Find out more
www.thebci.org

Thought Leadership

BCI Crisis Management Report 2024

F24

Leading the way to resilience

Contents

Foreword

It is our pleasure to introduce the BCI Crisis Management Report 2024. We are once again extremely grateful to F24 for their continued sponsorship of this important report in our portfolio.

2024 has been a busy year for crisis management teams: fewer than a quarter of survey respondents (23.0%) reported zero activations of their crisis team in 2024, while over a sixth (17.3%) said that they had greater than five activations. The increasing number of activations can undoubtedly be linked to a growing, and increasingly unpredictable, threat landscape. Severe weather events are becoming more extreme and encroaching on previously 'safe' areas, global and civil conflicts are testing organizations' resilience to new extremes, others are being forced to act to build counter-strategies for civil unrest and strikes, while cyber-crime continues its upwards trajectory with global conflicts now increasingly being mirrored in virtual landscapes.

Encouragingly, however, we are seeing professionals changing their strategies to ensure their organizations and their people are safeguarded at the time of a crisis. Some of this is as a results of organizations spending more time on reflective practices, and absorbing lessons-learned into their strategies. Indeed, nearly half (46.4%) of organizations are now conducting a post-incident review (PIR) or after-action review (AAR) after every single incident compared to 38.7% in 2023. Some of our members even report going a stage further, conducting reviews of 'near misses' as well.

Such practices are vital to ensure continuous improvement in practices, something that the majority of respondents agree is vital. Just 22.4% considered their crisis management capabilities to be 'excellent' which is partially indicative that most are acutely aware of the need to continually update plans to suit the changing environment they are operating in.

One of the most notable takeaways from this year's report is an appreciation of the need to consolidate information and take a non-siloed approach to crisis management. An increasing number of organizations are centralising crisis management structures (45.9% compared to 44.9% in 2023), while the adoption of a hybrid approach — often considered the best approach to take — has risen to 38.8% (2023: 35.2%). Hybrid structures provide a degree of local autonomy to different regions/business units but maintain centralised control; consistently proving to provide a more successful response. Taking both centralised and hybrid into account, 84.9% of organizations now have some degree of centralisation in their processes; realising the benefits of more fluid teams, expert input, and technological enhancements to the process. When also considering that fewer than 1 in 10 organizations (8.9%) still operate in a decentralised manner (a near-halving of the figure seen in this year's report), there has clearly been a step-change in efforts to reduce the siloes that have been so inherent in crisis team practices over the recent years.

Next year, it would be great to see organizations further developing their crisis management strategies to tackle some of the issues that are being experiencing with crisis management processes: lack of awareness of plans, the absence of sharing plans, and the crisis team not being sufficiently trained are the top three areas cited for improvement by professionals. With 84.4% of respondents saying that investment will be directed to training and exercising in 2025, the signs are encouraging.

We hope you find that this new report serves as a useful tool for benchmarking your own practices and provides valuable learnings for your own organization on crisis management. We would once again like to thank F24 for their continued, valued support of this report.

Rachael Elliott
Knowledge Strategist
The BCI

F24

Foreword

In an era of unprecedented disruption, organisations around the world faced a wide range of crises last year. In this complex threat landscape, flexibility, rapid decision-making and comprehensive preparedness have become key pillars of success. Therefore, having robust crisis response strategies and adaptable teams in place has become more important than ever.

Extreme weather events, third party failures, cyber-attacks, civil unrest and health and safety incidents were among the top triggers for activating crisis teams over the last 12 months. This diversity of crises highlights the need for comprehensive plans that cover a wide range of potential disruptions. And facing multiple disruptive events simultaneously, or dealing with the interaction of several crises, is becoming an increasingly common reality for organizations. Encouragingly, more and more companies make use of today's technological possibilities each year to better manage these highly complex incidents, with over 80% saying that technology has helped their organisation's crisis response. In particular, the move from physical to virtual crisis rooms has been another notable trend over the years, with around 25% of respondents now using such technologies in their crisis response. Of these, the vast majority (94.1%) reported improved internal efficiencies through virtual crisis management to respond faster and more securely.

The report also highlights the need for diverse skills within crisis teams to respond quickly and efficiently to both internal and external challenges. In this regard, it once again clearly shows that collaboration is key. Fortunately, this fact is widely recognised by companies, with 90.5% agreeing that a team's ability to interact with other functions is key to successfully managing a crisis.

However, challenges remain. A significant number of organisations still face problems such as a lack of awareness of crisis plans among staff (30.1%) and insufficient training for crisis team members (27.0%). It is also striking that, despite today's technological capabilities, 44.5% of respondents still use call trees as part of their organisation's crisis response. This highlights the gap between technological potential and actual adoption, and shows that we still have a long way to go to make crisis management more efficient, streamlined and aligned with modern capabilities.

As the report shows once again, our world is becoming more complex, and with it, the need for resilience even more essential. At F24, we are committed to providing businesses with the right tools to navigate this complexity. We are very grateful for our continued trusted partnership with the BCI, which allows us to contribute to this important resource for anyone looking to improve their business resilience.

I trust that the report provides you with valuable insights into the current state of crisis management and inspires you to reflect on and enhance your own organization's preparedness. As the threat landscape continues to evolve, I hope this report serves as both an informative resource and a catalyst for proactive improvements in your crisis management strategies.

Benjamin Jansen
Senior Vice President
Sales; Emergency Notification Services and Crisis Management
F24

Executive summary

The majority of organizations have faced a crisis within the previous twelve months.

This highlights the importance of having a crisis management team that can rapidly and efficiently mobilise to orchestrate a response.

75.1% of organizations have activated their crisis management team over the past twelve months.

Primary triggers for crisis activation reveal a diverse range of threats in 2024.

This broad spectrum underscores the need for comprehensive crisis management strategies that address various potential disruptions, and the implementation of incident agnostic plans. Such a complex threat landscape also emphasizes the need for a diverse range of skills within the crisis management team.

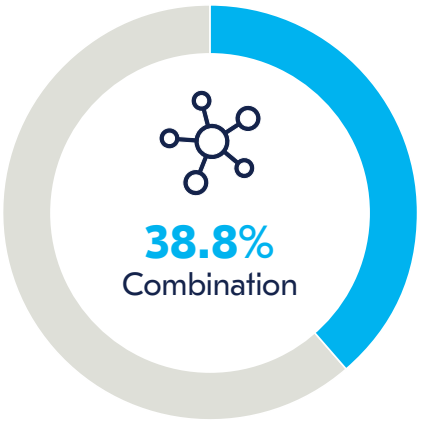
Top five drivers of crisis activation.

1. **38.5%** Extreme weather event
2. **27.6%** Third party failure
3. **27.6%** Cyber-attack
4. **19.0%** Civil unrest or conflict, vandalism, or activism
5. **14.9%** Health and safety incident

Most organizations favour a centralised crisis management structure, reflecting a preference for streamlined decision-making.

However, a growing number of organizations employs a hybrid approach, blending centralized and business units/regions strategies to balance control with localized adapted response. Encouragingly, both centralised and combined approaches have experienced a slight increase in 2024, leaving behind purely regional or business led approaches.

How does your organization manage its crisis management structure?



Organizations' top priorities in crisis management this year are quick mobilisation of the crisis management team, effective external communications, and staff wellbeing.

The emphasis on these factors reflects a growing recognition of the need for fast, efficient communication, a supportive team environment during crises, and the importance of cohesive PR messaging. The criteria highlighted by respondents are in line with 2023, indicating a consolidated trend.

How much do you strongly agree/agree with the following **positive** criteria applied to your crisis management processes?

88.7%
External communications and PR are considered in the crisis response

88.7%
The crisis team can be mobilised quickly

87.0%
Staff health and wellbeing is a key consideration of the crisis management team

82.2%
The team can adapt quickly to a rapidly changing scenario

79.8%
The crisis team contains the right people from each department

Challenges persist in crisis management processes, with notable issues such as inadequate awareness of crisis plans among staff and insufficiently trained team members.

The risk of burnout and the lack of awareness of plans amongst staff highlight the need for training and exercising to ensure that all team members are well-prepared and informed. Compared to 2023, there is growing concern about mental health issues and adequate training within the crisis management team, which sheds light on the importance of the human factor in crisis management.

How much do you strongly agree/agree with the following **negative** criteria applied to your crisis management processes?

30.1%
Wider staff are unaware of crisis plans which has/could lead to confusion in a crisis scenario

29.5%
Plans are not shared across the organization

27.0%
Members of the crisis team are not appropriately trained

25.0%
We do not change crisis team members out often enough

16.5%
The crisis team is at risk of burnout

An increasing number of professionals report senior executives "are recognising the importance of delegated control in the crisis management, and assuming more of an oversight role.

