned to move to cheaper suppliers to reduce costs. An interviewee from the United States explained the changes in plans that they had been forced to make, while others spoke how the issue had affected them.

“We opened a new international headquarters; we had a goal to hire an X number of people, but it has been hard to do. The hiring growth has been slowed due to economic factors, but we have also slowed down our plan. We may need to relocate people or hire people on a remote working basis instead of having as many people in the office than we initially thought when we opened.”

Business resilience programme manager, IT & communications, USA

“The increase in the cost of living in the community is having a negative impact on the population, which in turn demands more on our services because of the greater need for support.”

Business continuity manager, public sector, UK

“The increased cost of living impacts us professionally and personally; there is a ripple effect.”

Business continuity manager, financial services, South Africa

“We are seeing a lot of investments slowing down. Investors are being careful with how they invest; this puts a strain on our economic growth.”

Business continuity manager, financial services, South Africa

Supply chain disruption continues to disrupt organizations, with price volatility, global conflict, and extreme weather all weighing heavily on supply chains in 2023

Supply chain disruption is in fourth place in the 2023 risk index, with a score of 13.3. The third and fourth top risks for organizations in 2023, are clearly interlinked.

COVID-19 wreaked havoc with supply chains, the effects of which have been well-documented in previous BCI research reports¹⁵. Shipping lines were severely disrupted, factories were closed, and organizations that relied on just-in-time manufacturing sought to stockpile goods. Shipping costs increased massively and organizations which were not prepared for supplier disruption suffered, with some sadly having no choice but to enter into liquidation. The emergence of the Delta variant of COVID-19 in May 2021 further exacerbated production delays and supply chain disruptions. Additionally, there were global shortages and disruptions in supply chains, including those resulting from ongoing lockdowns in China, which led to a severe shortage of shipping containers. Inflation in late 2021 was a due to a combination of excessive demand and rising costs. In February 2022, the conflict in Ukraine caused another shock to supply chains and led to changes in global energy and commodity markets. This, in turn, led to increased fuel and food prices in many countries. Other contributing factors to the current cost of living crises include China’s persistent zero-COVID policy and extreme weather events, such as heavy rainfall, flooding, wildfires, and droughts experienced worldwide in 2022 and 2023. These events affected agricultural outputs and contributed to rising freight costs.¹⁶

Supply chain disruptions are expected to persist throughout 2024 and, according to KPMG¹⁷, a secondary wave of supply chain risks is expected to materialise during the year. Escalating global conflicts could result in lack of availability of materials or major trade routes closing. Simultaneously, there may be fluctuations in key commodity prices and availability, including fuel, construction materials, and packaging. Ensuring that sound resilience measures are in place for supply chains, together with strict supplier due diligence methods should help to shield organizations from the worst effects.

“Lack of components was a huge impact for us during COVID-19; getting laptop replacements for employees to new hires was tough; these were on back order for 18 months. The impact was also felt in our supply chain, and we were not able to have certain products needed for our customers and were waiting on back orders.”

Business resilience programme manager,
IT & communications, USA

“When we are all working from home, we are reliant on IT equipment; getting sufficient rotation of new equipment is a problem because there has been supply chain issues with the chips that go into the laptops.”

Business continuity manager,
public sector, UK

It is clear that organizations need to continue to work to ensure that their supply chains are resilient to the known – and unknown – threats to their organization. While the steps taken to bolster resilience still surpass pre-pandemic levels, overall focus on resilience declined in 2022 as the immediate pandemic pressures started to ease¹⁸. Given the mounting challenges affecting entire supply chains, particularly amid different events, there remains a need for heightened resilience measures.

“We are now trying to forecast further ahead than we did before COVID because when that happened, things just shut down and nothing was being delivered for a long time.”

Business resilience programme manager, IT & communications, USA



COVID-19 remains in fifth place in terms of disruptions for 2023 – but shoots down the list of concerns for 2024

The fifth most disruptive event for organizations in 2023, down from first place since 2021, is non-occupational disease with a risk score of 13.3. This option has dominated the top of the rankings since 2020 as many organizations remained in the response phase of COVID-19 into 2022. However, as mentioned previously, the fact that COVID is not a PHEIC anymore, does not mean that the pandemic is over – and professionals should be minded not to remove the topic from future risk scanning activities. Indeed, the WHO’s regional director for Europe, Hans Kluge, said that summer 2023 was going to be “the first in more than three years that many of us will enjoy without the looming threat of COVID-19”, but the life-threatening virus has not gone away completely¹⁹. He also explained that, during the initial three years of the global health crisis, it is estimated that approximately 36 million individuals in Europe may have grappled with ‘long COVID’, a complex condition that remains poorly understood by scientists, but one which still having an impact on staff absence²⁰.

Globally, up to 12 October 2023 there have been 771,191,203 confirmed cases of COVID-19, including 6,961,014 deaths, reported to WHO²¹. Cases continue to develop and rise in winter months in most regions, but organizations are now accustomed to managing the threat posed by COVID-19. In the last edition of this report²², respondents highlighted that COVID-19 caused a long series of knock- on effects in various areas, from the transformation of business processes to issues with employees’ mental health. The importance of this is noted in this year’s report with health incidents identified as having the greatest impact on organizations.

“We had a small outbreak of COVID-19 in the organization as a new wave moved through the region. We were able to use one of the plans designed around infectious disease control to prevent it from going any further. Approximately, 15% of the organization were impacted and, with being a small organization, it could have had quite significant consequences. Our measures enabled us to get on top of the outbreak and prevent a wider outbreak.”

Organisational Resilience advisor, public administration, New Zealand

“There are ongoing impacts since COVID-19 because we are also involved with supporting health services as part of an integrated care system. Part of the pressure from COVID-19 is that there has been a delay in providing services over that time so we are still experiencing the knock-on effect of that. We are experiencing increase demand for support for children and adults.”

Business continuity manager, public sector, UK

“We still have several COVID-19 related issues, we are keeping a very close eye on this. If it escalates, we will scale down some services and redeploy staff to support critical frontline services.”

Business continuity manager, public sector, UK

Energy supply disruption enters the top six due to price volatility and energy scarcity

Disruption of energy supply rose to sixth place in the table this year, with a risk score of 13.1. Although gas prices have fallen from a peak of €300 per megawatt hour in August 2022 as a result of the conflict in Ukraine, volatility remains high. Tensions in the Middle East saw European gas prices hit their highest level since March in early October 2023, with the price of futures contracts for Dutch gas rising by more than a third in a month²³. In addition to large scale conflicts, there are also concerns about possible sabotage of energy supplies. With Finland currently considering sabotage as the cause of a leak in one of its major gas pipelines, the UK’s risk register has put an attack on UK energy infrastructure as having a ‘significant’ impact and being 5%-25% likely to happen over a two-year period²⁴. Meanwhile, loadshedding in South Africa continues with regular blackouts as the power network struggles to cope with demand.

“A lot of our patients are secure patients, so they need to be kept secure within the units. All our doors operate on magnet locks, so if energy goes down, it’s a case of getting as many people on doors as we possibly can.”

Resilience and response manager, health & social care, UK

“We’re having a lot of power shutdowns. So, it’s a case of the power being shut down for pre-planned hours. Even though we kind of get a heads up on it, it still takes quite a lot of work from us to make sure there’s the correct mitigations in place.”

Resilience and response manager, health & social care, UK



“The organization that we work for experienced an increase in capital expenditure due to the installation and operational costs of backup systems. When we run on a generator, we need an ongoing supply of diesel to keep the lights on, however we also need to invest in backup systems like UPS (uninterruptable power supply) or even small portable backup power batteries for staff with the hybrid working model in mind.”

Business continuity manager, financial services, South Africa

The frequency that events have occurred and the associated impact levels on respondent organizations

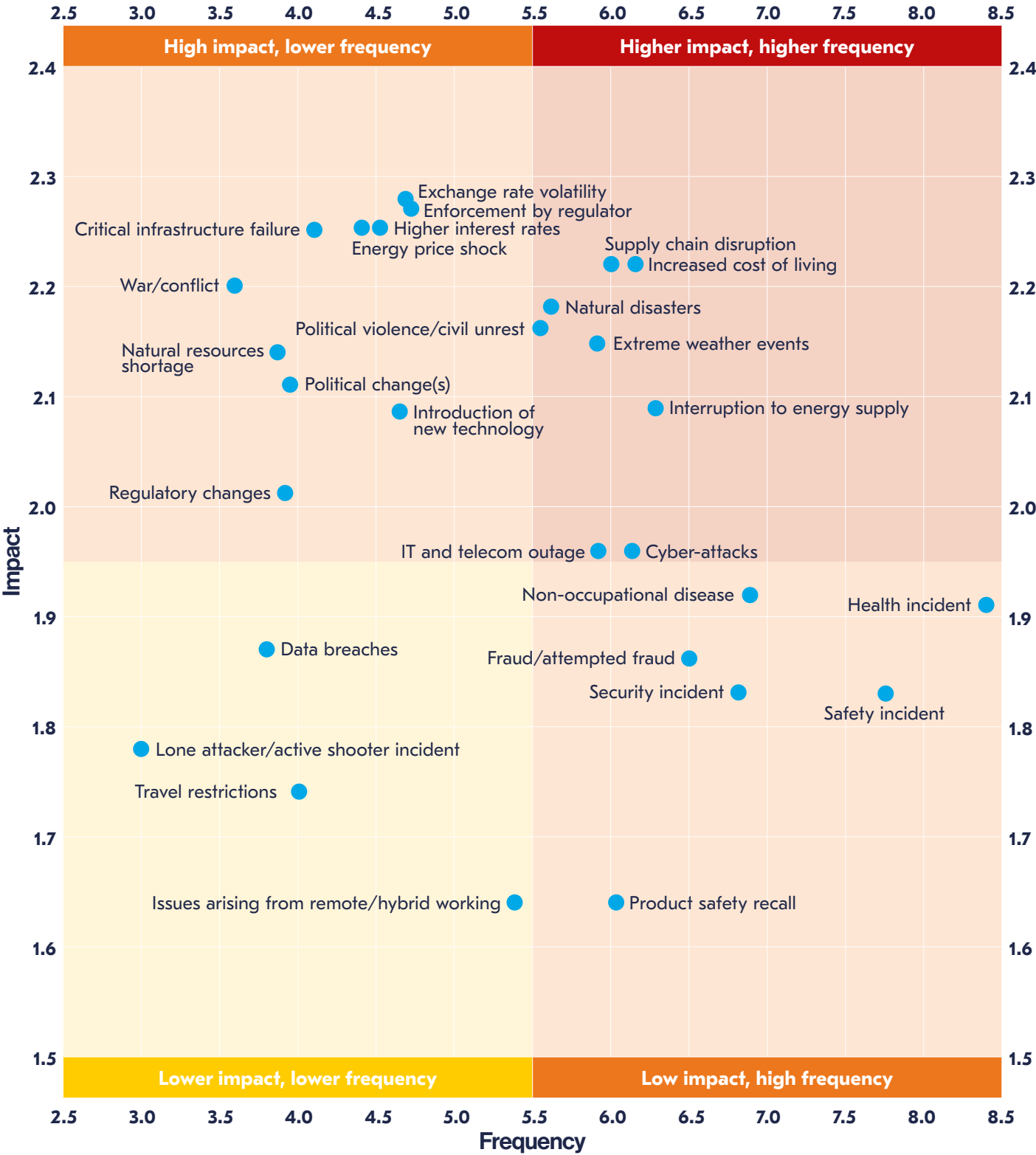


Figure 1. The frequency that events have occurred and the associated impact levels on respondent organizations

Rank	Event	Frequency	Impact	Risk Index
1	Health incident (occupational disease, stress/mental health, sickness absence)	8.43	1.91	16.14
2	Safety incident (personal injury, fatality, reportable incident)	7.75	1.83	14.22
3	Increased cost of living	6.12	2.22	13.56
4	Supply chain disruption	6.00	2.22	13.34
5	Non-occupational disease (e.g. pandemic)	6.93	1.92	13.29
6	Interruption to energy supply	6.26	2.09	13.10
7	Security incident	6.81	1.83	12.47
8	Extreme weather events (e.g. floods, storms, freeze, etc.)	5.90	2.05	12.09
9	Fraud/attempted fraud	6.50	1.86	12.08
10	Cyber-attacks	6.14	1.96	12.06
11	IT and telecom outage	5.92	2.04	12.05
12	Political violence/civil unrest	5.55	2.16	11.96
13	Natural disasters (earthquakes, tsunamis, etc.)	5.59	2.08	11.60
14	Enforcement by regulator	4.72	2.27	10.69
15	Exchange rate volatility	4.71	2.27	10.69
16	Higher interest rates	4.52	2.25	10.18
17	Energy price shock	4.44	2.25	10.01
18	Product safety recall	6.05	1.64	9.91
19	Critical infrastructure failure	4.10	2.25	9.19
20	Introduction of new technology (IoT, AI, Big Data)	4.61	1.96	9.05
21	Issues arising from remote/hybrid working	5.42	1.64	8.88
22	Natural resources shortage	3.91	2.14	8.37
23	Political change(s)	3.95	2.11	8.34
24	War/conflict	3.61	2.20	7.93
25	Regulatory changes	3.90	2.01	7.85
26	Data breaches	3.77	1.87	7.03
27	Travel restrictions	4.04	1.74	7.03
28	Lone attacker/active shooter incident	3.00	1.78	5.34

Table 1. The frequency that events have occurred and the associated impact levels on organizations

Regional discrepancies – and company-to-company discrepancies – are common in the disruption landscape

The disruption landscape for 2023 varies by region, as would be expected. Both Asia and North America report extreme weather events as being the main disruption in 2023.

“Heatwaves have gone through Europe, with the associated bushfires. We are also seeing similar weather events in Hawaii, USA, Australia, and New Zealand. There are a lot more severe and frequent hurricanes, typhoons, and cyclones (depending on where you are geographically) are causing a lot more damage; those one in hundred-year events are becoming more frequent.”

Organizational resilience advisor, public administration, New Zealand

Heatwaves stand as one of the most lethal extreme weather events, claiming thousands of lives annually. In the European heatwave of 2022, 61,672 lost their lives, with 18,010 in Italy alone²⁵. In July 2023, the northern hemisphere once again experienced severe heatwaves, affecting areas such as the south-western United States, Mexico, Southern Europe, and China. On 16 July 2023, temperatures went beyond 50°C (122°F) in locations such as Death Valley in the United States and north-west China. Numerous weather stations in China reported record-breaking temperatures, with Sanbao setting an all-China heat record on the same day (52.2°C). In Europe, Catalunya saw its hottest day on record, while daily minimum temperature records were shattered in various Spanish regions. In the United States, parts of Nevada, Colorado, and New Mexico equalled their all-time high temperature records. Some regions, including parts of Arizona and the Cayman Islands also reached record nighttime temperatures. Phoenix, Arizona, endured its longest period without dropping below 90°F (32.2°C).²⁶

In Africa, interruption to energy supply is the biggest cause of disruption. Africa is a continent which is rich in energy and related resources but, at the same time, is hindered by widespread energy poverty. For example, the South African energy crisis which has triggered load shedding, an ongoing period of widespread national blackouts, began in the later months of 2007 and still continues today. The South African government-owned national power utility, and primary power generator, Eskom, attributes the rolling blackouts to insufficient generation capacity.²⁷

“As a country, we are experiencing a lot of regular power outages because our power utility company is implementing loadshedding. We often depend on the backup generator to operate for some hours when loadshedding is implemented. If the power outages are prolonged, it does put a strain on our backup systems and that’s when we’ve experienced problems; for example, there are times when our generator didn’t kick in and we had network connectivity issues at that time.”

Business continuity manager, financial services, South Africa

Africa’s top three disruptions for organizations in 2023

1



Interruption to energy supply

2



Health incident

3



Exchange rate volatility

Asia’s top three disruptions for organizations in 2023

1



Extreme weather events

2



Political violence/ civil unrest

3



Fraud/attempted fraud

Australasia’s top three disruptions for organizations in 2023

1



Enforcement by regulator

2



Increased cost of living

3



Energy price shock

Europe’s top three disruptions for organizations in 2023

1



Safety incident

2



Health incident

3



Non-occupational disease

North America’s top three disruptions for organizations in 2023

1



Extreme weather events

2



IT and telecom outage

3



Cyber-attack

Respondents elaborated on other risks for their organizations, especially around the introduction of new technology and AI, internal politics, new regulation, geopolitical events, and natural disasters:

“Our company thinks that it will be good to introduce artificial intelligence especially for the production lines, along with robots.”

Risk management and business continuity practitioner, manufacturing, Japan

“AI is a big one, a lot of us are trying to figure out the right ways to use it but also dealing with other uses of AI that could be nefarious in nature.”

Business resilience programme manager, IT & communications, USA

“The “Nankai Trough” is said to have an 80% chance of causing a massive earthquake in the next 30 years. Additionally, there are numerous known and unknown active faults present within the country. Many Japanese companies operate in regions that are likely to be severely affected by them. Our company is also one of them.”

Risk management and business continuity practitioner, manufacturing, Japan



“One of the bigger issues that’s come from industrial action is that it’s becoming harder and harder to have people cover shifts. We have had people cover shifts and they can cover it once, twice, but when you have to say ask them to cover it a fourth time or a fifth time, it’s become a lot more difficult. When the industrial action stops, they will have a lot more work to catch up on. It’s again becoming a lot more difficult for personnel to cover their role.”

Resilience and response manager, health & social care, UK

“There is a lot of legislation coming in. Martyn’s Law legislation²⁸ will potentially be coming through next year; from an implementation perspective this is going to have a huge impact on us. We are currently working through what we think we need to do but this will be a huge legislative change for us and so we are going to have to build our planning arrangements around Martyn’s Law.”

Business continuity manager, public sector, UK

“The organization disputed a new pay offer, negotiations stalled and staff went on strike. Our crisis management team was deployed, which is the second line of defence in our business continuity structure.”

Corporate planning manager, public administration, UK

“The Russian invasion of Ukraine in February 2022 had an impact on our organization. We had offices in Russia and many employees based there. As a US company, we must abide by sanctions and cannot operate in a country with sanctions in place, so we had to shut down our business in Russia very quickly. There is still a ripple effect from this as we had contracts with customers and so we had to find ways to be compliant, whilst carefully monitoring the situation with our trade compliance and legal teams as we had to be careful about what we did to stay within regulations. There was also the people impact: some employees we were able to physically relocate to other countries to continue working, but others we were not able to keep.”

Business resilience programme manager, IT & communications, USA

“If there is a change in the political administration, many of our capital and big program of works that have already been agreed upon by current administration may be impacted upon by the incoming administration.”

Business continuity manager, public sector, UK

“The Liberty Protection Safeguards legislation has been delayed again by central government. This is something else that will have a huge impact on us from a business point of view because implementing that legislation is going to be very resource heavy for us to ensure we meet the standards that they are expecting us to meet.”

Business continuity manager, public sector, UK

“We are also mindful that next year, we will most likely have a general election and so we do not know what that will mean for us as an organization and if that changes the dynamic with the organization going forward. There are lots of unknowns at the moment.”

Corporate planning manager, public administration, UK

Most of the disruptions highlighted in the Horizon Scan survey and those mentioned by practitioners in interviews have the ability to interact and heighten the effect of one another, making the preparation for multiple simultaneous events a key element of organizations’ business continuity and resilience plans. Last year’s report evidenced the fact that organizations are increasingly concerned about facing multiple, simultaneous, events. Participants in regions susceptible to extreme weather were the most concerned about this. In these instances, business continuity and resilience professionals not only have to ensure the uninterrupted flow of operations but also navigate through multiple events happening concurrently, such as simultaneous wildfires and flooding (as often experienced in Australia). Many have gleaned valuable lessons from these experiences and are consequently better equipped to confront future challenges. By ensuring such incidences are accounted for in planning and incorporated into training and exercising programmes, organizations will be prepared to know what to do when multiple incidents occur at the same time.

“From a resilience perspective, COVID-19 has really shone a light on some of our practices. Each time we have a disruptive event, we realize that perhaps we are not as prepared as we thought we were, or our systems were not as resilient or robust.”

Principal advisor
organizational resilience,
public administration,
New Zealand



A simultaneous surge in mental health crises, escalating living costs for employees, rising costs for organizations, weather-related events, cyber-attacks, and geopolitical shifts are all concurrently affecting organizations. This convergence of challenges renders organizations more vulnerable, forcing them to enhance and adapt their resilience strategies to a new ‘polycrisis’ setting. The Global Risks Report 2023 from the World Economic Forum introduces the concept of ‘polycrisis’, to illustrate how current and prospective risks can intertwine, creating a network of interconnected global risks with cumulative consequences that surpass the sum of their individual impacts.²⁹

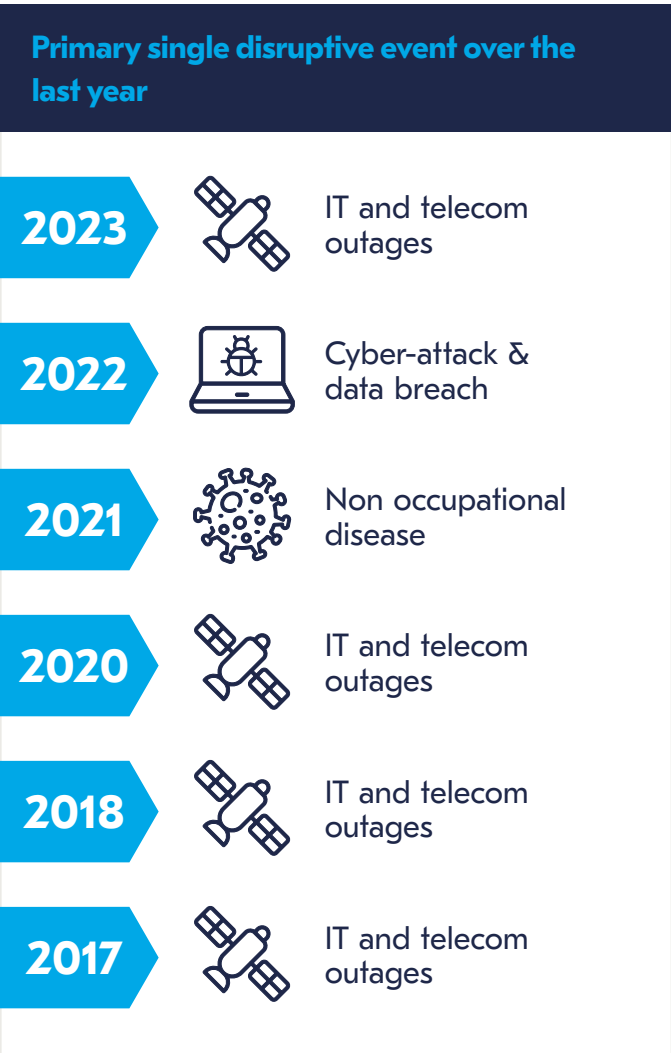
COVID-19 related disruptions have lessened throughout 2023, but some of the primary challenges organizations are facing still relate to the human factor: safety incidents and occupational health incidents. Indeed, in the period 2020-2023, key disruptions identified by organizations were health incident/ occupational disease and infectious disease (pandemic).

Top cumulative disruptions to organizations 2012-2023		
2023		Health incident (occupational disease, stress/mental health, increased sickness absence)
2022		Non occupational disease (pandemic)
2021		Non occupational disease (pandemic)
2020		Health incident* (occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)
2019		IT and telecom outages
2018		Cyber-attack
2017		Cyber-attack
2016		Cyber-attack
2015		Cyber-attack
2014		IT and telecom outages
2013		IT and telecom outages

* The survey for the 2020 BCI Horizon Scan report closed on 31 December 2019 — a day before the news of COVID-19 was broken on mainstream media.

Top single disruption to organizations in 2023

In addition to labelling the frequency and impact of all incidents over the past year, respondents were asked to indicate which event produced the biggest disruption to their organization. Historically, IT and telecom outages have dominated the top answer here and technology has been the top disruptor for organizations over the last seven years. In line with this, the greatest singular disruption organizations have experienced in the past twelve months is IT and telecom outages, with 20.4% of organizations saying such an incident was the cause of their main disruption in the year. These figures represent a considerable increase of 38% since the last edition of this report.



The number of organizations labelling IT and telecom outages as their largest single disruption is in line with data produced by the Uptime Institute which analyses global patterns in IT and telecom outages, as well as costs incurred.³⁰ In 2022, 25% of respondents reported that their most recent incident had cost the business more than US\$1m in both direct and indirect costs, compared to only 15% of respondents in 2021. The report blames the rising costs on inflation, fines, SLA breaches, the cost of labour, call outs, and replacement parts, but also notes that the greatest cost is because of the growing dependency of economic activity on digital services and data centres. New operational resilience regulations concerning third-party providers to the financial sector (e.g. the Bank of England/Prudential Investment Authority (PRA)/Financial Conduct Authority (FCA) operational resilience regulations in the UK and the Digital Operational Resilience Act (DORA) in the EU) will hopefully help to bring some of the risks associated with third-party IT supplier relationships down.

The shift in working patterns toward remote and hybrid models has elevated the significance of addressing IT and telecom outages for organizations. With a substantial portion of the workforce operating from dispersed locations, a reliable and robust digital infrastructure has become essential.

The enduring transition to remote work needs robust IT networks, but making this shift permanently poses its own set of challenges. Furthermore, many organizations are growing progressively dependent on a single platform to handle their IT and communication needs. While relying on a comprehensive solution provider like Microsoft may appear convenient, it does introduce operational risks. A global Microsoft Azure outage last June illustrates this, as it left users unable to access a multitude of services for an extended period of time³¹.

The second most singularly disruptive event for organizations in the past year is critical infrastructure failure (10.9%), which was in twelfth place in 2022. In the 2023 UK National Risk Register, the government anticipated that the majority of severe incidents affecting critical national infrastructure would encompass encryption, data breaches, destruction of data that CNIs depend on, or the complete disruption of operational systems. Nonetheless, the probability of such an attack over the next two years has been assessed as a four out of five, still categorising it as 'highly unlikely' with a 'moderate' impact. Even though the likelihood is deemed minimal, it remains crucial for organizations to ready themselves for a worst-case scenario.³²

The third single most disruptive event for organizations in 2023 were extreme weather events. The BCI Extreme Weather & Climate Change Report 2023³³ showed that almost 80% of surveyed organizations had suffered impacts from climate related events, to differing degrees. The effects of heatwaves have already been discussed in the previous section, but floods and heavy rainfall events lead the list at 58.8%, followed by extreme heatwaves (43.9%), hurricanes and tornadoes (35.2%), and wildfires (34.7%). These hazards have all recently made global headlines, affecting extensive regions. While these prominent threats are characterised by rapid and immediate weather-related impacts, the report also underscores the dangers of gradually unfolding incidents, especially water scarcity, which is anticipated to become an increasingly significant concern in the years ahead. Climate-related occurrences are directly affecting business operations and, consequently, financial outcomes. The BCI Extreme Weather and Climate Change Report 2023 labelled supply chain interruptions (47.3%), workforce absences (45.9%), short-term premises unavailability (44.5%), power outage (41.8%), and revenue loss (27.4%) as the primary consequences of severe weather disruption.

“Last December, we had a massive amount of rain in Lisbon. The water took over, it was a big thing and we had to close the sites to keep people safe at home.”

Business continuity coordinator,
support services, Portugal

“In Portugal, we had extreme heat in the summer, but heavy rain is also becoming more regular during winter, so we can have a very dry winter and then rain for three days in a row. These extremities in weather are becoming more common and repetitive.”

Business continuity coordinator,
support services, Portugal

“Most of our inpatient buildings are very old, one building is 250 years old. Aircon is not everywhere, so it is very much a case of ‘we must try and deal with it’ in terms of extreme heat as best we can, which can become very difficult.”

Resilience and response manager,
health & social care, UK

“We have had a significant flooding event between January and February for the last four years. We are well versed on how we manage this but obviously it has implications for us. In some respects, it is easy for us from a work perspective because predominantly we have all remained working from home, but sometimes people have to uproot and relocate because they know their village or area is going to be flooded.”

Business continuity manager,
public sector, UK

“We look after patients with mental health conditions, and there are people who have certain triggers that can set them off, and extreme temperatures are triggers that can cause our patients to have acute episodes. That’s a real concern for us. We are doing what we can, such as having portable aircon units put in in certain places. However, when those heat weather alerts are sent out it can cause panic.”

Resilience and response manager,
health & social care, UK

According to the World Meteorological Organization (WMO), extreme weather, climate, and water-related events resulted in 11,778 documented disasters, causing just over 2 million fatalities and economic losses totalling US\$4.3 trillion between 1970 and 2021.³⁴ While economic losses have surged in recent years, enhanced early warning systems and coordinated disaster management have significantly reduced the human casualty count. Developing nations have borne the brunt of the global death toll, with over 90% of reported deaths occurring in these regions.

“We had an extreme weather event that triggered a state of national emergency in the country. A large swath of the North Island was impacted by severe weather; this kicked us into action. We ensured that our people in those affected regions were looked after. We responded and provided essential policy advice in support of the recovery effort. It is not just support and policy, we need a more holistic approach to how we manage incidents.”

Organizational resilience advisor,
public administration, New Zealand

The fourth most disruptive event selected by organizations is cyber-attacks. While organizations are making substantial investments in technology and implementing fresh controls to bolster their resilience against attacks, the rate of attacks is steadily rising and the attack methods are growing increasingly intricate and challenging to identify.³⁵ Cyber-attacks have increased, causing financial losses in the past twelve months. Cybersecurity Ventures states that IT analysts struggled to predict the rapid escalation of cybercrime, the ransomware crisis, the shift of malware from traditional computers to smartphones and mobile devices, the widespread deployment of inadequately secured Internet of Things (IoT) devices, the proliferation of freelance hackers, and the increasing complexity of cyber-attacks targeting organizations, governments, educational institutions, and individuals worldwide³⁶. According to Embroker, cybercrime will cost companies worldwide an estimated \$10.5 trillion annually by 2025, up from \$3 trillion in 2015.³⁷

Respondents to the Horizon Scan survey highlighted the need for more integration between technical teams, such as cyber security, business continuity, and risk management, in order to increase organizational resilience. However, while cyber-attacks might only be the fourth most disruptive event, it is typically a subject area that dominates the concerns of senior management due to the potential financial loss and reputational impact of such as attack. Indeed, when looking at practitioners' concerns for the next twelve months in section 4 of the report, cyber-attack comes to the top of the list.

▶ **"Last year, we suffered a cyber-attack on this software which provides a lot of services to NHS trusts. Our electronic patient record system is run by this impacted software and so we lost access to all our patient records. We had the business continuity system that we purchased but we only had access to limited amounts of data."**

Resilience and response manager, health & social care, UK

“We had a major operational event earlier this year; our internal domain name server was not operating effectively and became overloaded. It was an operational issue, but it played out much like an internal DDoS; and therefore impacted our operations and customer’s ability to access their systems.”

Resilience lead, financial services, Australia

► **“Like all businesses, we have had an eye watering number of hacking attempts on our firewalls. In the first six months of this year, we blocked 400 million unauthorized attempts to access our ICT infrastructure from the Internet.”**

Business continuity manager, public sector, UK

Which of the following events produced the biggest disruption to your organization in the past 12 months?

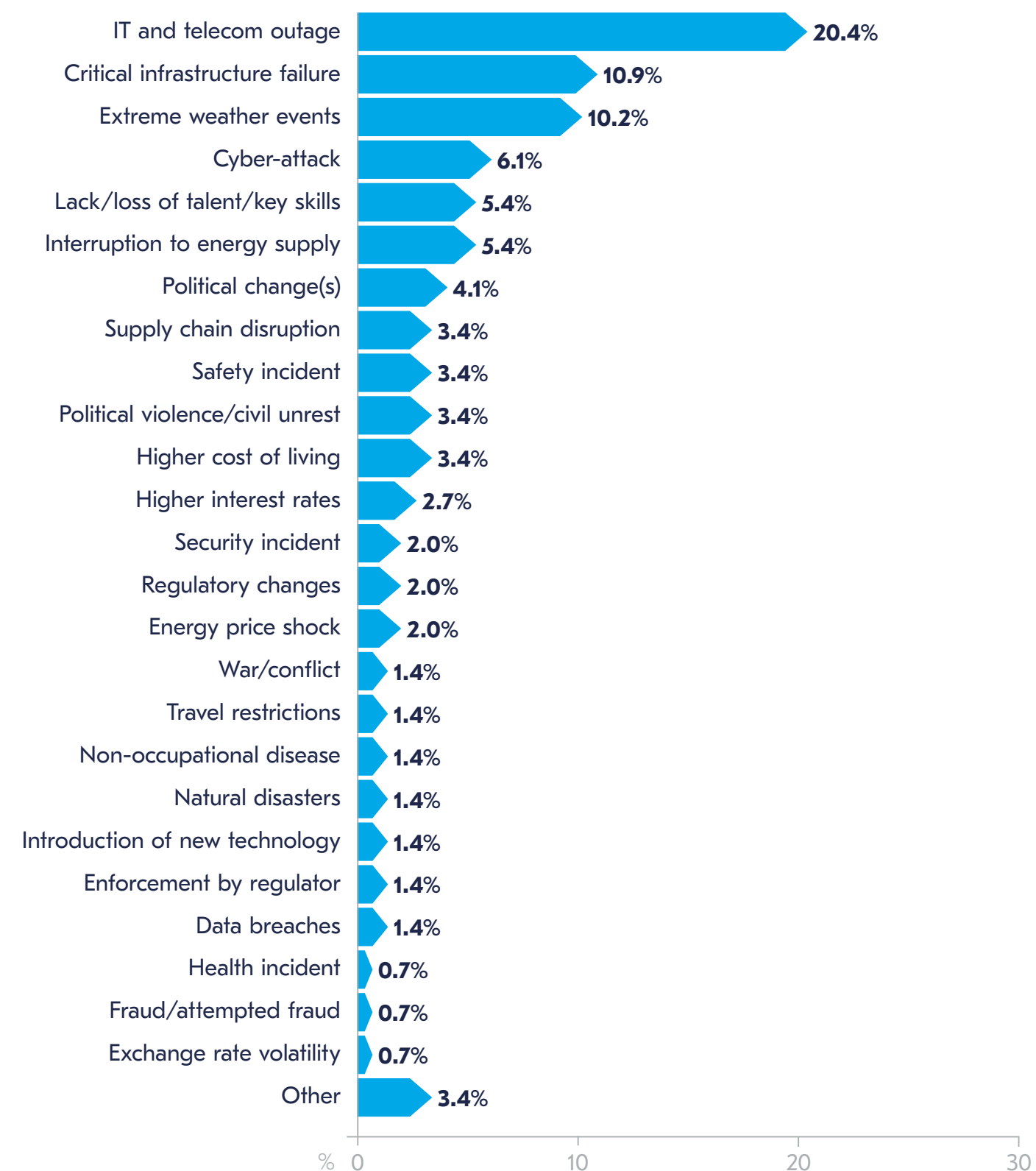


Figure 2. Which of the following events produced the biggest disruption to your organization in the past 12 months?

The lack/loss of talent/key skills and interruption of energy supply share fifth spot on the table this year, both equally affecting 5.4% of organizations.

Lack or loss of talent was the fifth biggest threat for organizations in 2022, with a risk score of 17.3. Rapid technological advancements and evolving industry requirements have created a gap between the skills that organizations need and the skills available in the labour market. Some may lack the specific skills required for some jobs, whereas other positions are being lost due to automation of roles with technology. Organizations are competing on a global scale to secure the best specialists, making it challenging to attract and retain top talent.

The problem of retaining IT staff was highlighted in the 2022 Horizon Scan Report³⁸. In that year, respondents raised concerns about the resilience of IT and telecommunications systems due to the shortage of available hardware, but also emphasised the challenge of finding IT and technical staff. This shortage is now further exacerbated by shifts in employee preferences. The pandemic has sparked changes in employees' work preferences, with many showing a heightened interest in remote work and seeking roles that do not demand extensive commutes. Indeed, those organizations that require employees to be on site may find themselves with a limited pool of candidates given that remote and hybrid patterns are now becoming commonplace, even for previously onsite operational positions such as IT.

With increasing inflationary pressures, organizations are having to offer the best talent the required salaries, while also ensuring that attractive benefits are offered. The public sector and healthcare are two of the areas where it is increasingly difficult to attract and retain talent due to salaries tending to be lower than those of the private sector.

"We are seeing a loss of staff, meaning we are losing skills and knowledge from the organization. With the current climate across recruitment markets this makes it difficult to recruit and retain new staff which is concerning."

Corporate planning manager,
public administration, UK

"In the public sector we do not see the huge salary increases that can be acquired in the private sector. This hinders our ability to attract new talent because we can not match what the private sector offers"

Corporate planning manager,
public administration, UK

"There are shortages in some parts of the workforce and we have had a problem with recruitment and retention."

Business continuity manager, public sector, UK

"The demographic population in Portugal is decreasing, our active population is expected to become residual in the next 25 years. As a result, Portugal is currently opening borders for an influx of immigration, but few of those people are qualified and will not stay for the next 25 years because we are not competitive enough. My company's services are very specific in terms of skills, it's going to be a constant challenge to find the right skills in the market".

Business continuity coordinator,
support services, Portugal

"This country is not particularly attractive for working (pay level vs cost of life), so the local companies don't have enough money, even the international companies have to be very accurate in bringing someone from the USA, England, or Germany to work here. My fear is that many specific areas of knowledge get transferred to specific countries where the economic conditions are better."