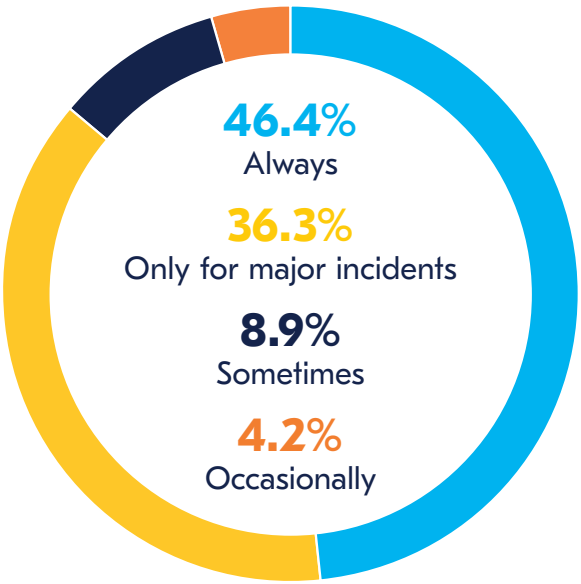
This marks a difference compared to 2023, where top management was likelier to participate from the start. This reveals a recognition of the need to allow regional/business unit managers the ability to make quick decisions without having the wait for a response from senior management.

How much are the board/senior executive team involved in the decision-making process during a crisis?

Regular post-incident reviews are a common practice, with many organizations conducting them consistently or at least for major incidents.

This highlights a commitment towards learning and improvement, which is in line with international good practices and guidelines on crisis management and organizational resilience. This elevated recognition of the importance of reflective processes post-incident is one of the positive learnings that resulted from the pandemic.

How often do you conduct a post-incident/after action review (PIR/AAR)?



Senior leadership, business continuity, and IT departments are typically well-represented in post-incident reviews in three-quarters of organizations, reflecting their critical roles in managing and mitigating crises.

Outside the top three departments, the involvement of operations and security teams also highlights the broad, cross-departmental engagement necessary for effective review and response. Collaboration among these units is crucial in light of the variety of drivers that have led to the activation of crisis management teams in the past twelve months.

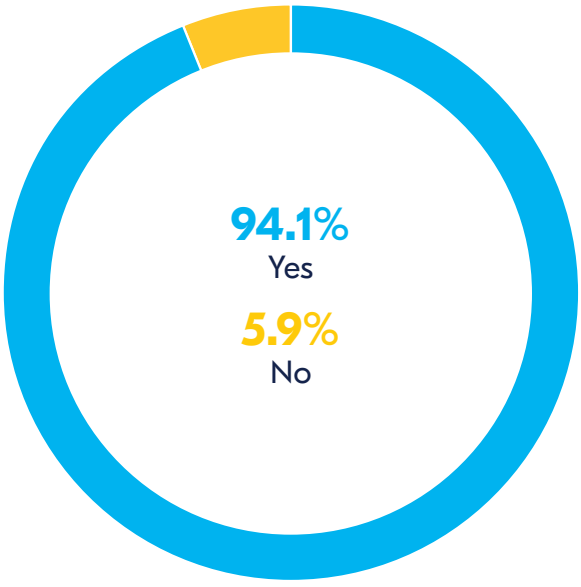
Top three departments represented in post-incident reviews

1. **79.3%** Senior leadership
2. **74.4%** Business continuity
3. **74.4%** IT

An increasing number of organizations are switching away from physical crisis rooms and choosing to manage crises virtually - to great benefit.

Virtual crisis rooms are being increasingly adopted by organizations, often replacing on-site, physical crisis rooms. Virtual crisis rooms allow for immediate activation of teams, access to global subject matter experts, and can have additional security measures attached such as the disabling of screenshotting. Other commonly used tools include enterprise software and messaging apps, reflecting a blend of structured and informal communication methods. AI is increasingly seen as beneficial, particularly for real-time monitoring, data analysis, and automating response protocols, indicating a growing reliance on an increasing trust in advanced technologies to bolster crisis management capabilities.

If you use virtual crisis room management, has it simplified or enhanced your organization's internal efficiency?



Top three technology tools used within the past year as part of organizations' crisis response.

1. **73.8%** Enterprise software (e.g. Microsoft Teams)
2. **48.8%** Free messaging apps (e.g. WhatsApp, Microsoft Messenger)
3. **25.6%** Virtual crisis room/ dashboard technology

Top five areas where respondents think AI can help within crisis management.

1. **72.5%** Data analysis and decision support
2. **70.6%** Real-time monitoring and alerts
3. **56.2%** Predicting potential crises
4. **49.7%** Automating response protocols
5. **44.4%** Communication and coordination during a crisis

Introduction

In the current, increasingly dynamic, landscape organizations operate the ability to swiftly adapt and respond to diverse threats has become increasingly crucial. Over the past twelve months, a significant number of organizations have activated their crisis management teams, highlighting the persistent and varied nature of crises. This report delves into the key phases of crisis management — preparedness, threat identification, response, communications, recovery, and evaluation — providing a comprehensive overview of current practices and challenges.

This year's research reveals that while many organizations have established robust mechanisms for crisis response, there remains a diverse range of triggers that necessitated activation. These range from extreme weather events and cyber-attacks to third-party failures and civil unrest, underscoring the need for adaptable and multilayered strategies. While professionals favour centralised structure due to their streamlined decision-making, many are now adopting hybrid approaches

The report further explores how organizations prioritise aspects such as rapid mobilisation, effective external communication, and staff wellbeing during crises. Notably, challenges persist in areas such as crisis plan awareness and team training, pointing to the need for continual improvement. Senior leadership's involvement has evolved, with varying levels of engagement throughout the crisis decision-making process, reflecting shifts in crisis management approaches.

Post-incident reviews (PIRs)/after-action reviews (AARs) are widely practiced, signifying a commitment to learning and enhancing future responses. The role of technology, including virtual crisis management tools and AI, is being increasingly recognised for its potential to streamline operations and support decision-making. As organizations navigate these complexities, this report offers insights into how they are adapting their crisis management strategies to remain resilient in an ever-evolving threat landscape.

1 Crisis management within organizations

Crisis management within organizations

- The majority of organizations experienced multiple crises in the past year, with extreme weather, third-party failures, and cyber-attacks being the primary drivers, highlighting the complex and varied nature of modern crises.
- There is a preference for centralised crisis management approaches, which are seen as more effective in ensuring clear decision-making and consistency across global operations. However, many organizations combine this with regional or business unit-led teams for flexibility.
- A significant concern is the lack of awareness and training of crisis plans among staff, which may lead to confusion during crises. Respondents emphasise the need for more agile, well-trained crisis management teams to adapt to rapidly changing scenarios.

In 2024, data was gathered for the first time on the frequency of crisis activations. More than half of survey participants (57.9%) experienced between one and five crises during the year, while an additional 19.1% faced six or more incidents. This data highlights a challenging threat landscape, where the majority of organizations had to rely on their crisis management function multiple times throughout the year. Only less than a quarter (23.0%) managed to avoid activating their crisis management team over the past 12 months.