Business continuity coordinator,
support services, Portugal

Consequences of disruptions



Consequences of disruptions

- **Loss of productivity is the greatest consequence of disruption:** this demonstrates the increased importance of attending to the human side of resilience and the need to focus on staff wellbeing programmes to support employees and build stronger organizations.
- **Complaints received and reputation damage were reported as the second and fourth greatest consequences of disruption:** customers are unforgiving of service that is not up to standard and organizations are also more aware that the external perception of their organization's image requires careful management, particularly when hit with a crisis such as a cyber-attack.
- **Three in ten organizations have reported loss of revenue as a consequence of disruptions.**



The main consequence of disruption this year is the loss of productivity, with two-thirds of respondents noting this as an impact. This has risen from second place in 2022 to first position in 2023, with an increase of 1.6 percentage points. A McKinsey report estimates that, for a medium sized company, the estimated cost of employee disengagement and attrition is between US\$228m and US\$555m per annum³⁹. Also, according to Gallup’s State of the Global Workplace: 2023 Report⁴⁰, the global economy bears a significant burden of \$8.8 trillion in lost productivity due to employees who are disengaged with their work. This amount accounts for a substantial 9% of the worldwide Gross Domestic Product (GDP).

However, the human factor is not the only factor when talking about loss of productivity for organizations. According to the World Bank⁴¹, since 2000 there have been three significant global economic slowdowns, with the most recent and severe one being sparked by the COVID-19 pandemic. Simultaneously, many nations have struggled with major adverse occurrences, including natural disasters, conflicts, and financial crises; all of which can result in enduring harm to productivity.

Loss of productivity is closely linked to the third most popular consequence of incidents in this year’s survey: that of the negative impact on staff morale/wellbeing/mental health with over a third of respondents reporting this as a consequence of disruption. The impact on the mental health of organization’s employees has already been discussed in this report and, to corroborate this, the WHO estimated some 12 billion working days are lost globally every year to depression and anxiety, at a cost of US\$ 1 trillion per year in lost productivity.⁴² The importance of personal resilience is a topic which frequents contemporary conference programmes and its importance cannot be ignored when considering an organization’s resilience footprint.

Customer complaints received and reputational damage take the second and fourth spot in the table at 37.0% and 33.6% respectively. The 2021 BCI Horizon Scan Report saw a decrease in customer complaints received with the consensus being that consumers were more forgiving of poor service during the pandemic. However, this rose again in 2022 as ‘pandemic fatigue’ crept in, and the same consumers were not as forgiving of continual supply chain disruptions, poor service, and higher prices⁴³.

It is positive to see that, this year, respondents note that customer complaints have decreased by two percentage points, although this is somewhat muted by the criterion rising from sixth place to second place this year. With businesses under more pressure in a challenging economic environment, the importance of customer satisfaction cannot be emphasised enough. Research by Gartner⁴⁴ reveals that 81% of marketers consider customer satisfaction to be the primary battleground in their industry, while findings by PwC show that 59% of customers will no longer shop with a company after enduring multiple negative experiences.⁴⁵ There is clearly much work to be done in this area as, according to a Harvard Business Review article, customer satisfaction is at its lowest point in the past two decades.⁴⁶

Another important consequence that arose from disruptions within respondent’s organizations is the issue of reputational damage. Over one in three organizations reported damaged reputation as an effect of disruptions. Reputational damage has seen an increase of 11.5 percentage points since the last edition of this report and climbed from eleventh position in 2022 to fourth position in 2023. Previous Horizon Scan reports have discussed how customers tend to be more forgiving of events which are beyond the control of the organization (such as severe weather events or earthquakes) and less forgiving of those where they deem the organization to be somewhat or fully at fault (such as a cyber-attack or service outage).

“Australia, like many nations, has had a substantial increase of interest rates over the past 12 to 14 months, which combined with broader inflation has significantly impacting the cost of living. Our profit announcement this year was a record profit and so of course there is a direct correlation with many observers asking ‘Why are you making such a large profit when the people are feeling such a cost-of-living increase and impact?’ It impacts reputation.”

Resilience lead,
financial services, Australia



To minimise the risk of reputational damage, media messaging should be carefully controlled. Training staff to respond to negative press is something which many organizations are now employing to avoid the wrong messages emerging which could, in the extreme worst case, result in failure of the organization.⁴⁷ The responsibility for training and exercising of crisis scenarios often falls to the business continuity manager and/or crisis manager. Currently practitioners are reporting that training budgets are more open⁴⁸.

The high number of organizations reporting having suffered reputational damage underscores the value of establishing a business continuity management system, which includes the creation of a crisis management committee or an incident response framework that incorporates crisis communications as a fundamental component. The manner in which management reacts and communicates during an incident or crisis has a substantial influence on reputation. Hence, it is vital for senior management to be prepared to deliver consistent and well-structured communications, avoiding contradictory or inaccurate statements. The BCI Crisis Management Report 2023 further highlighted the importance of communications and PR in a crisis, in order to avoid reputational damage. Respondents concluded that the role of communications and PR in a crisis is the top factor for consideration in crisis response. 80% of respondents agreed or strongly agreed that external communications and PR are integrated into their crisis response, showing how important a coordinated PR response is in an era of instant news generation and social media.⁴⁹

What impacts or consequences arose from the disruptions experienced in the last 12 months?

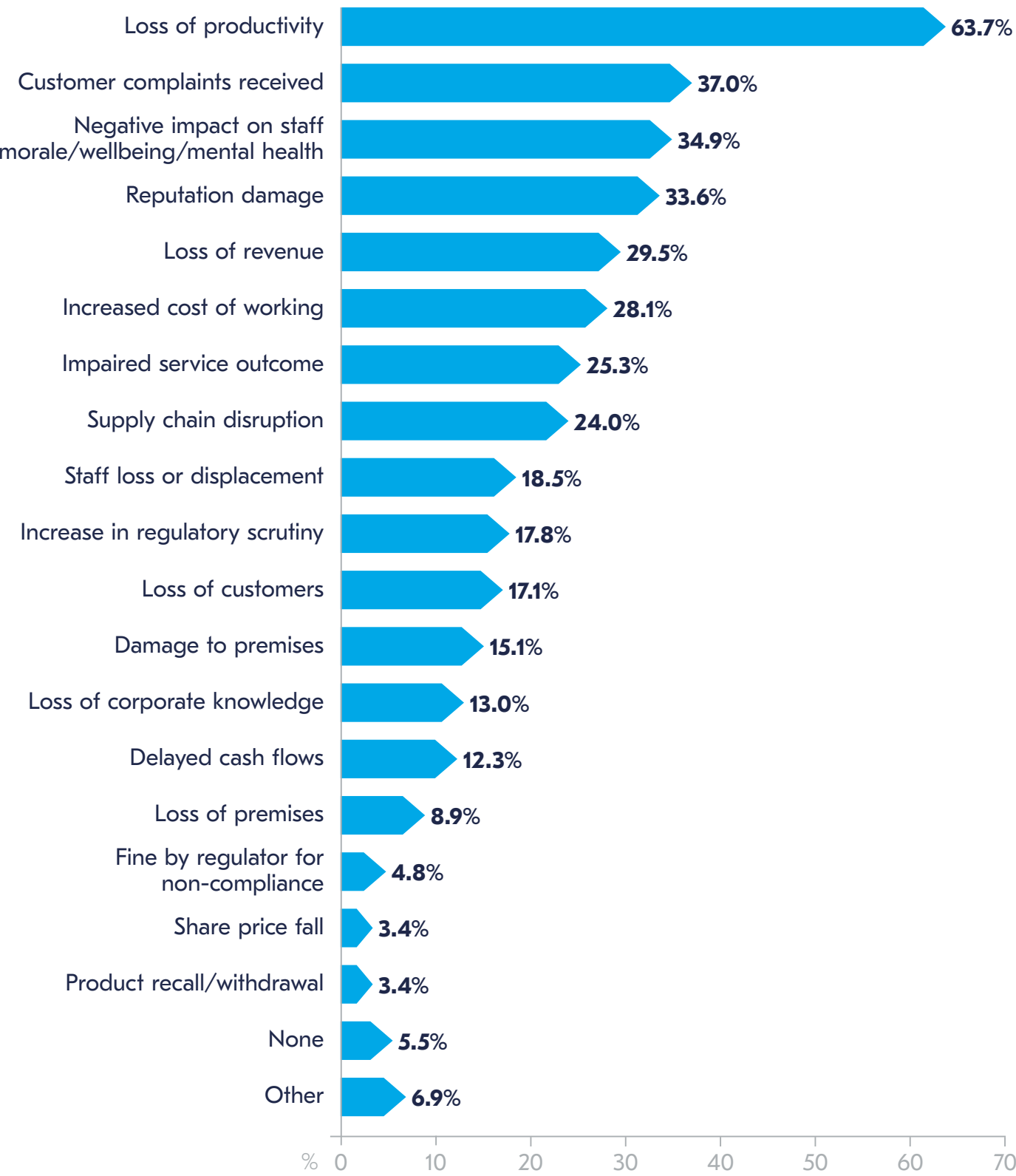


Figure 3. What impacts or consequences arose from the disruptions experienced in the last 12 months?

Risk and threat assessment: the next twelve months



Risk and threat assessment: the next twelve months

- **Cyber-attacks are top of organizations' concerns for 2024:** organizations are being tested with more sophisticated phishing attacks and ransomware incidents. While the number of cyber-attacks has slightly diminished in the first half of 2023, the cost for organizations to counteract these incidents has increased considerably.
- **In 2023, extreme weather events have surged from the sixth to the second position among organizations' top threats consideration for 2024:** organizations are most concerned about the chronic and worsening characteristics of these events; as well as the potential consequences.
- **Interruption to utility supply has jumped to the forefront of organizations' concerns:** this is primarily a consequence of the effects of global conflicts upon the global energy supply market, as well as interruptions caused by extreme weather.

Historically, this report has demonstrated that, although the risk landscape is evolving, practitioners' concerns for the short-term future persistently focus on the biggest threats encountered in the previous year. However, there has been a shift from this in this year's report. Although the main disruptions in 2023 were related to workforce health, respondents highlight the main threats for 2024, as being cyber-attacks, extreme weather events, IT and telecom outages, increased cost of living, and interruption to energy supply.

Non-occupational disease slides from second place to 21st in 2024, with cyber-attacks back on top

For the first time since 2021, non-occupational disease has been unseated from the top three risks on the table with cyber-attacks now the greatest concern for organizations over the upcoming twelve months. With a risk score of 6.9, it moves from second place in 2022 to 21st in 2023.

In the BCI Cyber Resilience Report 2023⁵⁰, 74% of respondents have experienced an increase in cyber-attacks in the past 12 months. It was also reported that phishing and ransomware, while less frequent, were the most common and disruptive threats, causing the most significant impact for organizations. Other sources confirm that within the world of cyber security, phishing remains the most common cyber-attack, with approximately 3.4 billion phishing-related spam emails daily⁵¹. The FBI’s Internet Crime Report for 2022 revealed total losses due to phishing attacks exceeded \$10.3 billion in 2022. Furthermore, phishing attacks account for 90% of data breaches, largely because phishers frequently adopt the identity of a trustworthy and reputable entity in their electronic communications and know how to penetrate the first line of defence in an organization: that of the user. In this respect, an interviewee described a phishing attempt on his organization and how the close-knit nature of the organization helped it to evade the attack:

“The phishing attacks coming our way are quite sophisticated. My colleague received an email, purportedly from me, asking them to update my banking details in our payroll system. On turning around, I saw a well prepared and deliberate email that, to the untrained, appeared genuine. I was saved from financial harm by the size of our organization (there is four of us) and my colleague asking me why I sent an email rather than speak with her. If we were a larger company, it is likely that we would have been hit by that one. What it triggered was precautionary phone calls to our clients and suppliers to let them know of the issue and that any change of banking details will be by way of a phone call first and then confirming email.”

Senior associate, professional services, Australia

While some attack vectors are increasing, others are decreasing — or changing in their nature. In 2022, SonicWalls⁵² recorded 493.3 million ransomware attempts, marking a 21% reduction compared to the previous year. This decline followed a 62% increase in 2020 and a 105% surge in 2021. Nevertheless, ransomware attacks continued to make up to 12% of critical infrastructure breaches in 2022. However, while the number of attacks and ransom amounts diminished from 2021 to 2022, there is an increase in the average number of records impacted, signifying a more substantial impact with each attack. The primary vectors of ransomware incidents include phishing, the misuse of Remote Desktop Protocol (RDP), and software vulnerabilities.



“One of our factories has been affected by ransomware which has resulted in our operation being stopped for a period of time.”

Risk management and business continuity practitioner, manufacturing, Japan

Some organizations are still not aware of how to approach the issue of ransomware, failing to have a clear path in place on how to deal with this issue, how to engage with government bodies, and what policies to follow. In other organizations, there is sometimes a lack of communication between IT and business continuity/resilience which can mean that the wider impacts of an attack on an organization are not properly accounted for in business continuity plans. Indeed, in the recent BCI Crisis Management Report 2023⁵³, improved inter-departmental communication and community resilience were highlighted as key areas for improvement in crisis management by respondents. One interviewee spoke about incorrect expectations from another organization’s senior management in relation to the involvement of government when dealing with cyber threats:

“We facilitated a cyber threat exercise for a critical infrastructure client and one of their peer organizations. When debriefing the exercise, the CEO of the peer organization outlined an expectation that a phone call to the Australian Cybersecurity Centre would have the ACSC take over the response. The activity, especially the debrief, provided an opportunity to drill down into and then clarify assumptions. At the conclusion of the activity, the CEO better understood their internal controls, available external support and, like every risk, the CEO remains accountable for the organization’s reputation.”

Senior associate, professional services, Australia

Other issues relating to cyber are the relationship with third-party providers and the risk of downtime and data breaches.

"We had a few outages, one of them was with a software supplier for our business processes but it was on their side. They needed to do an update, a straightforward procedure, but for some reason it went wrong and so we had a few hours outage. We are a global shared services centre and so if you fail to pay an invoice on time, this can lead to complaints, reputational damage, and financial damage from having to pay compensation."

Business continuity coordinator, support services, Portugal

"There have been many data breaches where a third-party organization, which may or may not have a direct relationship with us, had a breach of their customer database. Even though it wasn't our data, it wasn't our issue, or wasn't stolen from us, their customers are also our customers, therefore stolen banking and contact details are relevant to us. As a result, practically every time there's a major data breach there is a very good chance that we're impacted directly, particularly given our relative size in the Australian market."

Resilience lead, financial services, Australia

"We have identified our risks well and historically we try to mitigate the impacts. In the case of our software suppliers, they failed two to three times over the years and this is becoming more frequent, so we need to invest in more support."

Business continuity coordinator, support services, Portugal

State-sponsored cyber-attacks continue to be an issue and, with increasing global conflicts, the likelihood of them increasing further is high. Over the last year, cyber-attacks have had an impact on 120 countries, driven by government-backed espionage and an increase in influence operations (IO), according to Microsoft⁵⁴. Notably, as many as 50% of attacks have been directed at NATO member nations and over 40% have targeted government or private-sector entities responsible for constructing and upkeeping critical infrastructure. While many high-profile attacks in the past year have centred on causing destruction or financial gains through ransomware, the data reveals a significant shift in the primary motive toward information theft, covert surveillance of communications, and the manipulation of information that people consume.

Extreme weather events are also a top threat for the next twelve months for organizations, with a risk score of 6.26, an increase of 1.76 points compared to 2022, and jumping from sixth position in 2022 to second in 2023. According to the BCI Extreme Weather & Climate Change Report 2023⁵⁵, threats related to climate-related events are increasing and, whether organizations believe that man-made climate change is at the root of the developments or not, it would be difficult for organizations to consider removing it from their risk radars.

"I think it is a reality that we are going to see more concurrent events in the future, certainly in the case of extreme weather; the duration between events is going to be shorter and so when we are recovering from one incident the next one will be upon you. Climate change is the massive elephant in the room that is being overlooked. We are failing to meet any targets in terms of emissions and we are starting to see the impact of that."

Organisational resilience advisor, public administration, New Zealand

"In New Zealand, we have broken a lot of heat and rainfall records this year. We have witnessed flooding that we have not seen in 30 to 50 years and that is only going to get worse. All the predictions indicate that sea level will rise which, for some of our Pacific neighbours, is going to trigger mass migration and they will start to have salination of their fresh water. In the equatorial regions, we are going to start to see food insecurity, which is going to trigger security issues; and it's really going to amplify some of those underlying issues."

Organisational resilience advisor, public administration, New Zealand

Climate-related events pose significant concern for organizations in 2024

Floods and heatwaves rank as the primary climate-related hazards faced by organizations, with some having to adapt to climate events previously unseen in their regions, such as wildfires. Additionally, practitioners expressed concern about other variations and consequences of these occurrences, including snowstorms and droughts.

"In 2017 a town in northern NSW was affected by a so-called 1-in-100-year flood. In between October 2019 to February 2020 there were bushfires from Melbourne in the South, along the eastern seaboard and up to north of Brisbane; that is nearly 3,500 kilometers of fire. The fires were extinguished by the onset of La Niña conditions. That northern NSW town experienced another 1-in-100-year flood again in 2021. As rebuilding commenced in 2022, they were flooded again by 1-in-100-year floods in March and July. Weather patterns are becoming more extreme and greater preventative and preparatory activities are needed."

Senior associate, professional services, Australia

"The Australian state governments are now starting to work out that you should not build on floodplains. Floodplains are great for agriculture because the floodwaters replenish the fields. Currently, there are 200,000 residents living on floodplains, if you get the 1 in 250-year flood, your planning must include how to evacuate that number of people and then assist them recover. To do this you must also recognize that while they were permitted to build in that area, the residents are faced with unaffordable insurance premiums."

Senior associate, professional services, Australia

The ripple effects following extreme weather-related events (such as operational disruptions, infrastructure damage, and employee displacement) represent one of the most complex outcomes of climate-related disturbances. Consequently, climate-related incidents remain a top concern for professionals and senior executives alike. In this context, one emerging consequence to monitor in the near future is the issue of water scarcity, which can have operational, social, and political implications.

“My main concern is that Portugal is already extremely dry and lacking in water, this has been happening for the last 30-35 years and it is only going to get worse. There are also reports that the north Africa climate has been gradually more present in the south of Spain and in Portugal since the mid 80’s (less and less rain). Maybe, during my lifetime, the south of Iberian peninsula will be a very arid area where most likely there will not be water reserves to make possible the current economic activities being developed there.”

Business continuity coordinator, support services, Portugal

IT and telecom outages are in third place, with organizations concerned about external factors bring down networks

IT and telecom outages are the third highest risk identified by respondents over the next twelve months, with a risk index of 5.93, an increase of one point since 2022 and jumping from fifth place in 2022. According to a survey by Opengear, 91% of organizations experience network downtime at least once a quarter⁵⁶. Furthermore, the economic repercussions of such outages are escalating, a trend expected to persist with the increasing reliance on digital services. Over two-thirds of all outages incur costs exceeding \$100,000, reinforcing the business rationale for heightened investment in resilience measures and staff training⁵⁷. Furthermore, the disruptions are not only limited to internal operations: professional third-party digital infrastructure providers, including cloud, colocation, telecommunications, and hosting companies, are responsible for an expanding share of these outages, underscoring their growing role and significance. Indeed, the increased dependence on third-party providers is something that needs increased attention from a business continuity perspective. An example of this is the Microsoft cloud outage on 25 January this year that affected several of its products, including Teams and Outlook. The disruption left users globally unable to access multiple Microsoft 365 services for over four hours.

“In the office, we had resilient backup systems for our services, however now we have moved people out of the office to work from home; we are now dependent on the services where they live.”

Senior associate, professional services, Australia

The increasing cost of living, inflationary prices, and energy supply disruptions rank highly on list of threats for 2024

As discussed, when analysing incidents which caused the most disruption to organizations in 2023, the increased cost of living is still one of the main threats perceived by practitioners for 2024, with a risk score of 5.5. As mentioned earlier, this issue affects organizations as well as their employees, amplifying the overall impact on an organization.

Interruption to energy supply concludes the top five risks that organizations are concerned about in the next twelve months, with a risk rating of 5.49. This issue ranked in sixteenth place in 2022 and, tellingly, the survey for that report was closed just as the conflict in Ukraine started. The conflict triggered a notable upsurge in energy costs and considerable instability within energy markets. Worries about potential energy supply interruptions, combined with increasingly stringent sanctions imposed on the Russian energy industry, have led to substantial price fluctuations. Interruption to energy supply cannot purely be related to global conflict, however. In nations such as South Africa, for example, supply cannot keep up with demand. These, coupled with the fact that the conflicts affecting the global energy supply market are far from over, ensure it is high on the risk table for 2024.

“Interruption to energy supply is a big one for us because, again, most of our buildings don’t have backup.”

Resilience and response manager, health & social care, UK

“Australia is looking at its carbon reduction targets and has shut down coal-fired power plants as they approach end of life. Concurrently, State and local governments are considering banning gas appliances to further reduce emissions from fossil fuels. The implementation of renewable energy generation is, however, lagging. We have an increasing population and demand about to come into our very hot summers and our energy security is reduced. Until the renewable energy generation targets can be met there will be significant reliance on things like diesel-power generators to take up the load.”

Senior associate, professional services, Australia

However, to get a full picture of the risk landscape for 2024, the whole table needs to be reviewed for context. This provides an overview of the same phenomenon that has been noted in previous Horizon Scan reports — that of practitioner concerns diverting to those which have been top of mind over recent years. Indeed, despite pandemic being at the top of national risk registers, the issue has fallen to 21st position in terms of top practitioner concerns for 2024 showing that, at least for some practitioners, ‘out of sight’ does mean ‘out of mind’. This emphasises the importance of ensuring that organizations are prepared for the unexpected. Organizations should consider adopting a planning approach where an organization prepares for the symptom of an incident, rather than a cause. This means that, even if an organization faces a natural resources shortage (the event that takes last spot on the table), it should have a plan in place to mitigate the symptoms of it (such as ensuring manufacturing facilities can switch to a different input material, products can be developed using a different raw material, and power can be generated from an alternative energy source).

The likelihood and impact levels for incidents occurring in respondent organizations in the next twelve months

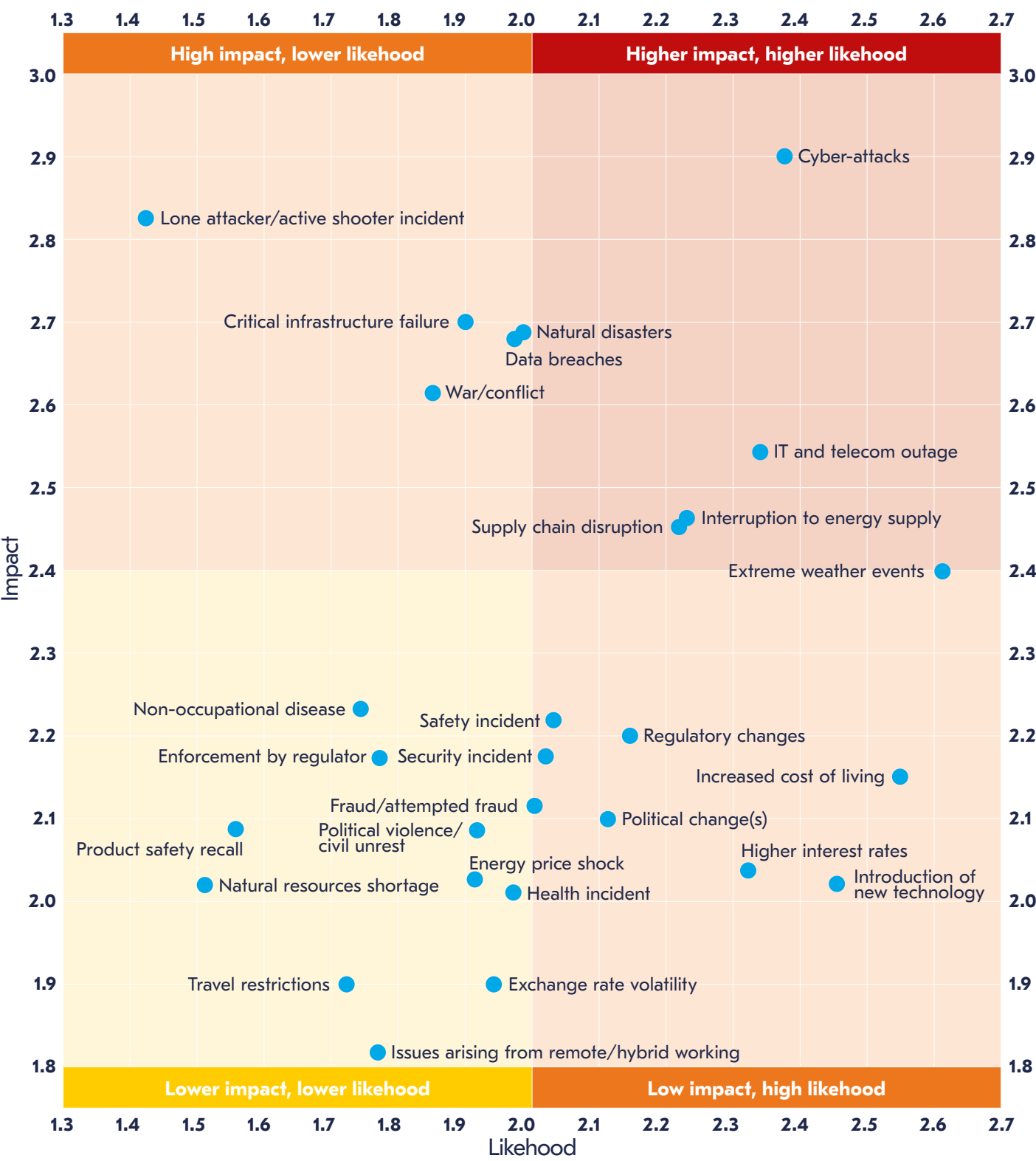


Figure 4. The likelihood and impact levels for incidents occurring in respondent organizations in the next twelve months

Rank	Event	Likelihood	Impact	Risk Index
1	Cyber-attacks	2.38	2.90	6.92
2	Extreme weather events (e.g. floods, storms, freeze, etc.)	2.61	2.40	6.26
3	IT and telecom outage	2.34	2.54	5.93
4	Increased cost of living	2.57	2.15	5.50
5	Interruption to energy supply	2.23	2.46	5.49
6	Supply chain disruption	2.21	2.45	5.42
7	Natural disasters (earthquakes, tsunamis, etc.)	1.99	2.69	5.34
8	Data breaches	1.98	2.68	5.31
9	Critical infrastructure failure	1.90	2.70	5.14
10	Introduction of new technology (IoT, AI, Big data)	2.45	2.02	4.93
11	Higher interest rates	2.32	2.04	4.74
12	Regulatory changes	2.14	2.20	4.72
13	War/conflict	1.75	2.61	4.57
14	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	2.03	2.22	4.52
15	Political change(s)	2.11	2.10	4.43
16	Security incident	2.02	2.18	4.40
17	Fraud/attempted fraud	2.05	2.11	4.32
18	Political violence/civil unrest	1.93	2.09	4.04
19	Lone attacker/active shooter incident	1.42	2.82	4.00
20	Health incident (NOT transmissible disease such as COVID but occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	2.01	1.97	3.97
21	Non-occupational disease (e.g. pandemic)	1.74	2.23	3.87
22	Energy price shock	1.91	2.02	3.86
23	Enforcement by regulator	1.77	2.17	3.85
24	Exchange rate volatility	1.94	1.90	3.68
25	Travel restrictions	1.72	1.90	3.28
26	Product safety recall	1.55	2.09	3.23
27	Issues arising from remote/hybrid working (the new working environment)	1.78	1.81	3.22
28	Natural resources shortage	1.51	2.02	3.05

Table 2. The likelihood and impact levels for incidents occurring in respondent organizations in the next twelve months

Benchmarking long-term threat analysis



Benchmarking long-term threat analysis

- **Organizations are increasingly centralising their risk scanning processes, learning from past experiences:** the response to COVID-19 was muddled in some organizations, with different areas of the business using different approaches to risk scanning. As a result, many organizations are now looking to centralise their risk management processes.
- **The use of the outputs from long-term trend analysis has increased to a historic high of 77.5%:** this is a positive step and shows that practitioners are not only considering the 'now', but also looking at how they can ensure that their organizations are resilient to future risks, the known unknowns, and, potentially, the unknown unknowns.
- **There is a low uptake of technology to help with risk scanning activities:** most work continues to be done manually, via public sources and through peer collaboration. Furthermore, most organizations do not have a formalised electronic system to manage disruptive incidents.

One of the main takeaways from the pandemic experience is that organizations need to be prepared for the unexpected. Consequently, practitioners must maintain a comprehensive perspective of the risk landscape, exploiting the free resources that are available and, where budget allows, considering investing in products that can help build a comprehensive risk landscape for the organizations.

Broadly, organizations are seeking to better understand the landscape: with more than three-quarters conducting long-term trend analysis. However, although this number is marginally higher than in 2022, it is still lower than in 2021, when COVID-19 was rife.

While this could be seen as a stagnation in practices, the way in which organizations are carrying out their activities is improving. 57.9% of organizations are now carrying out horizon scanning activities from a centralised perspective, an increase of 11 percentage points compared to 2022 and also higher than in 2021.

For many organizations, the catalyst for this shift has been the COVID-19 pandemic, which spurred efforts to acquire more data for risk planning, centralise risk management processes, and invest in data mining methods to extract valuable insights. This approach eliminates siloes and ensures a consistent, uniform view of risks and threats across the organization. It also helps to eliminate work duplication and improve efficiency: different departments using different approaches to risk scanning means different conclusions may be drawn, as well as time wasted due to different people potentially performing the same activities. A coherent, management-driven, approach can help to resolve such issues.

"We have a centralised risk team who work with SME across the organization to scan internal and external sources, looking for emerging risks to explore and report. The team will break that down into two axis, the expected timeframe to potentially occur and the degree of potential impact, so the quadrants then provide a view on the required prioritisation and timeline for action to respond to that emerging risk and provides an indication of the relative urgency."

Resilience lead, financial services, Australia

While nearly three-quarters of organizations have adopted the development of long-term trend analysis, there remains significant room for improvement, particularly considering that one in five organizations (20.6%) do not engage in this type of analysis at all.

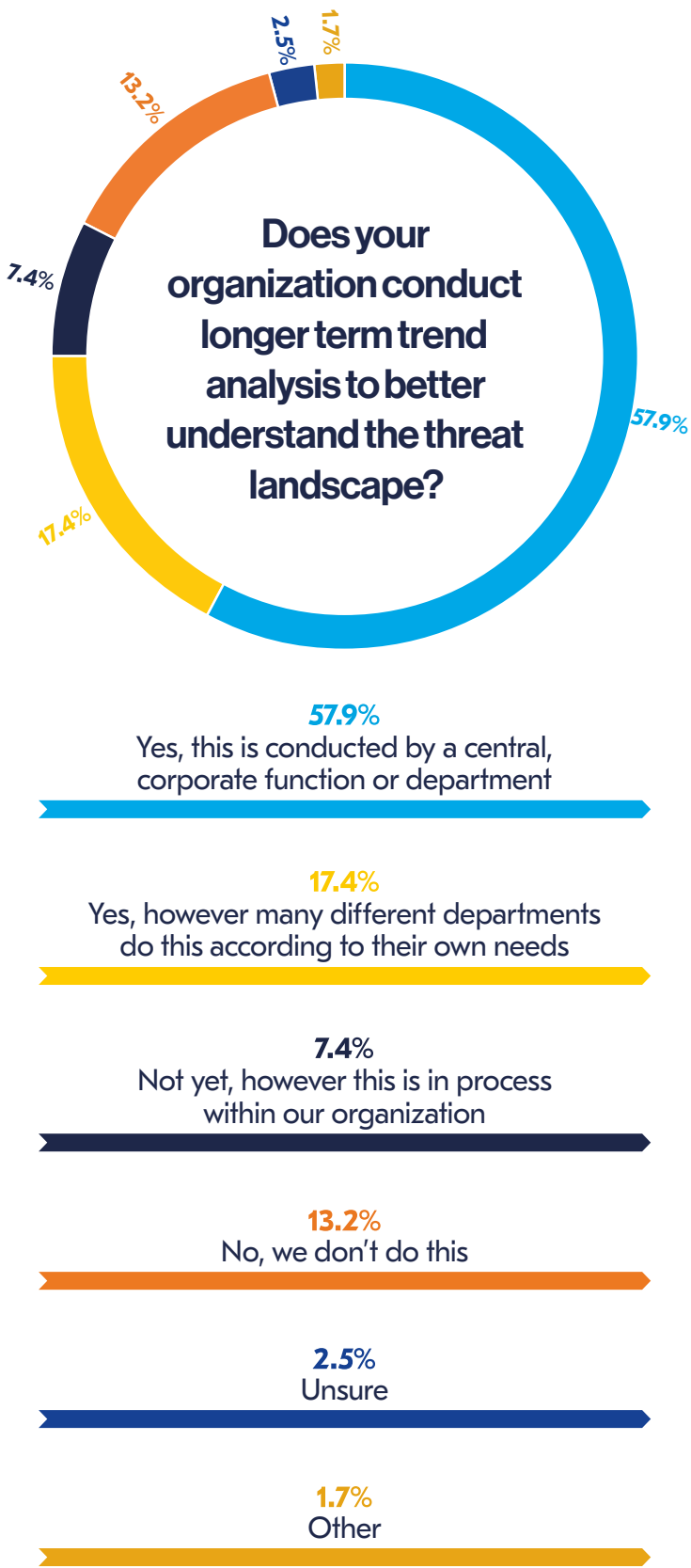


Figure 5. Does your organization conduct longer term trend analysis to better understand the threat landscape?

One in five resilience professionals do not have access to trend analyses to develop their programmes

While organizations may still encounter challenges in efficiently gathering and analysing data, practitioners are increasingly using the results of trend analyses to incorporate into their own programmes. By using the insights generated, practitioners can ensure that the planning process is closely linked to the specific risks of their own organization. This will ensure that plans are better linked to management's longer-term objectives, ultimately leading to better buy-in. It is therefore encouraging to see that the usage of the outputs of long trend analysis has increased to a historic high of 77.5%. Furthermore, nearly a third of practitioners (28.3%) actively participate in shaping the analysis itself, a positive trend and a 3.4 percentage point increase since 2022.

However, nearly one in five (18.3%) practitioners lack access to the outcomes of trend analyses, demonstrating that a barrier exists between risk and business continuity and pointing towards siloed working practices. Encouragingly, however, this figure has declined from 24.0% in 2021.

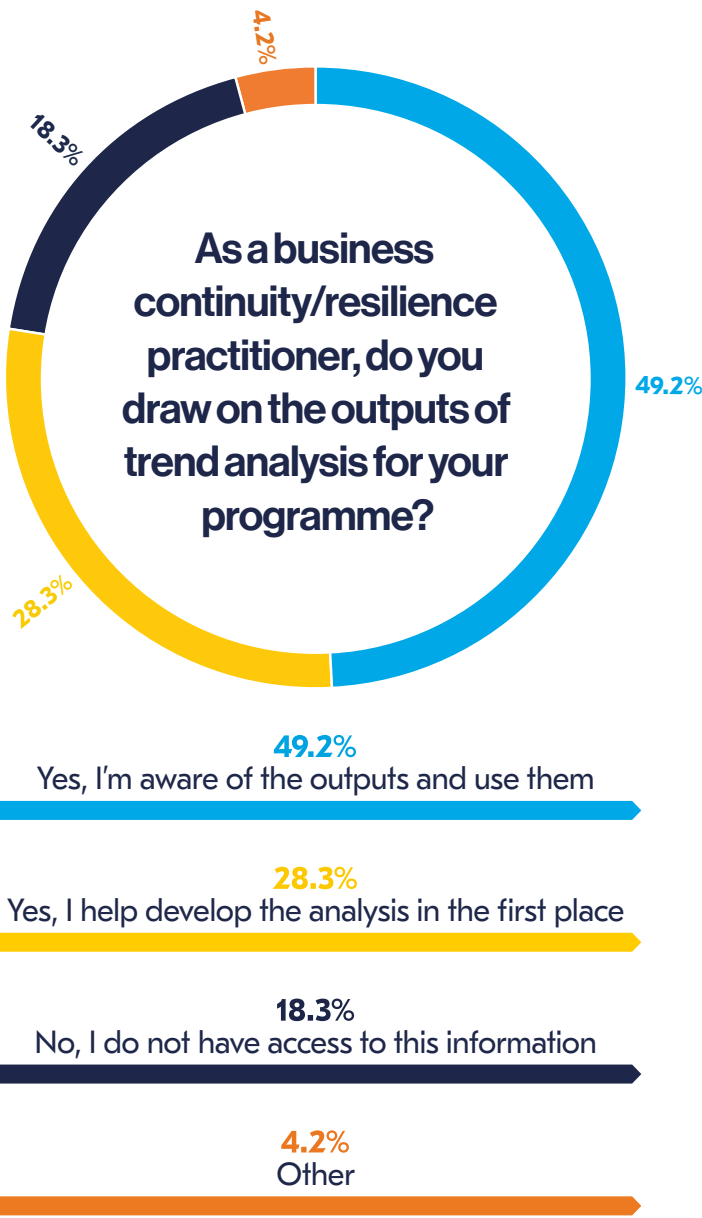


Figure 6. As a business continuity/resilience practitioner, do you draw on the outputs of trend analysis for your programme?