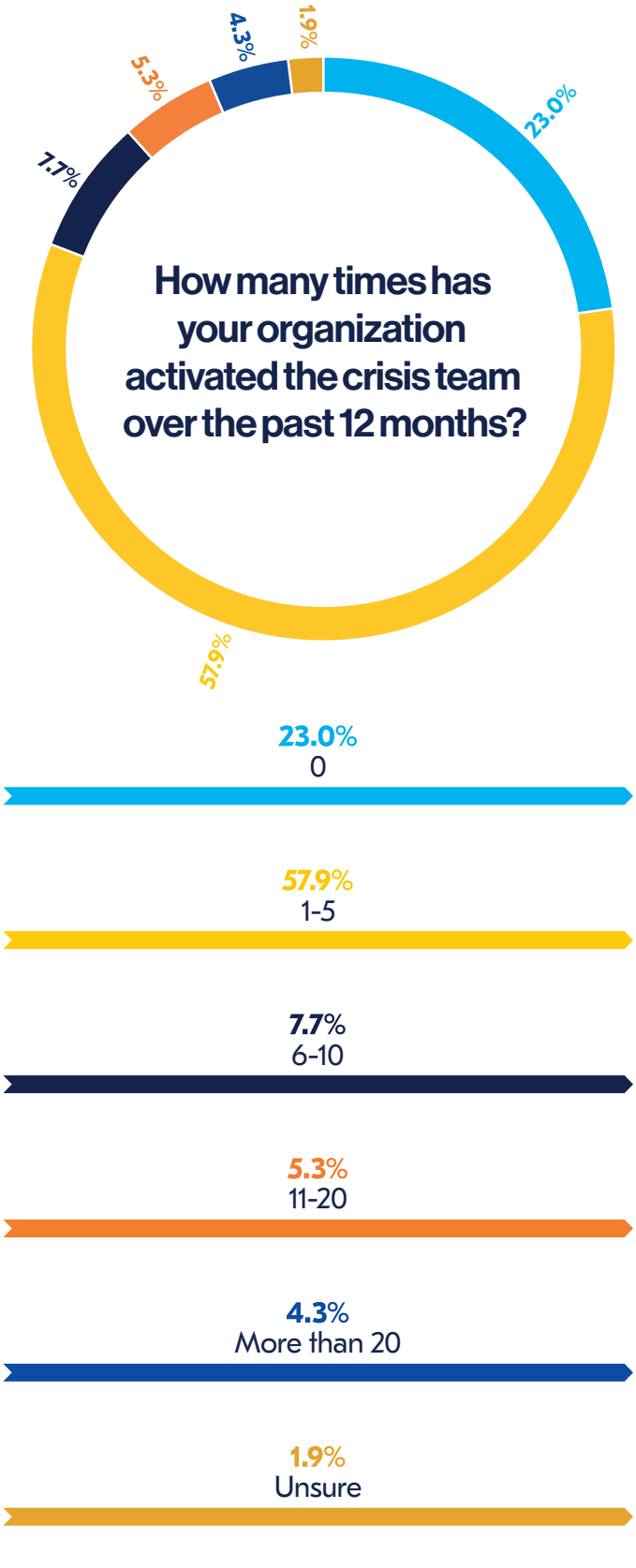


Figure 1. How many times has your organization activated the crisis team over the past 12 months?

The drivers of these crises were diverse and varied. The most frequent cause was extreme weather (38.5%), a predictable outcome given the increasing frequency and intensity of unprecedented weather events in recent years[1]. Violent natural phenomena have repercussions that can cause widespread disruption[2]. For instance, in May 2024, unprecedented rainstorms and floods swept across Gulf countries, including the UAE, Bahrain, Qatar, Saudi Arabia, and Oman, causing widespread devastation. Dubai experienced its heaviest rainfall on record, leading to significant infrastructure damage. The floods severely disrupted operations at Dubai International Airport, the world's second busiest, forcing the cancellation of hundreds of flights. Roads, bridges, and other critical infrastructure were overwhelmed, exposing the region's vulnerability to extreme weather. The damage, likely amounting to hundreds of millions of dollars, revealed the urgent need for more resilient infrastructure as climate risk continues to increase the frequency and severity of such events[3].

Two other significant triggers were third-party failures (27.6%) and cyber-attacks (27.6%). The equal frequency of these two drivers underscores the need for versatility in crisis management, given their distinct nature. While third-party failures and cyber-attacks can be interconnected, they can also occur as separate, very different events. For instance, a third-party failure might relate to supply chain issues (12.1%) and involve a contractor in another country, necessitating international oversight. Conversely, a cyber-attack might lead to internal disruptions and a data breach (14.4%), requiring skilled personnel to precisely identify the disruption's scope and determine the necessary recovery time. Despite their differences, both events could lead to reputational damage, underscoring the need for sound crisis communication protocols. The reality of facing more than one disruptive event, or have multiple events interacting, at the same time is a phenomenon that it is becoming more common for organizations.

On the other hand, incidents like civil unrest (19.0%) and health and safety incidents (14.9%) introduce a physical threat to staff, adding a new dimension to crisis management. In these cases, organizations must prioritise safety while managing operations and protecting their reputation. For example, in situations involving civil unrest or activism — events that often intersect with political issues — communications teams must carefully consider the language and stance in the organization's statements to avoid negative public backlash.

"We activated the crisis management team for a severe weather storm event this year. We knew from the weather forecasts it was coming, and we planned beforehand, but the wind was exceptionally high, and we had to suspend non-essential working operations."

CEO, private sector, UAE

"We dealt with storm flooding which led to a number of people being left homeless and a number of business locations being unable to operate. It had an impact across more than one area of our business. We have also activated for civil unrest or conflict."

Head of Risk & Assurance, Private Sector, South Africa

"Triggers that result in a major incident potentially being declared for our organisation often relate to systems because we provide digital services, but common triggers could include supply chain, industrial action, or cybercrime incidents."

Head of Civil Contingencies, public sector, UK

What was the cause of activation of crisis management teams within your organizations over the last 12 months?

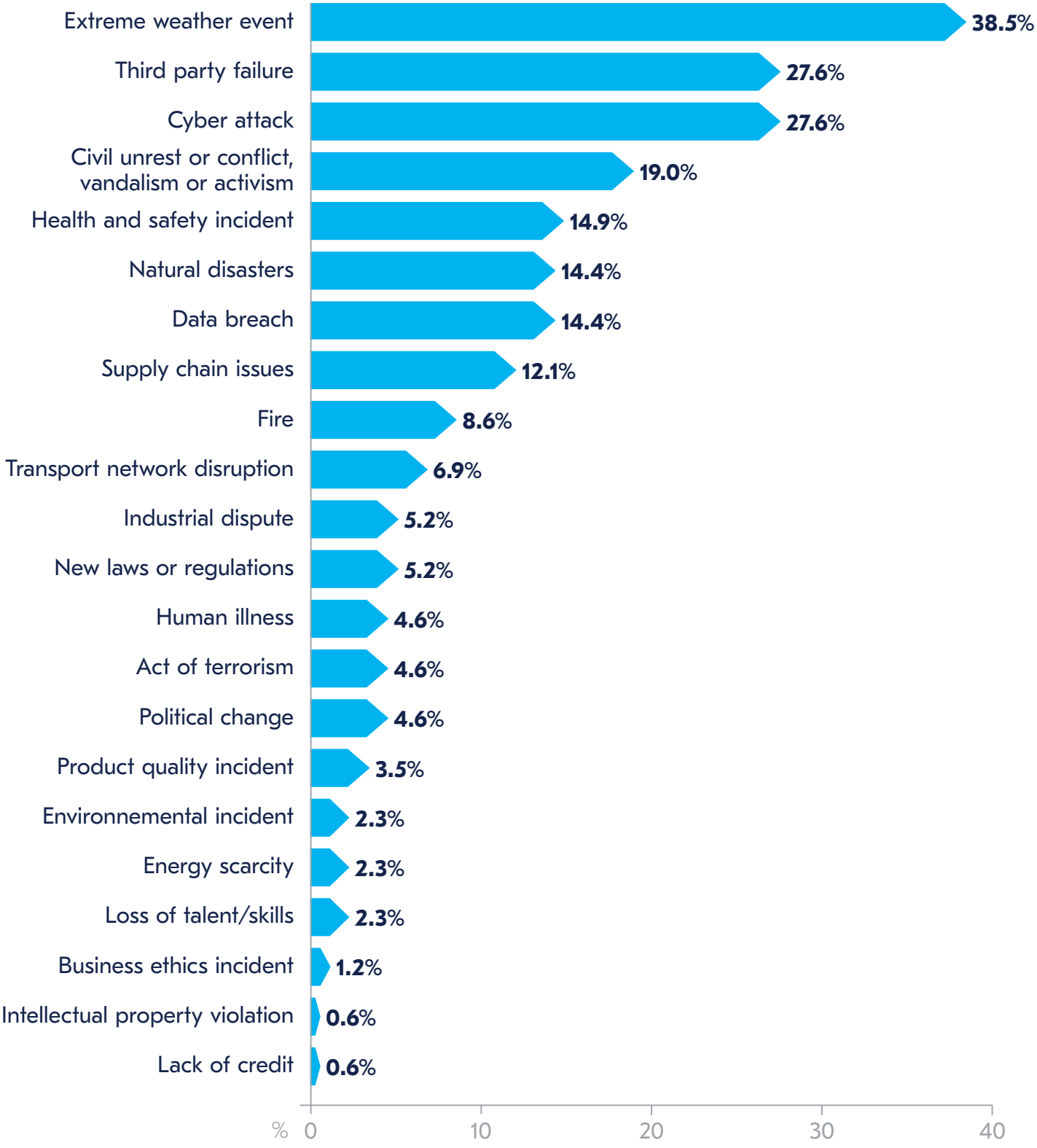


Figure 2. What was the cause of activation of crisis management teams within your organizations over the last 12 months?