The usage of outputs of long trend analysis within organizations has reached an all-time high

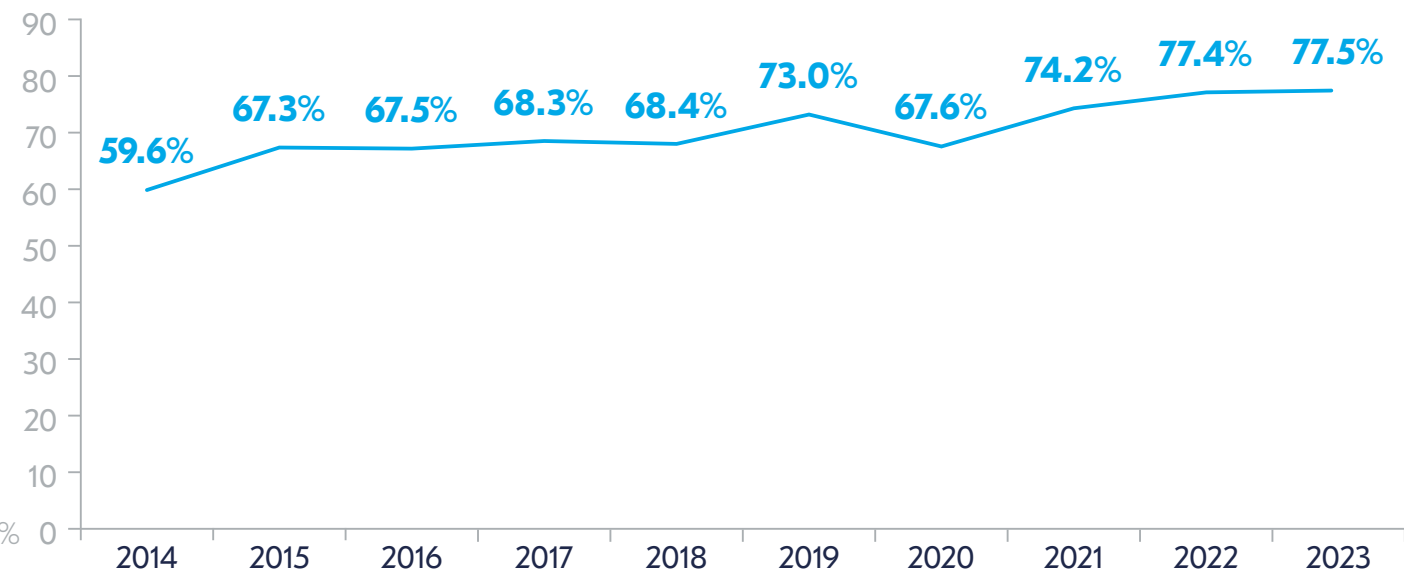


Figure 7. The usage of outputs of long trend analysis within organizations has reached an all-time high

The absence of direct access to risk scanning activity does not necessarily mean that practitioners are not conducting their own independent analyses. There are various freely available resources, such as the BCI Horizon Scan, national risk registers, and reports like the OECD Cross Country Perspectives on global risk, which are valuable tools for risk mapping. Additionally, external forums, conferences, and open information exchange with peers, customers, and suppliers serve as valuable sources of information.

Risk and threat assessments are only as good as the actions taken from it

In this regard, we asked respondents which tools they use to conduct long trend analysis/horizon scanning within their settings. This showed a discernible preference for traditional methods over automated systems. This is best depicted in the top answer to this question: for the second consecutive year, the primary tool for gathering intelligence remains internal risk and threat assessments, with nearly nine in ten (87.9%) respondents using this approach. This longstanding method remains at the root of risk planning as well as business continuity activities but should not be taken in isolation as a method to ensure an organization is protected against risk. Indeed, a risk assessment is only as good as the actions taken from it, so regular reviews of the risk assessment need to be made and relevant actions should be taken.

The use of external reports and industry insights takes second place, with 77.6% of participants now incorporating these resources into their analyses. Participation in industry events/conferences and collaborating with peers have taken the third and fourth positions, with 61.2% and 60.3% respectively.



Industry research plays a pivotal role in assisting professionals in various aspects, offering a broader perspective and enabling them to benchmark their practices against industry peers. Meanwhile, access to insights from other organizations, which can be gained by peer-to-peer discussion groups, serves as a highly effective means to assess an organization’s risk posture and make necessary adjustments.

Social media monitoring, in third place this year, has seen an increase of 38 percentage points in usage this year, from 39.6% in 2022 to 77.6% in the current edition. While social media has to be used with care due to the potential of unverifiable information or misinformation, it can act as an early indicator of potential issues, as well as a collaboration platform with industry peers. Some organizations use sources to effectively monitor social media content, others have searches set-up on various topics, while others might tap into the feed of official information sources.

Some of the newer solutions are situated towards the bottom of the list due to their relative market infancy, but usage is rising for software-based solutions, automated solutions, and those which are more specialised in their application. This includes automated systems for cyber security (20.7%), risk assessment software (13.8%), forecasting tools (10.3%), and simulation technology (6.9%).

Which tools do you use to conduct trend analysis/horizon scanning of the risks/threats to your organization?

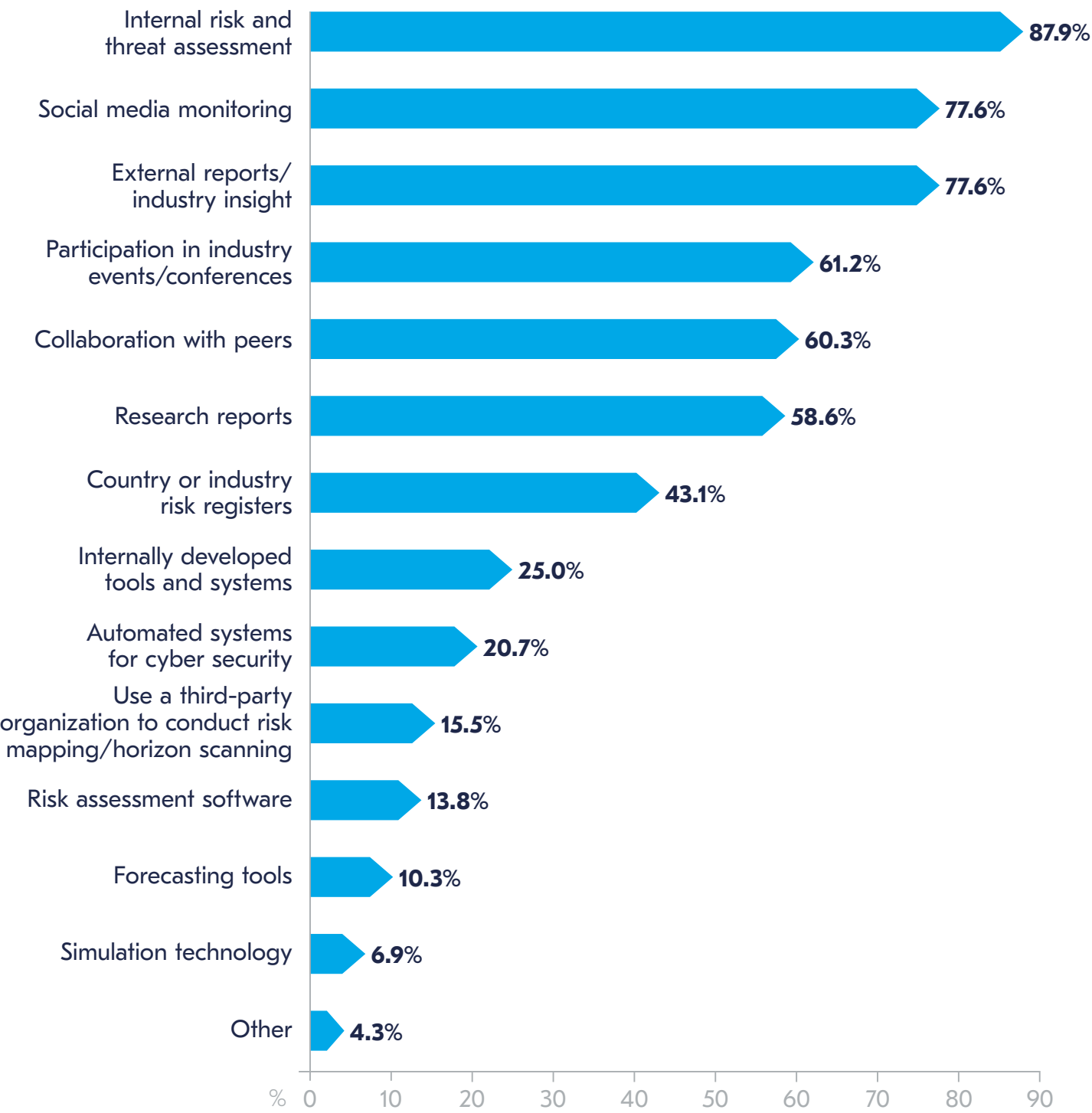


Figure 8. Which tools do you use to conduct trend analysis/horizon scanning of the risks/threats to your organization?

“Internally we organize ourselves using a lot of BCI information and a bunch of other sources. Our risk assessments are done locally. We do not have an official, deployed tool, where everyone can register problems for us to then analyse.”

Business continuity coordinator, support services, Portugal

“We look at thematic emerging issues whenever we do our risk reviews. We also look across operational areas, across the corporate capital program, project risk areas, and look at what those issues are. We work closely with our emergency planning team as they are part of local resilience forums as well. We just generally do constant analysis of anything that we know is coming on the horizon, which is why we’ve always contributed to this report. We have always found it really useful.”

Business continuity manager, public sector, UK

“We are conducting a [risk analysis] at the moment, but I wouldn’t say it’s long term; perhaps the focus will be for the next 12 months or so, but it’s done internally with limited resources. It does not give us that broader scope of us having a well-researched or scientifically proven analysis where we can confidently say this is something that we can use as a guideline going forward.”

Business continuity manager, financial services, South Africa

A growing number of organizations are using specialist software to manage their disruptions

Surveyed organizations were also asked about the usage of software within disruptive events. Given that the answers from the previous section implied a low level of technology uptake, it is not surprising that 43.3% of organizations do not have a formalised electronic system to manage disruptive events. A further 35.8% of organizations use enterprise software to manage disruptions. However, a quarter of respondents use a dedicated incident management software, a further 17.5% incident use an integrated incident manager and business continuity software, while 10% use in-house developed software. These are both fairly positive outcomes given the lack of dedicated software for horizon scanning.

Are you currently using software to manage disruptions in your organization?

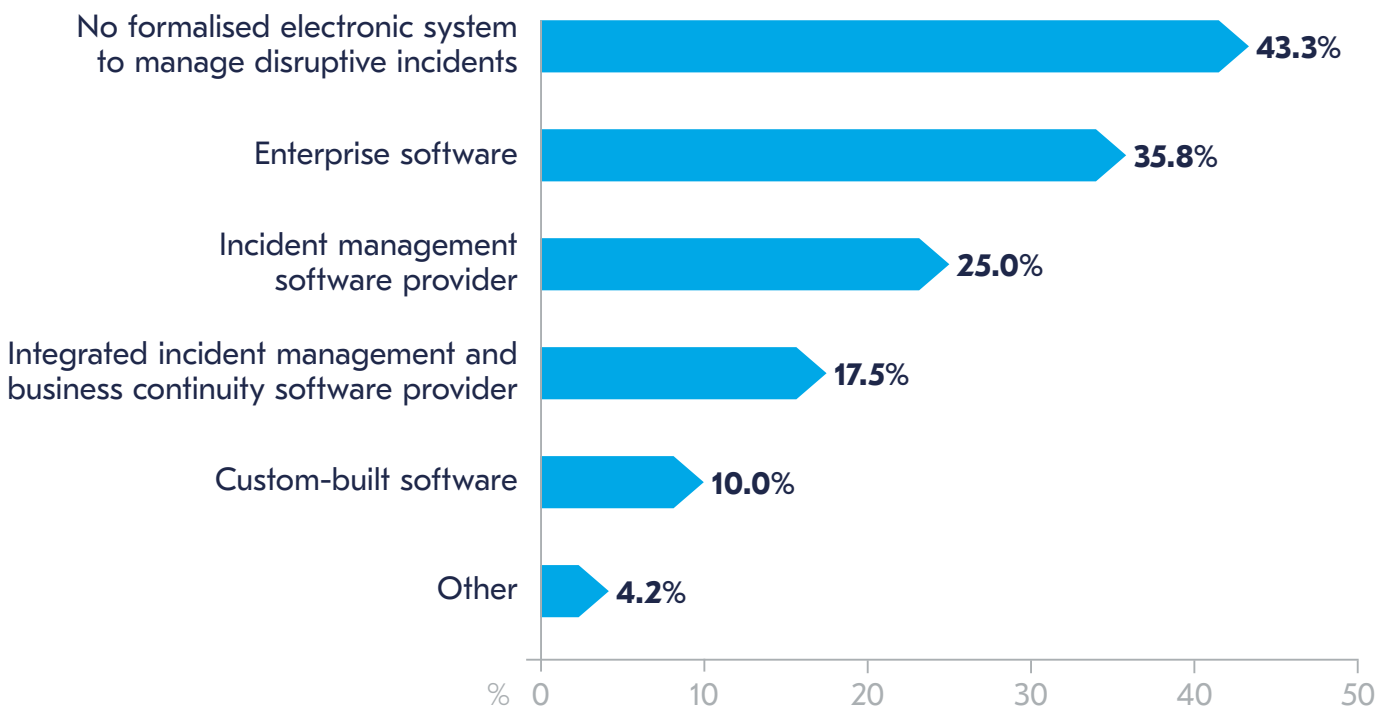


Figure 9. Are you currently using software to manage disruptions in your organization?

“We are a small organization. In my opinion, there isn’t really the need for any type of automation or systems that would hugely benefit the type of incidents that we deal with and the way in which we need to operate.”

Organisational resilience advisor, public administration, New Zealand

“You can bring in a system, but if someone’s not there to operate and maintain it, it can quickly become a dodo.”

Organisational resilience advisor, public administration, New Zealand

Benchmarking business continuity



Benchmarking business continuity

- **ISO 22301 remains the gold standard for benchmarking business continuity practices in almost nine out of ten organizations:** although certification levels fell during COVID, the number of organizations being certified to ISO 22301 is recovering, with numbers marginally increased on 2022 data.
- **The use of ISO 22301 as a framework (without having certified to it) has increased to the highest level ever recorded:** organizations are increasingly having to demonstrate that they align themselves with a recognised programme for supplier procurement and due diligence processes.
- **Organizations report that there is significant value in certification especially when having to demonstrate the effectiveness of their BCM programme to external stakeholders:** this topic becomes especially relevant as global legislation is increasing regarding third-party providers/third-party risk management.
- **Organizations that are not certified report reasons such as not being a business requirement yet, and lack of budget as key elements of this decision.**

While many professionals are now seeing the scope of business continuity augment in their organizations in a move towards resilience, the predominant benchmark for business continuity and resilience programmes continues to be ISO 22301. 85.8% of professionals report that they have not shifted away from this standard in favour of any other resilience standard in the last two years. An interviewee explained how being ISO certified pushed the organization to continuously improve its practices:

“Our company is ISO 22301 certified. When you have a certification, you have an audit which keeps you on your toes for regular improvements. Even if I am not directly responsible there is still a bunch of things that I need to do for that.”

Business continuity coordinator, support services, Portugal



Figure 10. Have you moved away from using ISO 22301 towards another resilience standard over the past two years?

The number of organizations using ISO 22301 as a framework reaches an all-time high

While some interviewees noted a diminishing relevance of ISO 22301 within their own organizations, there is a noteworthy increase in the number of organizations adopting the standard as a foundational framework. In 2021, 52.7% of respondents used ISO 22301 as a framework, rising to 63.6% in 2022. The proportion rose marginally more to 63.9% this year. It is worth mentioning that majority of these organizations do not possess formal certification, with 5.5% actively pursuing certification. Other interviews discussed how they had a good awareness and appreciation of ISO 22301 but used frameworks such as the BCI’s Good Practice Guidelines to build their programmes.

“Depending on what our clients want to achieve in their resilience journey, we will generally start with the GPG and ISO 22301. We assist them mature their thinking and planning by aligning their practices with other 223 series ISO standards. The key is to help the client find what works for their organization, is reasonably practicable and becomes sustainable.”

Senior associate, professional services, Australia

“We have always been interested in ISO 22301 but have never aimed at being certified or driven by it. We use it as a checkpoint. In fact, we have gained a lot more benefit out of the BCI Good Practice Guidelines and used that much more directly in terms of how we think about building our framework.”

Resilience lead, financial services, Australia

“For our organization, certification is not really a requirement, but we do use ISO 22301 as a framework, and we do implement the standard as well. We are also trying to gravitate towards the resilience approach where we now think more strategically and implement more resilient ways of working. It’s something we are considering, but in terms of certification, it’s not something that we’re really focused on or really want to achieve.”

Business continuity manager, financial services, South Africa

Around 7.4% of organizations that do not currently use ISO 22301 as a framework expressed their intentions to transition towards it in 2024. Despite the decline in certification rates during the COVID-19 pandemic, organizations are slowly starting to increase their certification numbers. In 2023, a slightly higher number of organizations were certified to ISO 22301 than in 2022. It is important to highlight that a substantial proportion of organizations remain committed to the standard. In fact, currently 15.7% are either certified or in the process of obtaining certification, compared to 15.1% in the previous year.

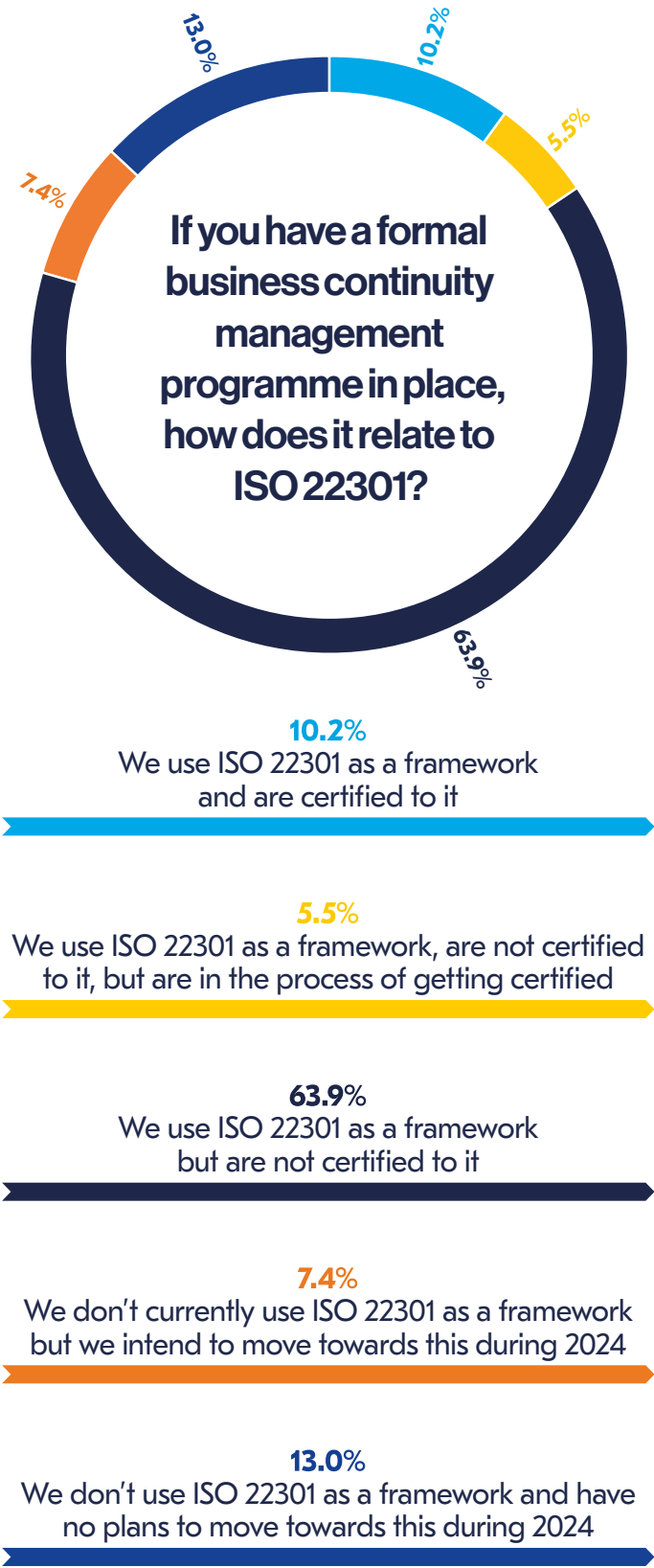


Figure 11. If you have a formal business continuity management programme in place, how does it relate to ISO 22301?

Since 2015, there has been a consistent increase of organizations that use ISO 22301 as a framework to improve their business continuity practices. Showcasing the same point, there has also been a decline in the number of organizations that have no plans to move towards ISO 22301 as a framework. This shows the value of using a recognised standard to showcase the resilience of an organization, which can be used as a competitive advantage when negotiating supplier contracts as well as winning new customers.

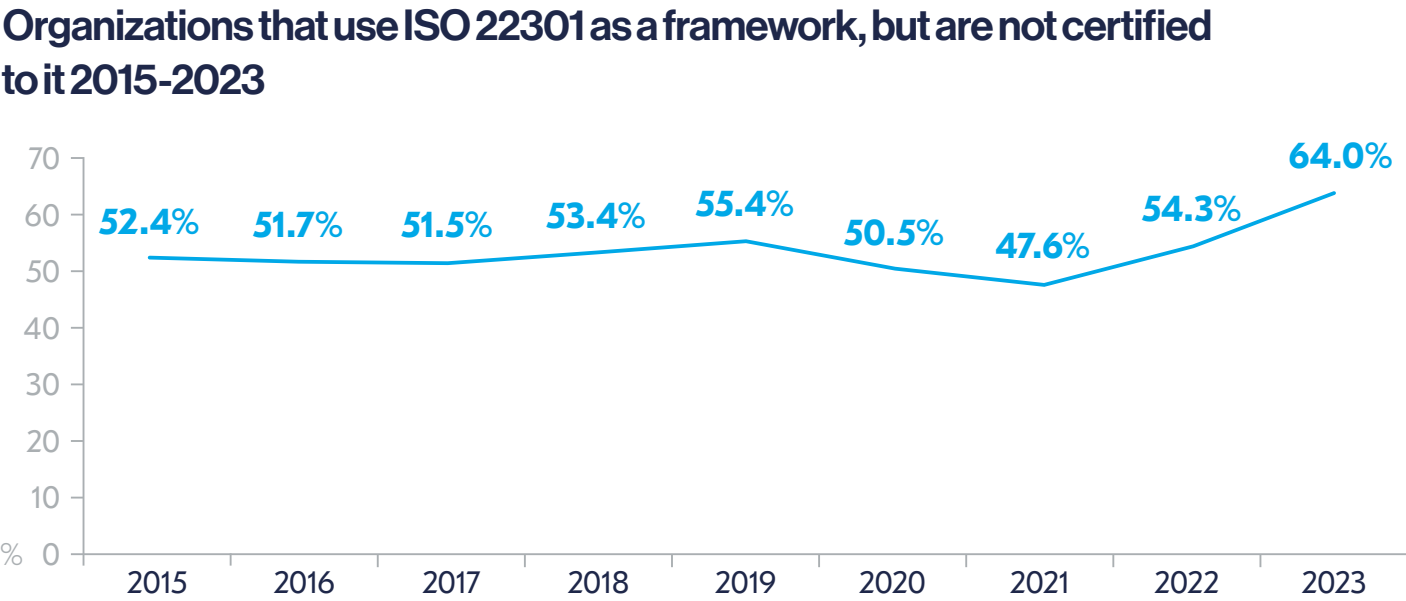


Figure 12. Organizations that use ISO 22301 as a framework, but are not certified to it 2015-2023

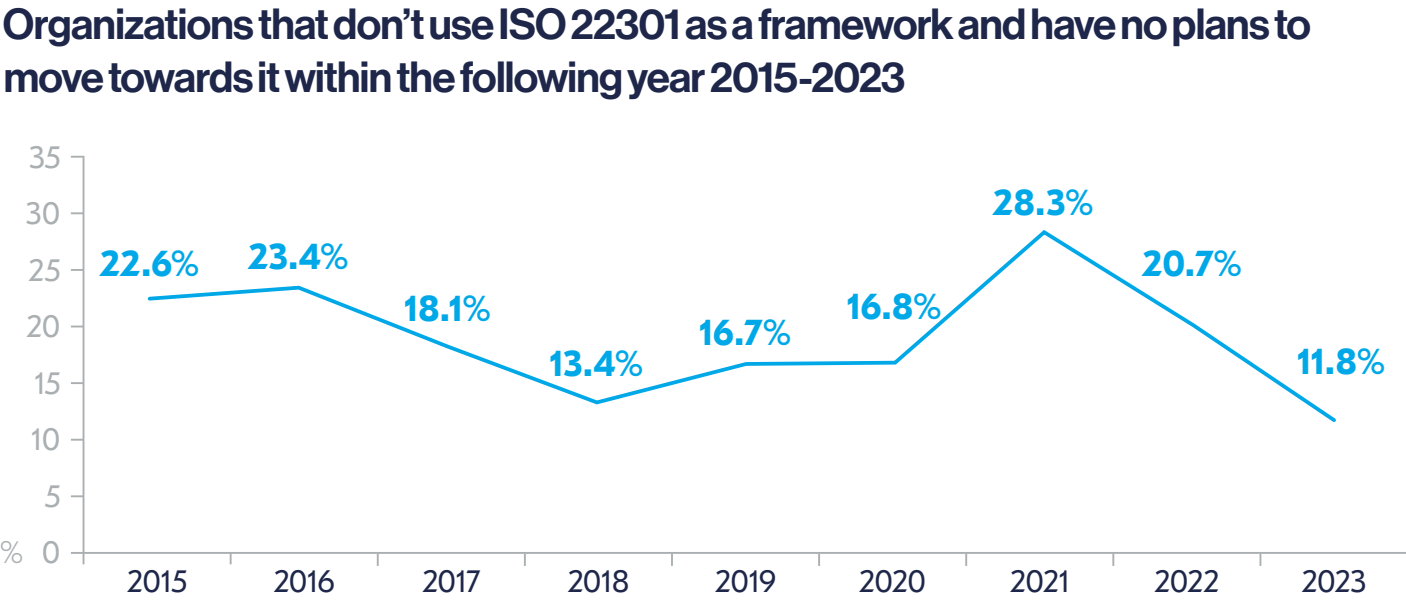


Figure 13. Organizations that don't use ISO 22301 as a framework and have no plans to move towards it within the following year 2015-2023

It is important to emphasise that choosing not to certify or align to ISO 22301 does not imply a lack of reliance on standards altogether. Organizations leverage a variety of standards and guidelines to enhance the resilience of their organization due to different reasons. In Australia, local standards are continuing to dominate in some sectors and regions, whereas others may choose to align to other related standards such as ISO 22316 (organizational resilience), or ISO 22361 (crisis management). Some interviewees explained their position in regard to their organization’s movement towards other standards:

“We are heavily driven by our national regulator, so we could spend a lot of time and effort going towards an ISO 22301 certification, but it would not achieve anything for us in terms of meeting our obligations, nor helping us on our path towards our maturity state.”

Resilience lead, financial services, Australia

“Japanese companies have shown great enthusiasm in obtaining certifications such as ISO 9001 (QMS) and ISO 14001 (EMS). However, they are generally much less eager to obtain ISO 22301 certification.”

Risk management and business continuity practitioner, manufacturing, Japan

While the ISO 22301 standard continues to maintain its popularity among resilience professionals, certain organizations are pushing the boundaries beyond standards to showcase exceptional organizational resilience. One interviewee discussed their initiative to launch a collaborative project with peers, cross-industry partners, and regulatory authorities to ensure the long-term resilience of the sector.

Organizations are increasingly certifying to ISO 22301 to showcase the effectiveness of their business continuity management system (BCMS) to external stakeholders

Respondents were asked about the benefits provided by certification. The current primary motivation was the need to demonstrate the effectiveness of the business continuity management system to external stakeholders, with nearly nine in ten (88.2%) saying this was the case. Although the top option in the previous edition of this report, it has seen a jump of 14.2 percentage points compared to 2022. BCI members regularly communicate that they are being increasingly asked to demonstrate the validity of their business continuity programme and showcasing certification or alignment to a recognised standard is a way of doing this. Furthermore, with the new DORA operational resilience regulations coming into force for critical third-party providers, the ability to demonstrate the quality of business continuity programmes is high. For some organizations, exhibiting certification to a standard can also help to negotiate more favourable terms with suppliers.

Another top choice for respondents is the fact that certification directly increases the resilience of an organization. As previously explained by an interviewee, being ISO certified and retaining that certification requires the business to ensure that resilience remains at the top of agendas. After all, the PR risk of losing a certification is far greater than the reputation gains of maintaining one. 82% of respondents responded positively to this option, an increase of 8 percentage points since 2022.

However, respondents raised a valid concern which is picked up most years: the ‘check a box’ exercise to demonstrate ISO 22301 certification compliance when entering into contracts with new buyers. In one interviewee’s case, it was argued that demonstrating resilience and gaining the trust of business partners required more than a perfunctory ‘box-checking’ exercise.

The third placed benefit of certification was to ensure faster recovery after a disruption. This option was checked by 58.8% of respondents, an increase of 4.8 percentage points since the last edition of this report and a jump from fifth to third place.

Enabling consistent BCM measurement and monitoring was selected as the fourth benefit of certification, with 52.9% of respondents choosing this preference.

Both the above factors show how certification can help ensure that operational practices are improved.

The benefit of improved communication and employee engagement (52.9%) and customer satisfaction (41.2%) close the top five positions. Both have increased 6.9 and 3.2 percentage points respectively and shows, in the case of the former, how the process of aligning/certifying can improve the communication flow within organizations, reducing siloing practices.

What benefits does certification provide to you and your organization?

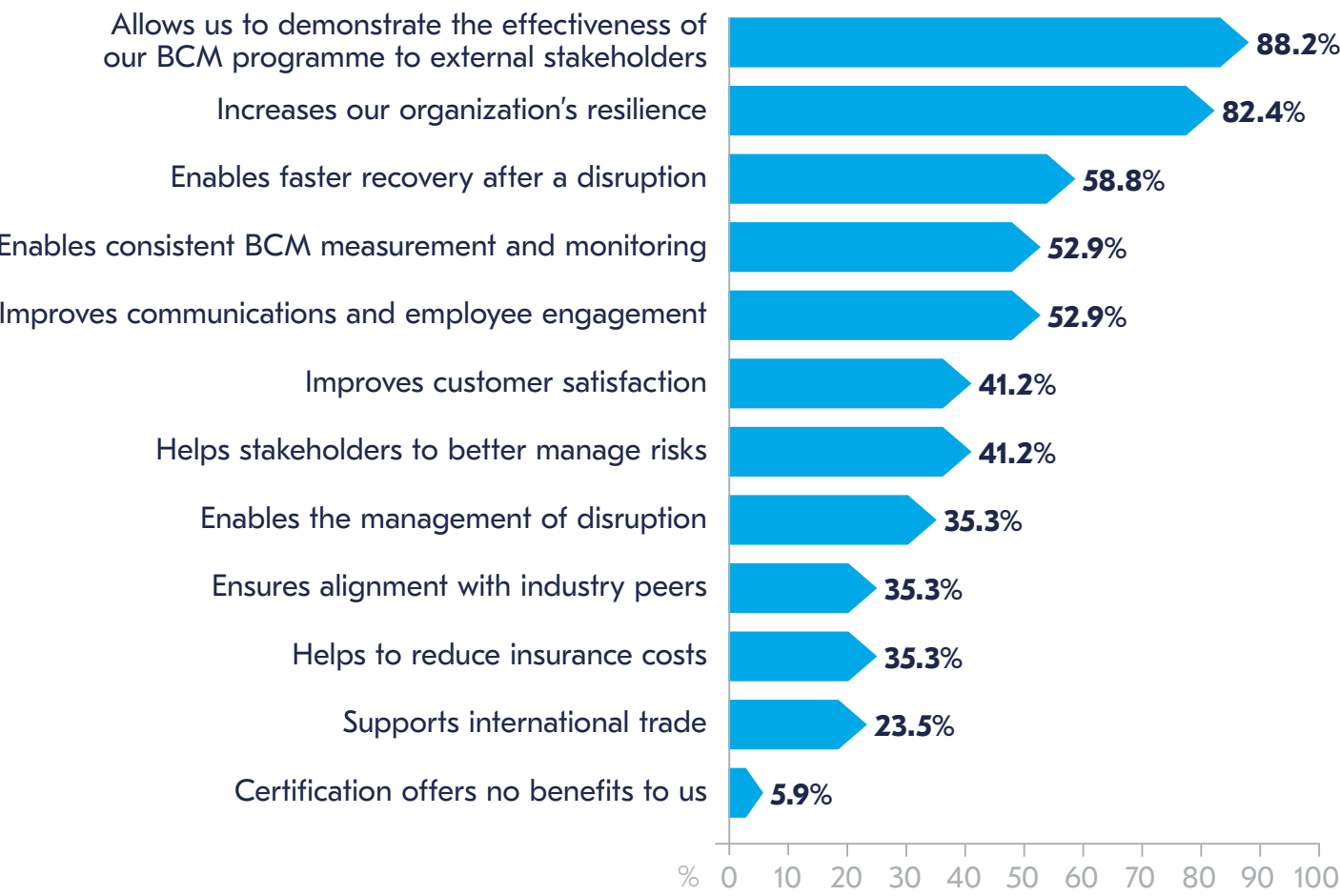


Figure 14. What benefits does certification provide to you and your organization?

Half of respondents who chose to align, but not certify, to ISO 22301 say alignment is enough for their own needs

As mentioned in the previous section, only 10% of organizations certify to ISO 22301, but over three-quarters (76.8%) do use the standard as a framework. When respondents were asked why they were not currently certified to the standard, half of respondents (50.0%) answered that was no need for their organization to certify as aligning was good enough for their needs. A further 48.9% of participants stated that there was no business requirement or, as in the case of one respondent, there were higher priorities for certification: “As a government contractor, we have other requirements to consider such as the operational assurance statement vs. certification.”

Budget is also an issue for more than a third of organizations. Getting certified can be expensive – both in terms of capital expenditure and staff time – and, for some organizations, particularly smaller ones, they feel they do not get a good enough return on investment. However, respondents answering this option were quick to point out that it was only the certification aspect which was expensive and they would continue to align with the standard.

“We are a small team, our program is so well embedded that it would not add anything to our business being ISO accredited; however we do try and align ourselves to the framework to say, ‘this is what we should be doing.’ We also use the Good Practice Guidelines as well.”

Business continuity manager, public sector, UK

“In terms of certification, I don’t know if it would give us a competitive advantage. Honestly the questionnaires we get from our customers ask, ‘Are you certified to ISO22301? If not, are you aligned to it?’ And I’m not aware of it ever costing us any business by saying, well, we’re aligned, but we’re not certified.”

Business resilience programme manager, IT & communications, USA

“The current financial climate means there are no available funds for us to attain ISO 22301. However we do align ourselves to the standard wherever possible.”

Corporate planning manager, public administration, UK



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



Figure 15. What are your reasons for not being certified or having no plans to be certified to ISO 22301?

Looking ahead



Looking ahead

- **In the medium to long-term, cyber security was quoted as the top concern for 78.5% of practitioners:** this aligns with the shorter-term concerns highlighted earlier in the report.
- **Climate risk is the second biggest threat for organizations in the mid- to long-term:** however, there is a notable disconnect with this elevated perception of risk and ensuring sound measures are in place to tackle the long-term effects of weather-related events.
- **Investment in BC/resilience is likely to increase, or remain at current levels, in 2024:** a quarter of practitioners expect investment levels to increase in 2024 while a further half expect funding to stay the same as in 2023. This is despite inflationary pressures in many economies.

Professionals were questioned about their concerns for the medium to long-term future (the next five to ten years). The prevailing concern identified was cyber security, with 78.5% of those surveyed expressed believing it is the greatest long-term risk to their organization.

Boards are increasingly engaging in more frequent discussions regarding matters such as cyber risk appetite, cyber risk tolerance, the quantification of cyber risk, and the adoption of a risk-based approach to cyber security. A report from the company eSentire projects that the anticipated global annual cost of cybercrime is set to reach \$8 trillion USD in 2023⁵⁸. This estimate is compounded by the increasing expenses resulting from cybercrime, which are likely to escalate to \$10.5 trillion by 2025. Given the worsening nature of cyber risk, practitioners need to ensure that senior management and the board are aware of the risks and supportive of both investing in staff and technologies to ensure that the organization is protected, as well as making sure that staff undergo continuous training so they can spot potential phishing emails. In this regard, business continuity management proves to be a valuable asset in the prevention, response, and recovery phases of cyber-attacks, particularly if working together with the IT and/or cyber security department.

In second place, climate risk was selected as a major threat by 48.8% of respondents. Climate risk has already been identified as a current risk to organizations, but its threat capability in the medium and long-term is likely to grow. As mentioned in the BCI Extreme Weather & Climate Change Report 2023⁵⁹, organizations are tending to respond to the short-term consequences of climate risk and/or natural disasters but are not investing in longer-term strategies. The financial resources necessary for building and system modifications, along with the additional time commitment expected from staff to address the heightened demands related to climate risk, stand as significant obstacles to the adoption of a new or enhanced climate risk strategy. Closely related to climate risks are natural disasters and, for organizations in areas prone to incidents such as earthquakes or volcanoes, this tends to dominate their longer term thinking.