The 2024 report, like the 2023 edition, highlights the different approaches to crisis management in response crises. Over the years, professionals have shown a preference for centralised crisis management structures, which was confirmed by 45.9% of respondents (2023: 44.9%). In contrast, only a small fraction of participants rely on regionally-led (7.1%) or business unit-led (6.5%) crisis management teams. The preference for centralised approaches is driven by several factors, including alignment with international best practices. According to ISO standards like ISO 22361, clear and direct decision-making is crucial, and a centralised team can provide employees with unambiguous directives to follow[4].

However, an increasing number of organizations (38.8% in 2024 vs 35.2% in 2023) effectively combine a centralised approach with a business unit or regional led structure, highlighting that the combination approach is becoming the universally recognised best practice. This hybrid model is particularly useful for organizations operating across diverse geographical areas, as it allows for better visibility into specific events and more timely information gathering. This approach is consistent with international best practices, which advocate for a top-down structure while recognising the need to delegate when appropriate. For example, while a centralised team might handle relations with large media outlets, technical measures to restore continuity can be managed by tactical or operational teams under the supervision of the crisis management room.

The organizational structure of a company also influences its crisis management approach. For instance, a large international group may have different legal entities in various countries, each with its own structure, management, working culture, and crisis management committees. In such cases, local management decides whether to escalate an event to the group level. As one respondent noted, "All crises are managed locally through a crisis management group, during which escalation levels are determined based on the risk level and the potential expansion of the risk to include additional SMEs. Escalation can then occur at the regional or group level."

"Currently, we operate with six regional crisis management teams which are supported at a strategic level by a national crisis management team. Ideally, this crisis management model will evolve into a broader operational resilience model, adopting a more holistic approach that combines risk management, emergency management, and business continuity management."

Senior emergency manager, health sector, Ireland

"Our business is global and split into three distinct operations for management purposes. Each of the three has its own management team and in the event of an incident the local team will handle the incident with support from the head office specialist functions."

Head of risk & assurance, private sector, South Africa

"We manage crises via a centralised and decentralised approach because we are a big, geographically dispersed, organization with different lines of business and many offices. We have a hierarchy of escalation procedure based on clear criteria."

Head of civil contingencies, public sector, UK

"We have regional hubs that manage minor incidents themselves and then major incidences or major national incidents are managed centrally."

BC and incident manager, public sector, UK

There is another reality that was explained by an interviewee, where the level of dependency on third party providers means that the organization loses control over its crisis response. In these occasions it is important it is to work with suppliers, so a crisis can be managed in partnership with them rather than delegating complete control.

"Most of our company is outsourced to third parties, so we don't have 100% control over a crisis response."

Business resilience manager, aviation, Hong Kong

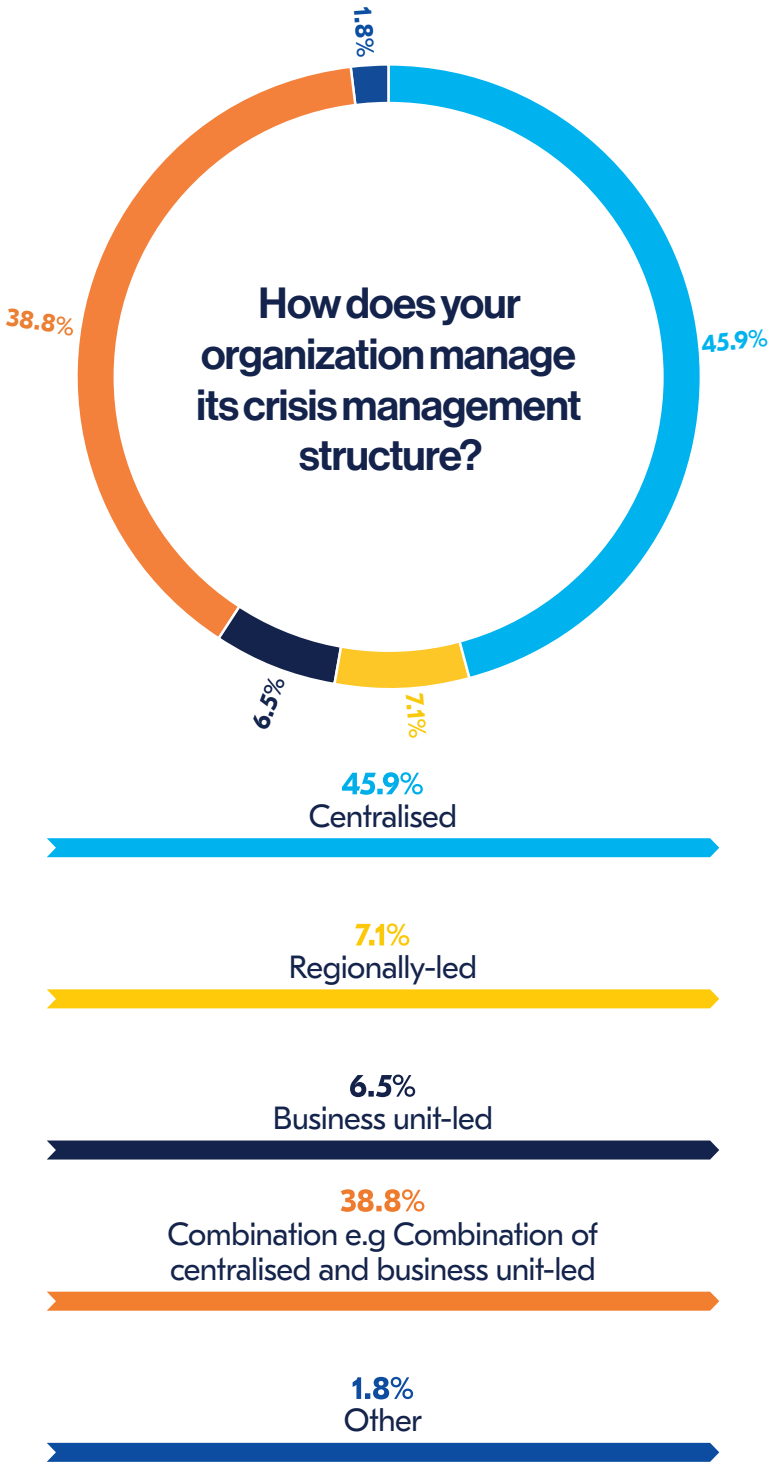


Figure 3. How does your organization manage its crisis management structure?

The data also reveals that current crisis management strategies are proving successful. The majority of participants (72.4%) rated their crisis management capabilities as either excellent (22.4%) or good (50%). This marks an improvement over 2023, when only 61.1% of respondents were satisfied with the effectiveness of their crisis response capabilities.

A good crisis management strategy involves input and collaboration between multiple departments. In this light, an interviewee highlighted the importance of good human resources when articulating a crisis response:

"The capability of people that are employed in crisis management roles is huge factor in determining the effectiveness of the team and the response. Not everybody is suited to crisis management, and sometimes people can end up in roles without having gone through appropriate training or exercising or developing the necessary subject matter expertise."

Head of civil contingencies, public sector, UK

Figure 4. How effective do you believe the crisis management capabilities are within your organization?

The report surveyed respondents on specific positive and negative aspects of their current crisis management capabilities. Positive aspects echo some of the previous findings in this section, regarding the unpredictable nature of crises, which can be the result of several different events. Therefore, organizations need agile teams with diversified skills that can respond quickly at an operational level while preserving the reputation of the organization.

Participants also value the inclusion of external communications and PR in the response (88.7%) even more than they did last year (80.0%). Managing crisis communications is a delicate task, which can help save an organization from a crisis, but it might also sink it deeper if not handled correctly. Current issues such as disinformation and the problem of misinformed individuals leaking out incorrect messages on social media should be especially addressed during a crisis. This has been the case of Singapore Airlines, which showed significant improvement in managing crisis communications during the unfortunate incident suffered by one of their commercial aircrafts in 2024[5].

A good PR response: the case of Singapore Airlines

In 2024, Singapore Airlines faced a significant PR crisis when one of its flights encountered severe turbulence, resulting in injuries to passengers and crew. The incident quickly became the focus of intense media scrutiny, challenging the airline's crisis management and communication strategies. Singapore Airlines responded with urgency by activating its crisis communications team, which played a vital role in managing the situation effectively.

The airline promptly issued a public apology, expressing deep concern for the wellbeing of those affected. This initial response was crucial in demonstrating empathy and responsibility, which helped to mitigate the potential damage to the airline's reputation. In addition to the apology, Singapore Airlines maintained clear and consistent communication with passengers, the media, and the public. Regular updates were provided on the condition of the injured, the investigation into the incident, and the steps being taken to enhance safety measures. The airline also engaged directly with affected passengers, offering medical assistance, compensation, and ongoing support throughout their recovery.

This response marked a notable improvement compared to how Singapore Airlines had handled crises in the past. Previously, the airline had faced criticism for delayed communication and a lack of transparency, which often led to increased public concern and negative media coverage. In contrast, the 2024 incident demonstrated that Singapore Airlines had learned from these past challenges. The speed and clarity of their communications, coupled with proactive engagement, showcased a more refined and effective approach to crisis management.

By swiftly addressing the incident, providing immediate support, and maintaining transparency, Singapore Airlines not only managed the crisis more effectively but also strengthened public trust. This incident underscored the airline's commitment to prioritising safety and customer care, highlighting significant improvements in its crisis management capabilities[6].

A significant subset of respondents prioritises the importance of teams that can be mobilised quickly (88.7%). Reducing reaction times is the result of training and rehearsing the resilience muscle memory of an organization. This requires investing time, energy, and budget in activities such as awareness initiatives, workshops, and different types of exercises. According to the ISO 22361[7] standard, crisis management is not a one-phase activity, but it evolves through an entire lifecycle. Before the response is even activated, there are four fundamental phases to consider: this starts at anticipation and moves on to assessment, prevention, and preparedness. This last component is key to swift action during a high-stress event such as a crisis; therefore, it is of primary importance that personnel have tested their reactions in a simulated environment and learn how to improve.

"The crisis management team in my organisation can be mobilised quickly because a core team is always on duty. In addition to that, there is also a surge pool of trained people that can be used to augment the core team, which provides extra resilience for a crisis or lengthy incident."

Head of civil contingencies, public sector, UK

"Mobilisation is straightforward. We notify our various crisis management teams of a sudden onset or emergent situation and convene a CMT meeting. Senior leadership are well versed in activation processes as we run drills and exercises."

Senior emergency manager, health sector, Ireland

"Because we are quite a small organization, I can very quickly draw on resources and people and mobilise very quickly."

BC and incident manager, public sector, UK

> **"We do a lot of work and exercising with our senior crisis management team so that when something is about to happen, or it happens, they are already well versed in what to do. The senior team has a lot of experience, and they have learned a lot through regular exercises."**
>
> CEO Private sector, UAE

Unfortunately, many companies overlook the importance of crisis management training and drills, even when they invest significantly in business continuity. Under stress, people often revert to old, ineffective habits, making training essential to ensure better responses during a crisis. Common mistakes due to insufficient training include dominant individuals sidelining others and ignoring the crisis management plan, teams focusing on tactics over strategy, forgetting key priorities, losing situational awareness, and failing to document critical information and actions. These issues highlight the widespread mismanagement that can occur during a crisis, with many, including high-level executives, struggling to effectively handle the situation[8].

Further down the chart, concerns for staff health and safety (86.4%) drop to third place compared to last year, but they have a higher consideration in percentage terms compared to 2023 (76.5%). Health and safety concerns rose to the top of the agenda during the COVID-19 pandemic, a trend that has been confirmed through the years, despite some slight variations. Health and safety issues can be the outcome of malpractice within an organization and through its supply chain. For instance, Adidas America faced nearly $400,000 in fines for safety violations at a New York warehouse according to an announcement by the Occupational Safety and Health Administration (OSHA). The penalties are the result of a 2021 inspection that identified hazards, including a lack of guardrails and an unsafe ladder, which put employees at risk of falls up to 10 feet. When OSHA reinspected the facility in early 2024, it found that these safety issues had not been corrected[9].

Participants also highlighted the need for their crisis management teams to be able to adapt quickly to a rapidly changing scenario (82.1%). This is consistent with the idea of having agile teams that can react to sudden developments within crises. A review of the crisis management capabilities of Singapore's government published on The Lancet provides an interesting case study on how to handle rapidly evolving crises such as a disease outbreak. According to the researchers, in this particular case a centralised approach proved to be a success factor in the response since it the team was able to better collaborate and take the necessary steps[10]. It is worth noting that as a crisis develops, coordination and collaboration are essential, as decisions often need to be made based on incomplete information. It is crucial that the decision-making process of the crisis management team is justifiable and reasonable, even in hindsight, based on the information available at the time. This approach ensures that decisions are grounded in facts rather than speculation.

How much do you agree/disagree with the following positive criteria applied to your crisis management processes?

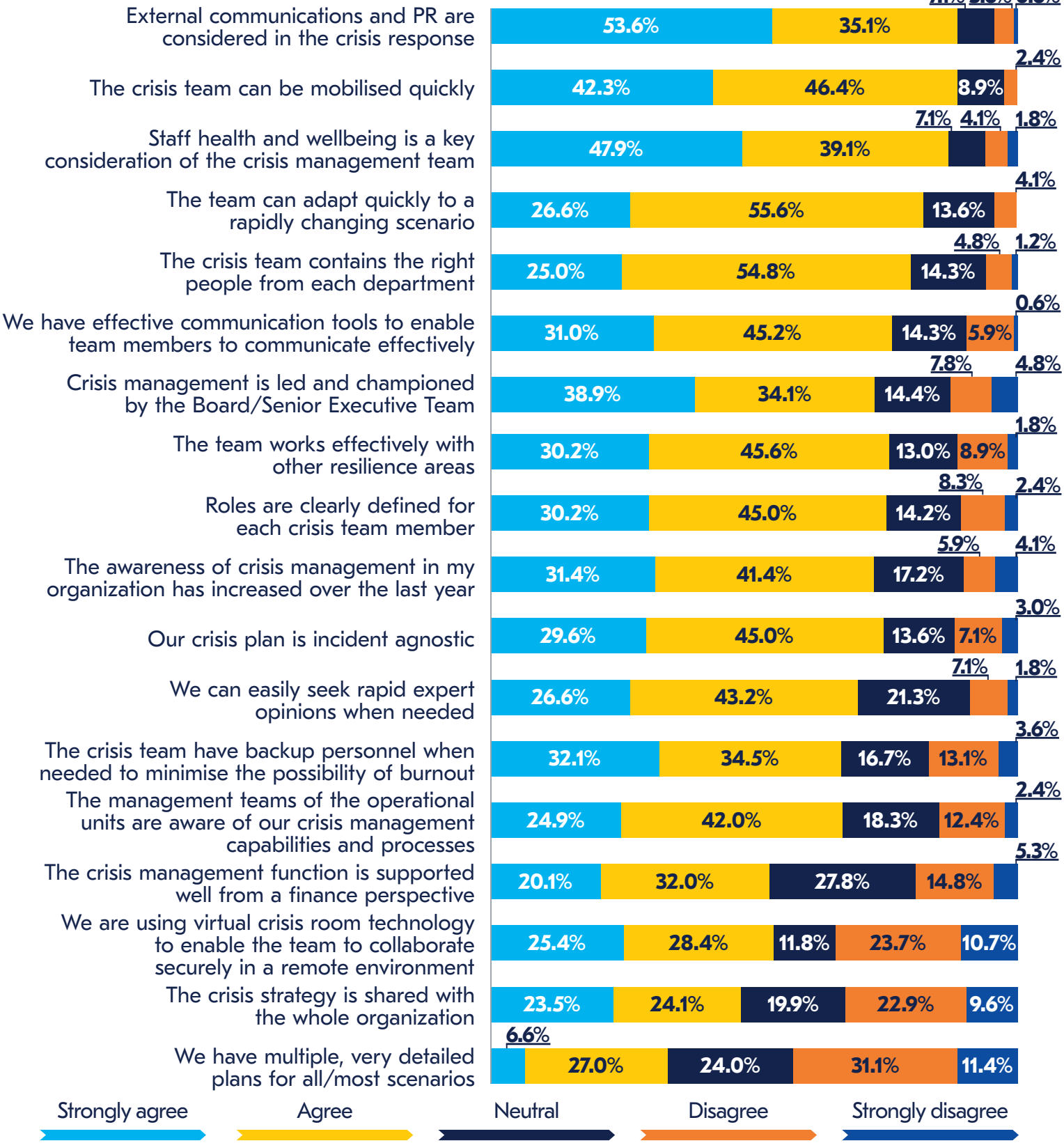


Figure 5. How much do you agree/disagree with the following positive criteria applied to your crisis management processes?

When asked about the shortcomings of their crisis management processes, respondents identified their primary concern as staff being unaware of crisis plans, which could lead to confusion during a crisis (30.1%). This concern aligns with last year's findings, where it ranked second, and it highlights the ongoing threat posed by a lack of internal awareness. Even in a centralised crisis management structure, every employee plays a crucial role. For instance, while there might be an appointed spokesperson, the rest of the workforce must avoid divulging any details about an ongoing event. Additionally, each staff member may encounter early warning signs of a disruptive event that could escalate into a crisis, making it essential that escalation procedures and reporting protocols are effectively communicated.