"It is not so much climate risk for us, but it is about climate adaption and how we respond to what is expected. We are doing everything we possibly can, but are we going to meet all the expectations by the date that we are expected to do it? There are lots of reasons why we may not be able to get there, it might be demographically, as it is a bit more difficult for us because we are so predominantly rural. It could also be that we do not have sufficient funds to deliver everything that is expected of us within that timeframe. Other strategic risks are cyber security and the health and wellbeing of our staff."

Business continuity manager,
public sector, UK

"There is a province called KwaZulu-Natal in our country which is experiencing a lot of floods, earthquakes, tremors and so on. There is a lot happening in that area. Also in Johannesburg there was recently a gas leak which caused a large amount of damage to the infrastructure in the [central business district]; this is highly likely to happen again because of the failing infrastructure in that city."

Business continuity manager,
financial services, South Africa

"For business continuity, we primarily focus on natural disasters, especially earthquakes, and continue to keep our focus on them. Essentially, we don't think about other issues related to business continuity. Personally, I don't think this is sufficient, but many Japanese companies limit their preparation and focus on earthquakes."

Risk management and business continuity practitioner,
manufacturing, Japan

"Longer term planning is around our exposure to natural hazards. We live on a fault line, and it is a very active fault line. There is a 75% chance that the fault line that runs the length of South Island is going to rupture in the next 50 years, and that's going to trigger a magnitude 8 plus earthquake. Up the east coast of the North Island, we have the Hikurangi Subduction Zone. If that fault triggers, we could have a large earthquake of a magnitude of 9 plus. This would have a devastating impact on New Zealand. There is a little bit of thinking starting to happen in that space but not a huge amount."

Organisational resilience advisor,
public administration, New Zealand

In third place, nearly a third (30.6%) of respondents said that supply chain issues are a medium to long-term threat for their organization. As indicated in the BCI Supply Chain Resilience Report 2023⁶⁰ many organizations have not adequately addressed supply chain risks within business continuity plans, despite the high frequency of disruptions. During the pandemic, some positive changes were made to enhance supply chain resilience such as increased and deeper due diligence of suppliers, but it is vital for resilience professionals, supply chain professionals, and procurement professionals to sustain this focus through regular promotion of best practices, management standards, and case studies.



“The war in Ukraine has thrown our liberal international order into disarray. It’s put chaos into our markets and energy commerce. Suddenly, from an economic perspective, it’s really highlighted our supply chain resilience or lack thereof; we are now seeing companies diversifying and so there is all these flow on effects, energy prices spiking and so it is just making everything harder.”

Organisational resilience advisor, public administration, New Zealand

Nearly a third (29.8%) of organizations indicated the potential threat that technology/telecoms failure imposes on organizations. This aligns with the crucial role of IT infrastructure in the present era, especially with the increasing reliance on technology to facilitate everyday working practices, particularly in remote environments. Another pressing issue, as mentioned in the first section of the report, is the reliance on the Internet for communication. While voice-over-IP (VoIP) is cost-effective and convenient, the consequences of Internet outages or cyber-attacks impacting entire platforms, such as Microsoft, including tools like Teams, require meticulous planning and the integration of robust backup processes. This will become even more critical over the next few years with the majority of countries phasing out copper telephone wires by 2030.

Geopolitical change is the fifth greatest concern, highlighted by a quarter (25.4%) of respondents. Current geopolitical changes are reshaping the global landscape in significant ways, producing lengthy impacts on organizations and pushing them to change the way that they operate. The ongoing tensions between major powers continue to influence international relations. Climate change and environmental concerns are also driving geopolitical discussions, with nations working to address the urgent need for sustainable practices and environmental security. Furthermore, COVID-19 helped to highlight the importance of international cooperation in times of crisis, while also revealing challenges in coordination and distribution of resources. Interviewees explained how they are considering the aforementioned issue within their context:

“Few people seem to be thinking about the potential implications of the likes of the Ukraine war or the Chinese tensions beyond the economic lens. They are not looking two or three steps down the line of what could happen and therefore what the impact might be.”

Organisational resilience advisor, public administration, New Zealand



“The Taiwan and China issues are a huge concern for us now.”

Risk management and business continuity practitioner, manufacturing, Japan

“Around 70% of the world’s supply of neon gas comes from Ukraine. It also supplies 90% of the high-quality neon gas required by the USA chip manufacturers. Noble gases are critical to semiconductor production. So too are the rare earth metals that are mined in Australia and processed in China using noble gases. We currently have a war in the Ukraine. The “sabre-rattling” in the Indo-Pacific region appears like that of the early 1930s which was about control of commodities and markets. If my manufacturing involves semi-conductors and smart chips, I would be doing a lot of work to ensure that my supply chain is resilient.”

Senior associate, professional services, Australia

“Tension or conflict in the context of China and the West, has a focus in Australia given that it’s our region, it’s where we live. The major trading partner for Australian exports is China. Given that the nation provides all the iron ore and natural gas; anything that would interrupt that would certainly have a material impact on the economy. This includes not just a potential China-Taiwan issue, but broader tensions with other regional nations around the South China Sea.”

Business continuity Advisor, financial services, Australia

“There are nearly 800,000 Chinese citizens living in Australia, with strong investment in property and businesses by both individuals and organizations. Sanctions that might arise due to some form of conflict would be extremely impactful for many organizations, just through the effort and attention needed to separate all of those connections and meet any mandated requirements.”

Business continuity advisor, financial services, Australia

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



Figure 16. Thinking about the next 5-10 years, which are your top five concerns for the mid- to long-term risks?

African organizations' top three mid to long-term threats

- 1 Cyber security
- 2 Climate risk
- 3 Mental wellbeing of staff

Asian organizations' top three mid to long-term threats

- 1 Cyber security
- 2 Climate risk
- 3 Geopolitical changes

Australasian organizations' top three mid to long-term threats

- 1 Cyber security
- 2 Climate risk
- 3 Supply chain issues

European organizations' top three mid to long-term threats

- 1 Cyber security
- 2 Climate risk
- 3 Supply chain issues

North American organizations' top three mid to long-term threats

- 1 Cyber security
- 2 Climate risk
- 3 Technology/telecoms failure

Expect the unexpected

Emphasising the importance of ‘expecting the unexpected’ is crucial. BCI research has shown that practitioners tend to focus on risks that they are currently experiencing, rather than taking a broader view of the risk landscape. One prevailing issue is that organizations often maintain a reactive approach to incidents rather than adopting a proactive, longer-term, mindset. This is demonstrated when respondents were asked about investment in BC/resilience in order to better prepare for the challenges/threats identified in horizon scanning practices within organizations. The highest proportion of respondents indicated that investment for 2024 will remain at the same level as 2023 with nearly half (48.3%) choosing this option in the current edition. However, professionals do have to work hard to showcase the importance of a resilience programme now the memories of COVID-19 are fading. An interviewee explained how BC/resilience is considered an ‘expense’ within the organization, impacting budget allocation:

“Most of these programs are not revenue-generating programs. We are administrative, right? If we don’t do our jobs properly on the administrative side, certainly it could impact revenue negatively. But there’s not a lot that we can do about it. I’m not going to go out and win a multi-billion-dollar contract for my company. So I think our investment’s going to stay flat.”

Business resilience programme manager,
IT & communications, USA

Only 5% of respondents believe they will have a cut in investment to their resilience programmes in 2024

Nearly a quarter (24.6%) of respondents indicated that they are expecting an increase in investment to meet the needs of a growing programme or new requirements in 2024. Although this is lower than the 33.9% reported in 2022, it is perhaps understandable given the increased economic demands placed on organizations in the past year, coupled with a weaker macroeconomic backdrop.

An interviewee explained how investment is going to grow to accommodate a growing programme, because of the introduction of new regulation:

“By 1 July 2025, we’ll need to transition to the new [operational resilience] standard. We are already scoping out that work, but it is additional work; so even in my own area we are likely to increase resources on metrics, testing, validation and alignment. As we commence more detailed end-to-end testing of operational process recovery, we will find gaps and issues in our capability to do so, which we will need to invest in. This may result in manual processes, alternate systems, alternate resilience, and improved resilience. The investment is in the programme itself, but then it’s the outcomes of the programme which will drive investment requirements into suppliers, technology and other areas.”

Resilience lead, financial services,
Australia

The number of organizations that are expecting a budget cut in BC programmes has dropped to 5.1% this year compared to 8.1% in 2022. Interestingly, there were zero respondents from Asia who expected a drop in investment, perhaps due to the more positive economic situation in many Asian geographies.

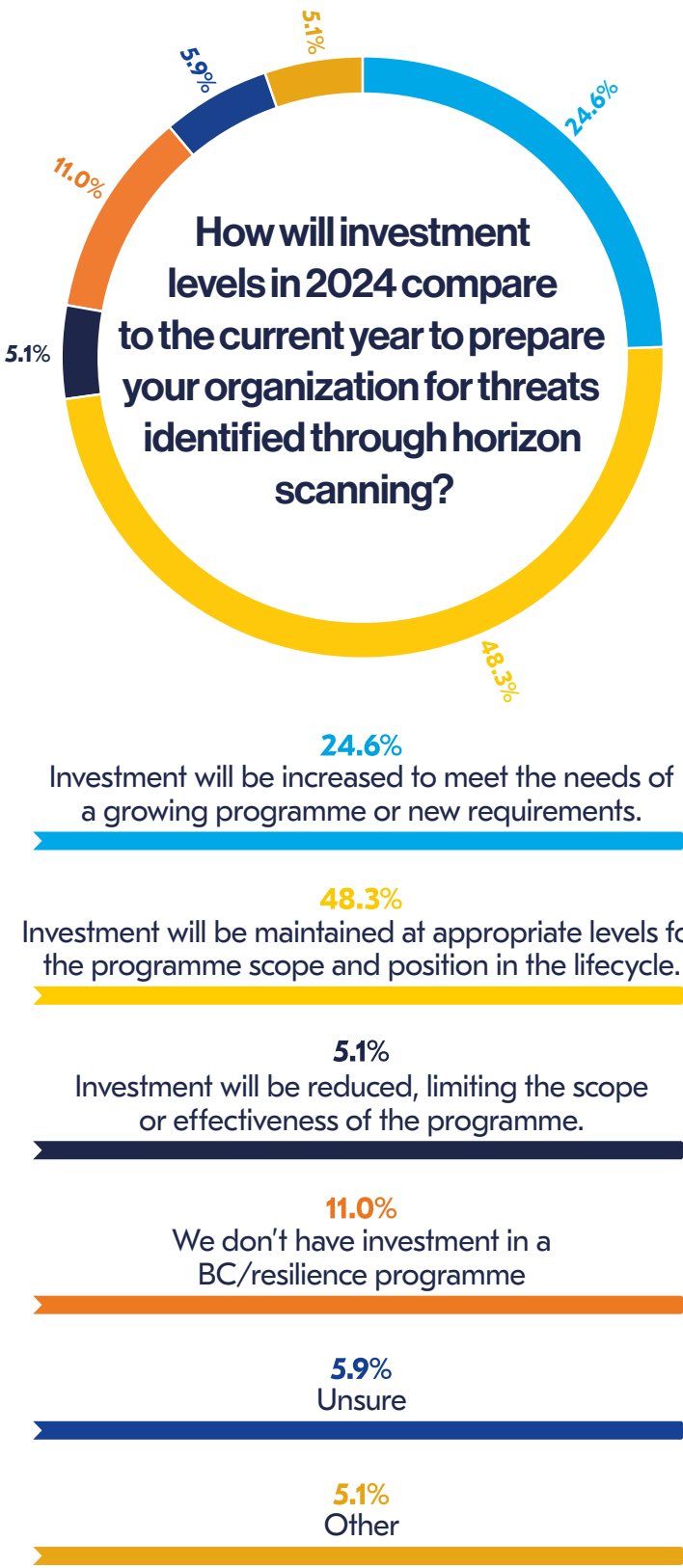


Figure 17. How will investment levels in 2024 compare to the current year to prepare your organization for threats identified through horizon scanning?

Annex



Figure 18. Which of the following best describes your functional role?

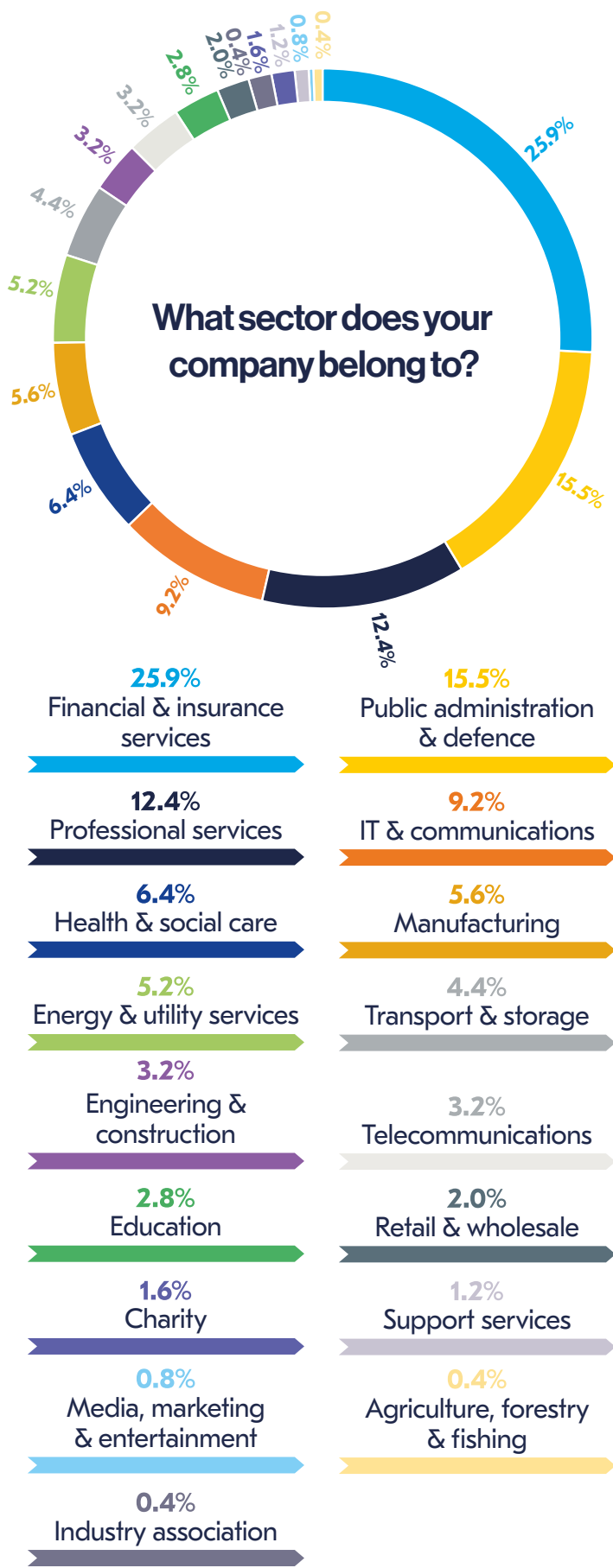


Figure 19. What sector does your company belong to?

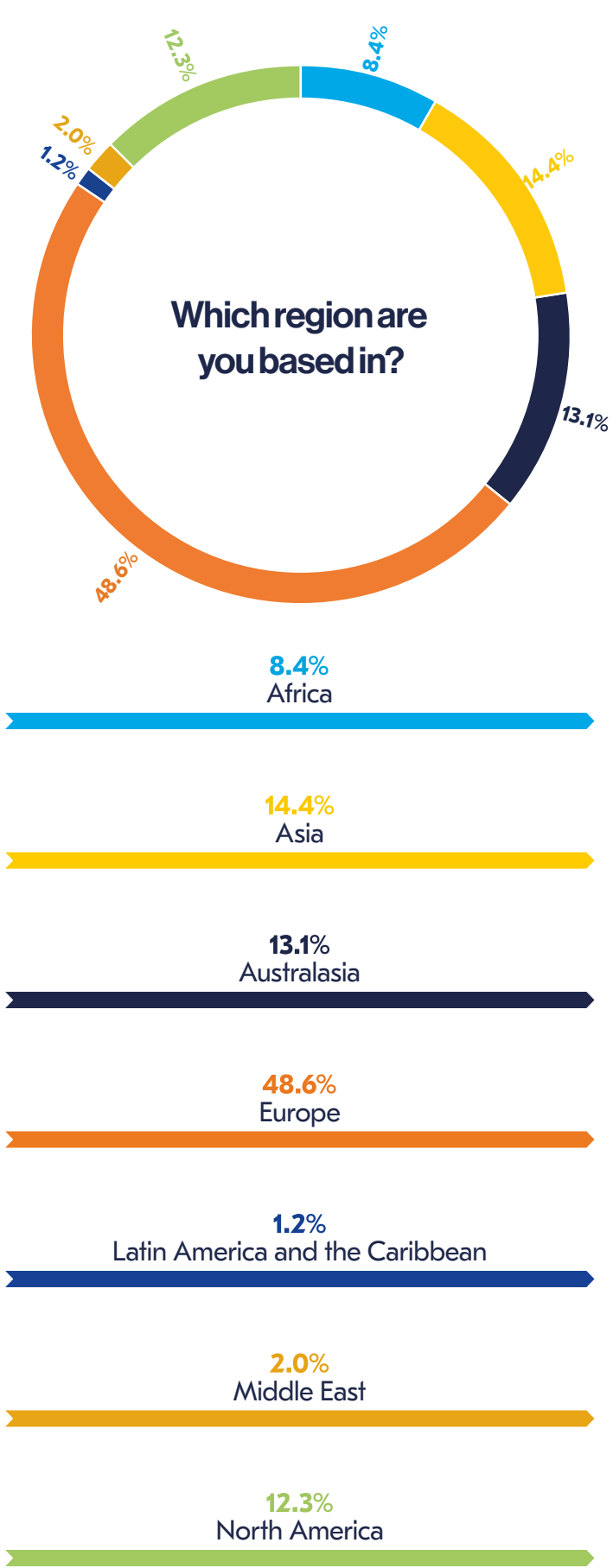


Figure 20. Which region are you based in?

Approximately how many employees are there in your organization globally?