In this context, it is concerning that the second-highest issue reported by participants is that crisis plans are not adequately shared across the organization (30.1%), which contributes to the overall lack of awareness.

> **"In the past we've had issues with siloed teams, which can lead to duplication of effort and inadequate shared situational awareness."**
>
> Head of civil contingencies, public sector, UK

While it might not be feasible to share entire plans due to confidentiality reasons, a successful response can only happen by ensuring every person in the organization knows what to do in a crisis, who they should collaborate with, and know which procedures to follow.

Moving further down the list, respondents expressed concerns about the composition of the crisis management team, particularly regarding rotation and training. According to 25.1% of professionals, crisis management team members are not changed frequently enough. This raises important questions about the rationale for rotating team members, a topic that has rarely been debated. An interviewee explained that since COVID they have started rotating personnel in order to avoid exhaustion:

> **"We learnt during COVID to break responders down into team to avoid burnout. It is part of our process to start looking at people after 8 hours."**
>
> CEO, private sector, UAE

> **"The crisis team has backup personnel to avoid burnout. We alternate three to four people in rotation because we potentially deal with 24/7 crises."**
>
> Business resilience manager, aviation, Hong Kong

International guidelines emphasise that individuals should not be included in crisis management solely based on their role, but should be selected only after receiving appropriate training. Also 16.4% of respondents highlighted the risk of burnout among crisis management team members as a pressing challenge bringing attention to the growing relevance of mental health in crisis management, especially given the increasing frequency and diversity of crises worldwide.

This point opens up further discussion, particularly on the value of leveraging different expertise based on the nature of the crisis. Past BCI research on crisis leadership[11] has suggested calling upon external experts if the necessary skills are not available in-house, but this data highlights the need for broader industry discussions.

Similarly, 27.0% of respondents believe that crisis management team members are not sufficiently trained. This is a critical issue, as crisis management skills should not be improvised.

"If there was investment in training, education, and exercising of a broad range of staff at key stages in their career, this could improve the organizations' ability to identify and respond effectively to a BCM issue, thus reducing the likelihood that it will escalate into a full-blown crisis. I think that, over time, such an approach could add huge benefits in terms of operational resilience and could minimise disruptions to the delivery of health services. This approach could be broadened out to the wider civil and public service."

Senior emergency manager, health sector, Ireland

"Our challenges are engagement and understanding from our executive leadership team and understanding what a crisis is, what isn't a crisis, and the scope of how our reaction within our plans works. We are proposing to put in place changes that will bring more accountability to senior leaders."

BC and incident manager, public sector, UK

How much do you agree/disagree with the following negative criteria applied to your crisis management processes?

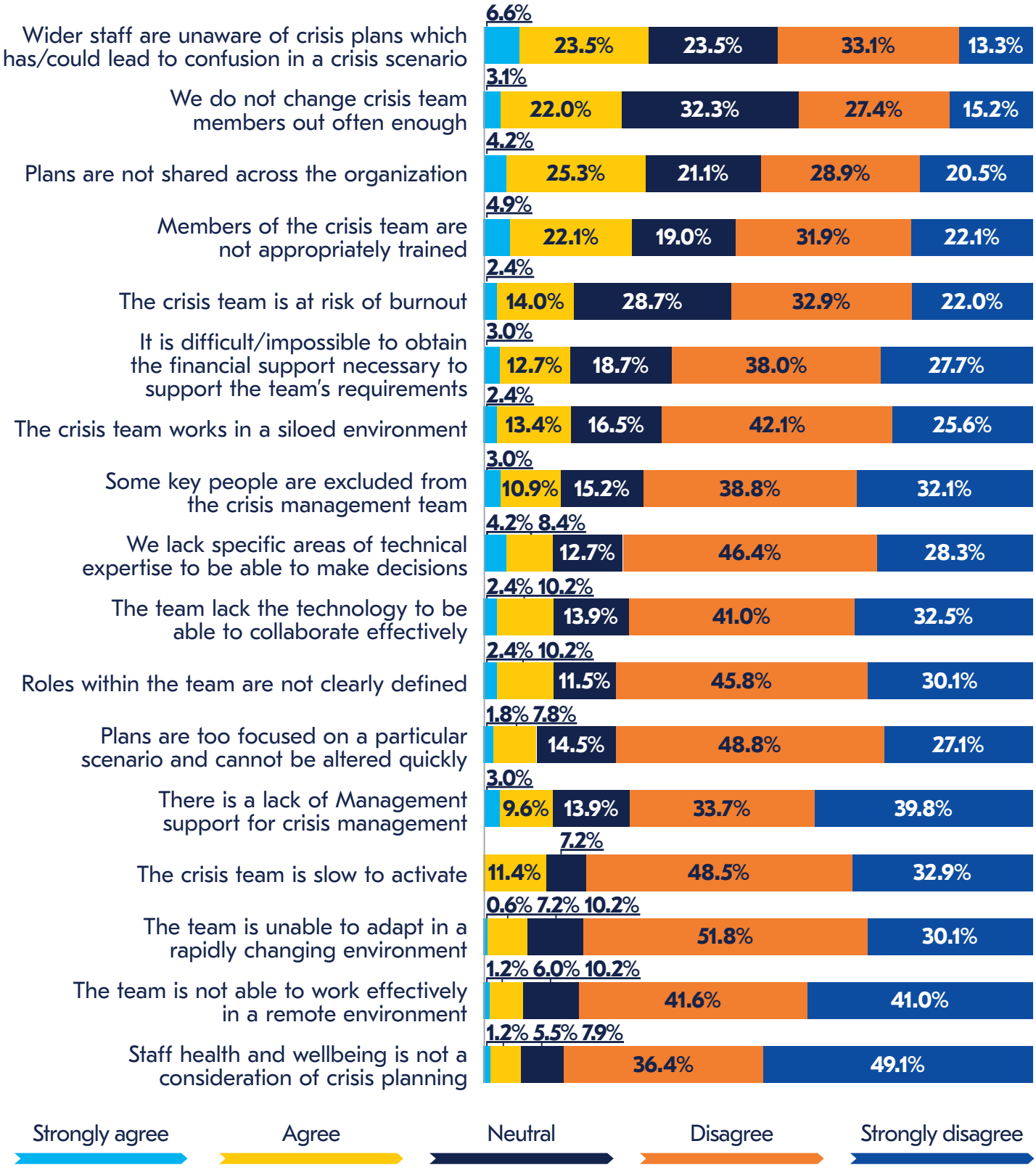


Figure 6. How much do you agree/disagree with the following negative criteria applied to your crisis management processes?

2

Collaboration in a crisis

Collaboration in a crisis

- Organizations report a good synergy between the BC and crisis management functions. However, remains room for improvement, particularly in the training and preparedness of crisis management teams.
- The level of involvement of top management in crisis management varies, with some organizations involving executives throughout the process, while others preferring selective involvement, balancing the need for strategic leadership with the flexibility of team operations.
- There is a need for cross-functional collaboration within crisis management teams, particularly in handling complex crises like cyber-attacks, where expertise from multiple areas is essential for an effective response.

Crisis management report have documented the evolving relationship between BCM and crisis management. Past reports have underlined areas for improvement in defining the synergy between the two, which may at times create confusion within organizations. Broadening the perspective on this discussion, it is useful to observe that emerging — and binding — regulations in recent years such as the UK FCA/PRA/Bank of England operational resilience policy and the EU Digital Operational Resilience Act (DORA) have been pushing for an integrated, holistic approach to resilience. This approach strongly encourages cooperation between BCM and crisis management, extending its reach also to other management disciplines such as risk management and security. Therefore, moving forward it would be reasonable to expect greater integration to align with the direction chosen by regulatory actors.

Interviewees explained different dynamics in the relationship between business continuity and crisis management functions within organizations.

> **"Currently business continuity leadership tends not to be actively involved in in the crisis phase, but that's changing and we're developing more a one team, end to end approach to resilience."**
>
> Head of civil contingencies, public sector, UK

> **"We used to have a designated lead person for business continuity, but that has evolved into a business continuity/ crisis management/operational resilience remit. In the future, we aim to have business continuity as a pillar within the resilience and crisis management areas."**
>
> BC and incident manager, public sector, UK

> **"A current area of focus is defining when a crisis is no longer a crisis. We have clearly defined triggers for crisis team activation, but not necessarily for business continuity and transitioning back to business-as-usual."**
>
> Head of civil contingencies, public sector, UK

Based on standards and good practices[12] such as the BCI GPG, BCM contributes to the crisis management process in several ways. First of all, it is not uncommon for the BC manager to provide training and awareness sessions to different teams at all levels, including strategic, tactical and operational ones. Also, the BCM team often contributes to the setup of validation activities, such as exercising and testing, which, in high level simulations, require the involvement of the crisis management team. Lastly, the BC manager often has a seat at the crisis management table. This year there seem to be indication that there is a more fluent and collaborative relationship between BC and the crisis management team, overcoming historic tensions. Interviewees explained how having several functions working together improved the crisis response:

> **"We have risk, business continuity, and crisis management in the same space. Having that line of sight and collaboration between functions has made crisis management easier."**
>
> Head of Risk & Assurance, Private Sector, South Africa

> **"In the past, responses have been focused on crisis management, whereas we've now brought in business continuity, so that we're not just looking at the immediate response."**
>
> CEO Private sector, UAE

> **"We run crisis management and business continuity exercises together. One of the objectives is to see at what point the incident commander should activate the business continuity plan."**
>
> CEO Private sector, UAE

This is reflected in the figures in this report, where participants were asked to estimate the effectiveness of the relationship between Business Continuity Management (BCM) and Crisis Management. On a scale ranging from "Not effective" (0) to "Very effective" (100), the average response was 73.4, representing a slight increase compared to 2023. A similar scale measuring the extent of BCM's involvement in Crisis Management, from "Not involved" to "Very involved," yielded an average value of 73.8. Overall, the data indicates that organizations are experiencing a strong synergy between BCM and crisis management, continuing a trend that has remained consistent over the years.

How effective is the relationship between Business Continuity and Crisis Management within your organization?

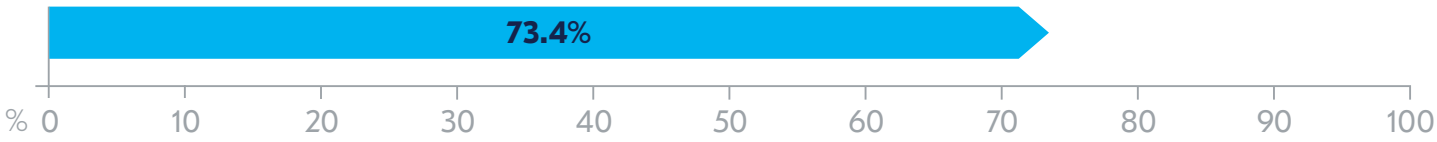


Figure 7. How effective is the relationship between Business Continuity and Crisis Management within your organization?

The overwhelming majority of respondents (90.5%) reveal that their team's ability to interact with other functions, as well as a network culture, is a key solution to successfully navigating a crisis. A sound crisis management team will benefit from flowing conversations and meaningful discussions across the table, which should feature representatives from key areas of the organization. This is especially true considering the increasing complexity of current crises.

For instance, should a large-scale cyber-attack occur, there will be need for different types of expertise. First of all, those responsible for the IT systems, cyber security, and information security will have to brief the room on the status of the infrastructure and the details of the attack with the information available at the time. In addition, there should be legal experts to illustrate the possible penalties and notification duties to different regulators, such as the Data Protection Officer in the case of the EU GDPR. Moving to the reputation aspect, the nominated spokesperson will have to address the media backlash from a potential loss of data or even data theft in the worst-case scenario. This is only one example of the type of complexity that surrounds a crisis, and it may apply to many other crisis drivers such as third-party failure or health and safety incidents, where events are not linear but have multiple different angles that require a cross-cutting approach to manage.

An interviewee highlighted the importance of counting with subject matter experts during a crisis, while another emphasised the importance of having a close-knit, highly collaborative, team.

"Everyone is really keen to get involved so our engagement when we have to call on subject matter experts to help manage incidents has been really good."

BC and incident manager, public sector, UK

"Because we are a small team, we work very closely together and feel comfortable talking to each other. This means the team has the practice of interacting with other functions, making it easier to navigate a crisis."

Business resilience manager, aviation, Hong Kong

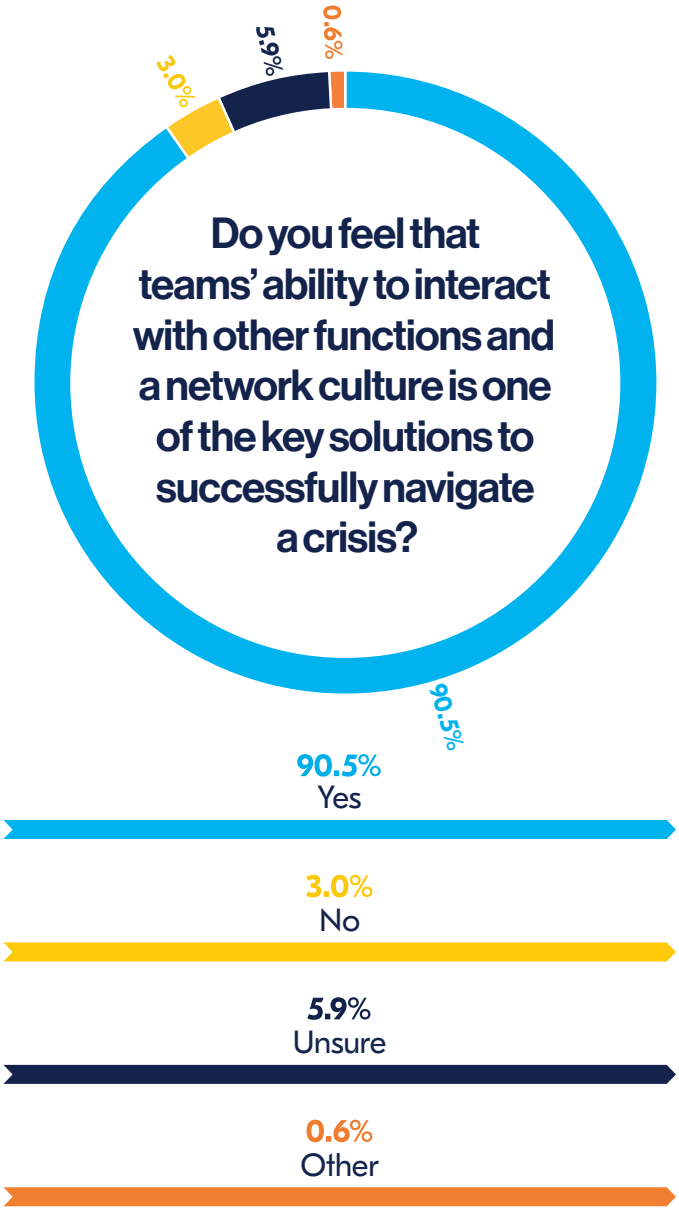


Figure 8. Do you feel that teams' ability to interact with other functions and a network culture is one of the key solutions to successfully navigate a crisis?

The average levels of training across the crisis management team (68.3%) are not as high as expected. To excel in a crisis, companies need to prepare in advance by conducting mock disaster exercises. Planning these exercises is a complex task that requires careful consideration to avoid potential pitfalls. The process begins by reviewing any disaster scenarios that have been used in the past. Reusing a previous exercise can be beneficial, especially if it exposed significant gaps that need reassessment. However, it is crucial to ensure that any unresolved issues from past exercises are addressed to prevent them from recurring.

An interviewee highlighted how the experience during COVID-19 served as practice for future crises, stressing the importance of training:

> **"When a cyber-attack occurred, the capacity and the ability of our crisis management teams to respond quickly was superb because they had been operating in crisis mode for the previous twelve months while directing the response to the COVID-19 pandemic."**
>
> Senior emergency manager, health sector, Ireland

What percentage of your crisis team members have received training in crisis management?

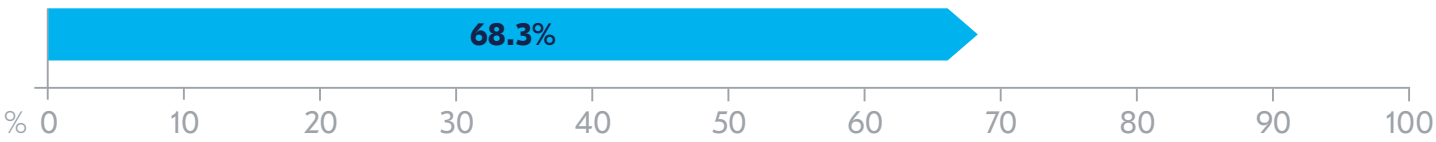


Figure 9. What percentage of your crisis team members have received training in crisis management?

"We do one or two simulations a month. We will start in the area where an incident may occur, and the branch out effects indicate who has got to learn. It is important because it installs muscle memory around what to do in an incident. In the past, we would have invoked a serious incident team for regional events, but today we won't need to because our plans are so well rehearsed everyone knows what to do."