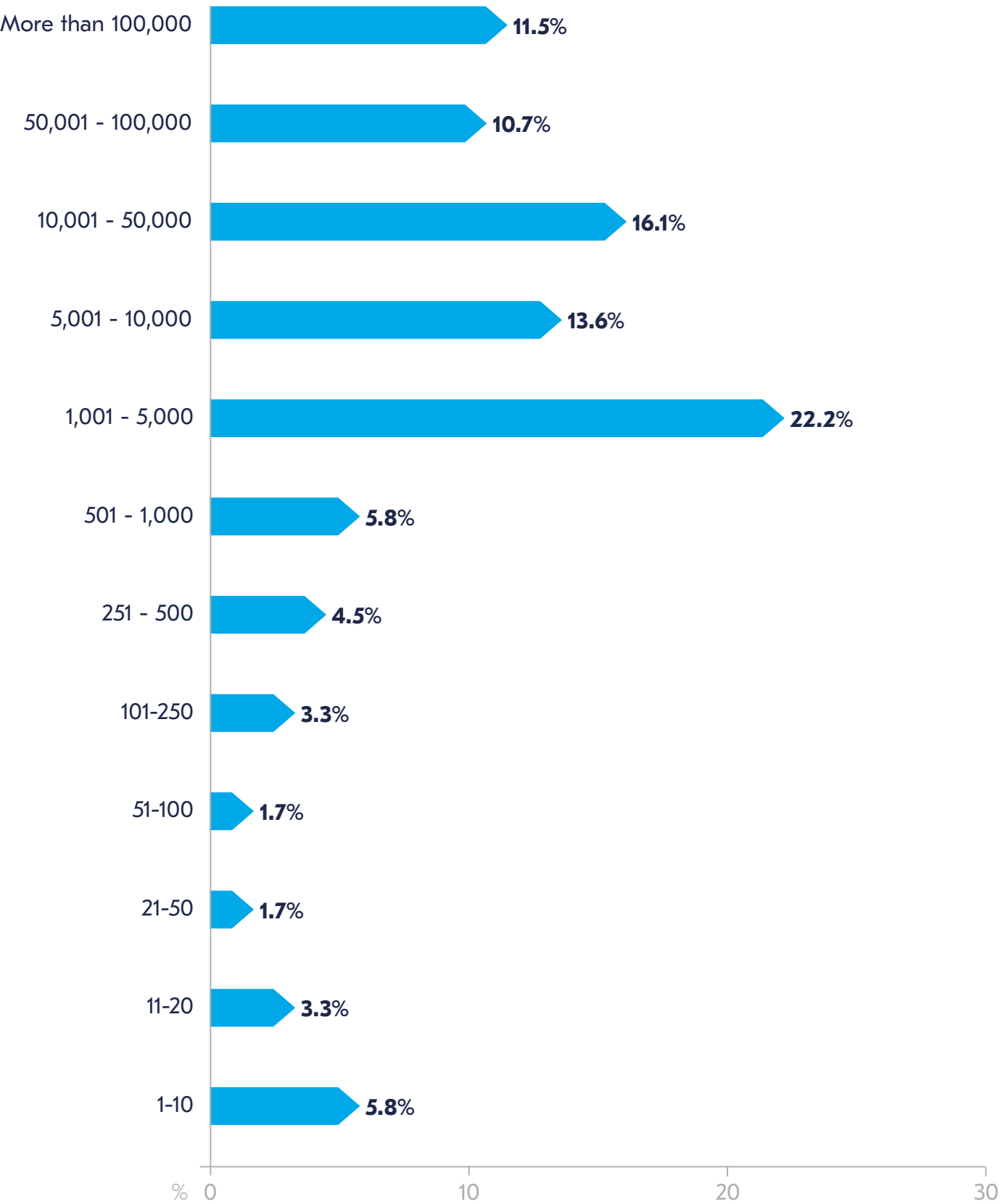


Figure 21. Approximately how many employees are there in your organization globally?

About the authors



Rachael Elliott
(Head of Thought Leadership, The BCI)

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 and 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



Maria Florencia Lombardero Garcia
(Research Manager, The BCI)

Maria has over 15 years of experience in academic and market research and has been responsible for the design and implementation of a wide range of policies within public and private organizations such as the Argentine Ministry of Defence, RESDAL, and BMI (Fitch Group). She has served as a policy advisor and political analyst at the Argentine Ministry of Defence and coordinated the Argentine National Security Council’s Office. She has particular expertise in geopolitical risk, defence, and intelligence and her work has been applied to develop government defence strategies and draft legislation on the matter. Her areas of interest relate to open-source research and how geopolitics impacts resilience within organizations.
She can be contacted at maria.garcia@thebci.org



About the BCI

Founded in 1994 with the aim of promoting a more resilient world, the 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 Corporate Membership 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
9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK



About Noggin

An industry-leader in integrated resilience management technology, Noggin provides a next-generation, cloud-based software platform that combines 10 primary solutions in one platform. Noggin’s award-winning integrated resilience workspace seamlessly unifies operational & third-party risk management, operational resilience, business continuity, incident & crisis management, emergency management, and security & safety operations.

For more, visit: www.noggin.io

References

1. World Health Organization (2023). Coronavirus disease (COVID-19) pandemic, WHO (online). Available at: <https://www.who.int/europe/emergencies/situations/covid-19#:~:text=This%20does%20not%20mean%20the,19%20on%20an%20ongoing%20basis.> (last accessed 12 October 2023)

2. The BCI Horizon Scan risk score is calculated by considering the number of times and event has occurred (analysing incidents in the past year) or the likelihood of an event occurring over the following year (threats for the following year), assigning these values a number and multiplying it by whether the impact was/will be minor (by 1), moderate (by 2), major (by 3) or extreme (by 4).

3. University of Sydney (2023). Moving on from COVID means facing its impact on mental health, says experts, Medical Xpress (online). Available at: <https://medicalxpress.com/news/2023-03-covid-impact-mental-health-experts.html> (last accessed 9 October 2023)

4. Panchal, N., Saunders, H., Rudowitz, R. and Cox, A. (2023). The Implications of COVID-19 for Mental Health and Substance Use. KFF (online). Available at: <https://www.kff.org/mental-health/issue-brief/the-implications-of-covid-19-for-mental-health-and-substance-use/> (last accessed 21 October 2023)

5. PwC (2023). Poor mental health is the main cause of long term sickness for the workforce, according to PwC research, PwC (online). Available at: <https://www.pwc.co.uk/press-room/press-releases/poor-mental-health-is-main-cause-of-long-term-sickness-for-the-workforce.html> (last accessed 9 October 2023)

6. UK Health and Safety Executive (HSA) (2022). Historical picture statistics in Great Britain, 2022. Trends in work-related ill health and workplace injury, HSE (online). Available at: <https://www.hse.gov.uk/statistics/history/historical-picture.pdf> (last accessed 9 October 2023)

7. Samson, P (2022). Business Continuity Management Lessons From The Pandemic, Forbes (online). Available at: <https://www.forbes.com/sites/forbestechcouncil/2021/03/15/business-continuity-management-lessons-from-the-pandemic/> (last accessed 12 October 2023)

8. International Labour Organization (ILO) (2023). Available at: https://www.ilo.org/moscow/areas-of-work/occupational-safety-and-health/WCMS_249278/lang-en/index.htm#:~:text=Worldwide%2C%20there%20are%20around%20340,of%20accidents%20and%20ill%20health. (last accessed 12 October 2023)

9. Sanderson, A and others (2023). Safety in the workplace: The decline of HSE investigations, Fieldfisher (online). Available at: <https://www.fieldfisher.com/en/insights/safety-in-the-workplace-the-decline-of-hse-investigations> (last accessed 12 October 2023)

10. Miller, Hon. G. (2008). Hidden Tragedy: Underreporting of Workplace Injuries and Illnesses. US House of Representatives (online). Available at: <https://www.bls.gov/iif/data-quality-research/hidden-tragedy-underreporting-of-workplace-injuries-and-illnesses.pdf> (last accessed 23 October 2023)

11. Sentis (2018). Underreporting of Safety Incidents in the Workplace, Sentis (online). Available at: <https://sentis.com.au/resources/workplace-safety-incident-reporting> (last accessed 23 October 2023)

12. Economist Intelligence Unit (2022). Worldwide Cost of Living 2022, EIU (online). Available at: <https://www.eiu.com/n/campaigns/worldwide-cost-of-living-2022-registration-confirmation> (last accessed 23 October 2023)

13. Economist Intelligence Unit (2023). Risk outlook 2024: continued high interest rates could lead to global recession, The EIU (online). Available at: <https://www.eiu.com/n/risk-outlook-2024-continued-high-interest-rates-could-lead-to-global-recession/> (last accessed 23 October 2023)

14. Cureton, S (2022). Coping with the cost of living crisis as a business, Funding Options (online) Available at: <https://www.fundingoptions.com/blog/education/coping-with-the-cost-of-living-as-a-business/>

15. Elliott, R. (2020). COVID-19. The Future of Supply Chain, The BCI (online). Available at: <https://www.thebci.org/resource/covid19--the-future-of-supply-chain.html> (last accessed 24 October 2023)

16. Hodgson, A (2022). Cost-of-Living Crisis: How Does It Impact Companies and Consumers?, Euromonitor International (online). Available at: <https://www.euromonitor.com/article/cost-of-living-crisis-how-does-it-impact-companies-and-consumers> (last accessed 12 October 2023)

17. KPMG (2023). The supply chain trends shaking up 2023, KPMG (online). Available at: <https://kpmg.com/xx/en/home/insights/2022/12/the-supply-chain-trends-shaking-up-2023.html>. (last accessed 12 October 2023)

18. Elliott, R and others (2023) BCI Supply Chain Resilience Report 2023, The BCI (online). Available at: <https://www.thebci.org/resource/bci-cyber-resilience-report-2023.html> (last accessed 12 October 2023)

19. UN (2023). Long COVID may obstruct return to normal life for 36 million Europeans, UN News (online) Available at: <https://news.un.org/en/story/2023/06/1138157> (last accessed 13 October 2023)

20. Berg, S. (2023). Unravelling the enigma of long COVID: What we know so far, American Medical Association (online). 13 September 2023. Available at: <https://www.ama-assn.org/delivering-care/public-health/unraveling-enigma-long-covid-what-we-know-so-far> (last accessed 30 October 2023)

21. WHO Coronavirus (COVID-19) Dashboard, WHO (online). Available at: <https://covid19.who.int/> (last accessed 13 October 2023)

22. Elliott, R and others (2022). BCI Horizon Scan Report 2022, The BCI (online). Available at: <https://www.thebci.org/resource/bci-horizon-scan-report-2022.html> (last accessed 12 October 2023)

23. Johnston, I. (2023). European gas prices soar on global supply chain fears, Financial Times (online). Available at: <https://www.ft.com/content/29ac8ac5-539e-43e3-b6eb-e86916fc5059> (last accessed 24 October 2023)

24. Mason, R. (2023). Attack on energy network a major risk, UK register says for first time, The Guardian (online). Available at: <https://www.theguardian.com/uk-news/2023/aug/03/attack-on-energy-network-a-major-risk-uk-register-says-for-first-time> (last accessed 24 October 2023)

25. Niranjn, N. (2023). Heatwave last summer killed 61,000 people in Europe, research finds, The Guardian (online). Available at: <https://www.theguardian.com/environment/2023/jul/10/heatwave-last-summer-killed-61000-people-in-europe-research-finds> (last accessed 24 October 2023)

26. World Weather Attribution (2023). Extreme heat in North America, Europe and China in July 2023 made much more likely by climate change, World Weather Attribution (online). Available at: [https://www.worldweatherattribution.org/extreme-heat-in-north-america-europe-and-china-in-july-2023-made-much-more-likely-by-climate-change/#:~:text=July%202023%20saw%20extreme%20heatwaves,China%20\(CNN%2C2023\).](https://www.worldweatherattribution.org/extreme-heat-in-north-america-europe-and-china-in-july-2023-made-much-more-likely-by-climate-change/#:~:text=July%202023%20saw%20extreme%20heatwaves,China%20(CNN%2C2023).) (last accessed 13 October 2023)

27. Harding, A. (2023). South Africa load-shedding: The roots of Eskom's power problem, BBC (online). Available at: <https://www.bbc.co.uk/news/world-africa-65671718> (las accessed 12 October 2023)

28. GOV.uk (2023). Terrorism (protection of premises) draft bill: overarching documents, UK Government; Home Office (online). Available at: <https://www.gov.uk/government/publications/terrorism-protection-of-premises-draft-bill-overarching-documents> (last accessed 25 October 2023)

29. Torkington, Simon (2023). We're on the brink of a 'polycrisis' — how worried should we be?, World Economic Forum (online). Available at: <https://www.weforum.org/agenda/2023/01/polycrisis-global-risks-report-cost-of-living/> (last accessed 19 October 2023)

30. Lawrence, A. & Simon, L. (2023). Annual outage analysis 2023. Uptime Intelligence (online). Available at: https://uptimeinstitute.com/uptime_assets/5f40588be8d57272f91e4526dc8f821521950b7bec7148f815b6612651d5a9b3-annual-outages-analysis-2023.pdf (last accessed 25 October 2023)

31. Sweney, M. (2023). Number of Britons facing significant internet outages doubles in a year, The Guardian (online). Available at: <https://www.theguardian.com/money/2023/sep/07/number-of-britons-facing-significant-internet-outages-doubles-in-a-year> (last accessed 13 October 2023)

32. UK Cabinet Office (2023). National Risk Register 2023, UK Government (online). Available at: <https://www.gov.uk/government/publications/national-risk-register-2023> (last accessed 13 October 2023)

33. Elliott, R and others (2023). BCI Extreme weather & climate change report 2023, The BCI (online). Available at: <https://www.thebci.org/resource/bci-extreme-weather---climate-change-report-2023.html> (last accessed 18 October 2023)

34. World Meteorological Organization (2023). Economic costs of weather-related disasters soars but early warnings save lives, World Meteorological Organization (online). Available at: <https://public.wmo.int/en/media/press-release/economic-costs-of-weather-related-disasters-soars-early-warnings-save-lives> (last accessed 13 October 2023)

35. Elliott, R and others. BCI Cyber Resilience Report 2023, BCI (online). Available at: <https://www.thebci.org/resource/bci-cyber-resilience-report-2023.html> (last accessed 13 October 2023)

36. Morgan, Steve (2019). Global Cybersecurity Spending Predicted To Exceed \$1 Trillion From 2017-2021, Cybercrime magazine (online). Available at: <https://cybersecurityventures.com/cybersecurity-market-report/> (last accessed 26 October 2023)

37. Mc Lean, Mike (2023). 2023 Must-Know Cyber Attack Statistics and Trends, Embroker (online). Available at: <https://www.embroker.com/blog/cyber-attack-statistics/> (last accessed 26 October 2023)

38. Ibid

39. De Smet, A and others (2023). Some employees are destroying value. Others are building it. Do you know the difference? , McKinsey (online). Available at: <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/some-employees-are-destroying-value-others-are-building-it-do-you-know-the-difference> (las accessed 26 October 2023)

40. Pendell, R (2022). Employee Engagement Strategies: Fixing the World's \$8.8 Trillion Problem, Gallup (online). Available at: <https://www.gallup.com/workplace/393497/world-trillion-workplace-problem.aspx> (last accessed 16 October 2023)

41. World Bank 2022. Global productivity: trends, drivers, and policies, The World Bank (online). Available at: <https://www.worldbank.org/en/research/publication/global-productivity> (last accessed 16 October 2023)

42. World Health Organization (2022). Mental health at work, WHO (online). Available at: <https://www.who.int/news-room/fact-sheets/detail/mental-health-at-work> (last accessed 16 October 2023)

43. Ibid

44. Pemberton, Chris (2018). Key Findings From the Gartner Customer Experience Survey, Gartner (online). Available at: <https://www.gartner.com/en/marketing/insights/articles/key-findings-from-the-gartner-customer-experience-survey> (last accessed 26 October 2023)

45. Szyndlar, M (2023). Customer Satisfaction: Why It's Important in 2023, Survicate (online) Available at: <https://survicate.com/customer-satisfaction/importance-customer-satisfaction/> (las accessed 17 October 2023)

46. Thomas, G and other. 10 Ways to Boost Customer Satisfaction, Harvard Business Review (online) Available at: <https://hbr.org/2023/01/10-ways-to-boost-customer-satisfaction> (last accessed 17 October 2023)

47. Elliott, R and others (2023). What are the effects of reputational damage?, the BCI (online). Available at: <https://www.thebci.org/resource/bci-crisis-management-report-2023.html> (last accessed 17 October 2023)

48. Elliott, R and others (2023). BCI crisis management report 2023, the BCI (online). Available at: <https://www.thebci.org/resource/bci-crisis-management-report-2023.html> (last accessed 17 October 2023)

49. Elliott, R and others (2023). BCI crisis management report 2023, the BCI (online). Available at: <https://www.thebci.org/resource/bci-crisis-management-report-2023.html> (last accessed 17 October 2023)

50. Elliott, R and others (2023). BCI Cyber Resilience Report 2023, The BCI (online). Available at: <https://www.thebci.org/resource/bci-cyber-resilience-report-2023.html> (last accessed 18 October 2023)

51. Kolesnikov, N (2023). 50+ Cybersecurity Statistics for 2023 You Need to Know — Where, Who & What is Targeted, Techopedia (online). Available at: <https://www.techopedia.com/cybersecurity-statistics> (last accessed 18 October 2023)

52. Sonicwall (2023). 2023 Sonicwall cyber threat report, Sonicwall (online). Available at: <https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf> (last accessed 18 October 2023)

53. Elliott, R and others. BCI crisis management report 2023, the BCI (online). Available at: <https://www.thebci.org/resource/bci-crisis-management-report-2023.html> (last accessed 17 October 2023)

54. Burt, T (2023). Espionage fuels global cyberattacks, Microsoft (online). Available at: <https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/> (last accessed 18 October 2023)

55. Ibid

56. Continuity Central (2023). 91 percent of businesses experience at least one network outage quarterly. Continuity Central (online). Available at: <https://www.continuitycentral.com/index.php/news/technology/8614-91-percent-of-businesses-experience-at-least-one-network-outage-quarterly> (last accessed 25 October 2023)

57. Lawrence, A. & Simon, L. (2023). Annual outage analysis 2023. Uptime Intelligence (online). Available at: https://uptimeinstitute.com/uptime_assets/5f40588be8d57272f91e4526dc8f821521950b7bec7148f815b6612651d5a9b3-annual-outages-analysis-2023.pdf (last accessed 25 October 2023)

58. eSentire (2022). 2022 Official Cybercrime Report, eSentire (online). Available at : <https://www.esentire.com/resources/library/2022-official-cybercrime-report#:~:text=According%20to%20Cybersecurity%20Ventures%2C%20the%20global%20annual%20cost,is%20expected%20to%20reach%20%2410.5%20trillion%20by%202025> (last accessed 24 October 2023)

59. Ibid

60. Elliott, R and others (2023) "BCI Supply Chain Resilience Report 2023", The BCI (online). Available at: <https://www.thebci.org/resource/bci-supply-chain-resilience-report-2023.html> (last accessed 24 October 2023).

BCI 9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK

bci@thebci.org / www.thebci.org