Head of Risk & Assurance,
Private Sector, South Africa

The complexity of the exercise should align with the maturity of the team involved. Less experienced teams should start with basic scenarios, while more seasoned teams can handle complex challenges. Defining clear objectives is essential; the focus should be on a core set of goals, such as testing documentation or evaluating team readiness. Engaging subject matter experts is also vital. These experts, whether from within or outside the organization, can provide valuable insights to help design a realistic and effective scenario[13].

Collaborating with experts to refine the scenario ensures that it meets the exercise's objectives and is free of flaws that could undermine its effectiveness. The scenario should be realistic, reflecting plausible real-world situations rather than fantastical or exaggerated events. A detailed timeline and list of events should be developed, considering the team's maturity when determining the duration and response times[14].

The scenario should be continuously refined through a process of drafting and revision, incorporating feedback to improve its effectiveness. Selecting the right facilitator is critical; this person should be knowledgeable about the scenario and capable of guiding the team without overdirecting. These steps might help organizations to create a realistic and challenging exercise. Some practitioners are now using artificial intelligence (AI) to help generate scenarios which are personalised to the type of incidents an organization may face. It can also create complex "what if" scenarios to help fully engage staff who are taking part in the exercise. This preparation of ensuring the scenarios are relevant, engaging, and to the point helps to fully engage teams and, ultimately, will lead to a better response in a crisis. Interviewees explained their situation in regard to training.

"I would like to see an opportunity for crisis management training and education embedded along the career path as part of employee's professional development. Our senior leadership team is extremely busy on a day-to-day basis. That limits the time available to provide training. However, when we do run exercises, they always provide positive feedback and look for more training opportunities. It would be better if such training opportunities were available at earlier stages of their careers and could be mandatory for certain junior and mid management roles."

Senior emergency manager,
health sector, Ireland

"We are a very lean organization and workforce is limited so I can only train limited amounts of people each year. People are required to do training, it is obligatory. However, it is difficult for them because they still need to take care of day-to-day business."

Business resilience manager, aviation, Hong Kong

"Our top decision makers come from a variety of sectors and functions, so the level of formal crisis management training they have had over the course of their career can vary."

Senior emergency manager, health sector, Ireland

To what extent does business continuity become involved in the strategic response in a crisis?

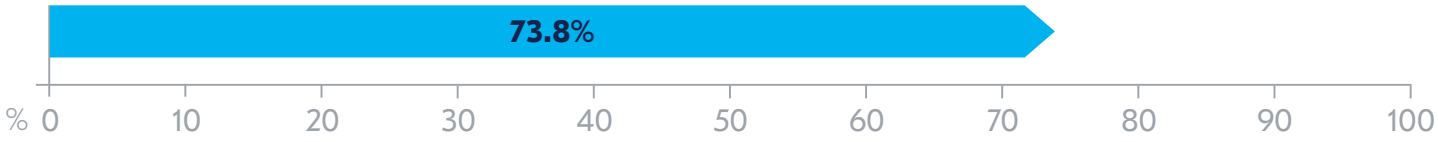


Figure 10. To what extent does business continuity become involved in the strategic response in a crisis?

Top management commitment is a key aspect of crisis management. It is often the case that members of the executive team will be actively involved in managing crises, due to their position within the organization. In 31.0% of the organizations surveyed, senior management is involved all along the process, taking a controlling role until the final decision, which is a slight decrease from last year (39.6%). However, a larger number of organizations prefer involving executives at points during the process and in the final decision (44.6%). As highlighted in the 2023 report, there are cases where management relies on other members of staff to coordinate or direct the crisis management team. This approach may leave other members free to voice their opinion without the pressure of having to immediately report to those with a higher profile within the organization. However, it is important to strike the right balance because this should not happen at the expense of leaving executives out of the loop on key decisions where their expertise is vital. Lastly, one in five participants (18.5%) report involving senior management both at the beginning and end of the process (8.3%) or only at the end (10.1%) for validation.

"The incident response team is made up of a core group of senior executives and then we call co-opted team members depending on the nature of the incident. The senior executive team are involved in all the processes of decision-making during a crisis."

Head of Risk & Assurance,
Private Sector, South Africa

"We have hands-on people who fix problems, but senior management will take care of the bigger picture like reputational damage and media strategy."

Business resilience manager,
aviation, Hong Kong.

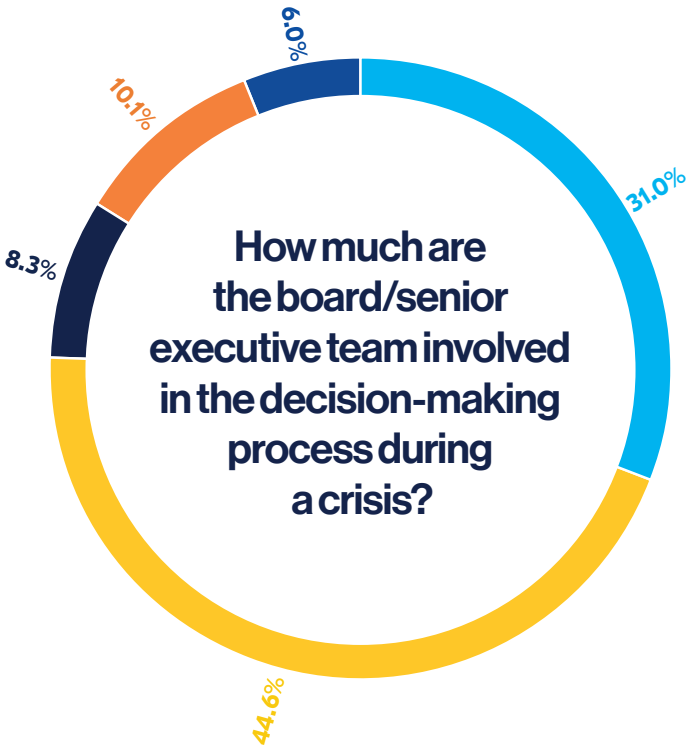


Figure 11. How much are the board/senior executive team involved in the decision-making process during a crisis?

3 Lessons learnt

Lessons learnt

- Many organizations demonstrate a strong commitment to continual improvement by consistently conducting post-incident or after-action reviews (PIR/AAR) after every incident. This regular analysis is crucial for learning from all types of incidents, increasing preparedness and enhancing the response in future crisis.
- Senior leadership is highly involved in post-incident reviews, which suggests a recognition of the importance of strategic oversight in the organization's response and recovery efforts. This involvement ensures that top management's insights and decisions are integrated into the process.
- Business continuity and IT departments play pivotal roles in post-incident reviews, reflecting the critical need to align operational stability with technical expertise. This collaboration is increasingly important as organizations face ongoing challenges from digital threats and other complex crises such as cyber-attacks, misuse of AI, and emerging threats such as deepfakes.

Data on the frequency of conducting post-incident or after-action reviews (PIR/AAR) provides a clear view of organizational practices aimed at ensuring continual improvement. A significant portion of organizations (46.4%) consistently conduct these reviews after every incident. The 46.4% figure is nearly eight percentage points greater than the previous year (2023: 38.7%), and shows a renewed commitment to regular post-incident analysis, some of which was borne out of the COVID-19 pandemic. Some practitioners go a stage further, analysing what could have been the impact of a near miss, helping to further deepen and refine their crisis management actions.

"There's always an after-action review. There is a hierarchy as to who leads on them and the level of detail depending upon the severity and the scope of the incident."

Head of civil contingencies, public sector, UK

Another 36.3% of organizations conduct PIR/AARs, but only for major incidents. This approach indicates a strategic prioritisation, where resources and attention are allocated primarily to larger-scale events that have a more significant impact on the organization. While this ensures that critical incidents are thoroughly analysed, it might miss opportunities to learn from smaller incidents that could reveal important trends or vulnerabilities. Similarly, organizations that conduct reviews "sometimes" (8.9%) or "only occasionally" (4.2%) risk missing key lessons to improve their response capabilities. Crisis management, as any other resilience discipline, should work as a cycle which feeds on experience and reviews. Without embedding lessons learnt, the cycle remains incomplete.

"We conduct post incident reviews for major incidents and incorporate findings into simulations."

Head of Risk & Assurance, Private Sector, South Africa

Overall, the data shows that while a majority of organizations recognise the value of post-incident reviews, there is a varied level of commitment to this practice. Organizations that consistently conduct PIR/AARs are better positioned to improve their resilience and response capabilities, while those with less frequent reviews may need to reconsider their approach to fully leverage the benefits of continual improvement.

"We always review any learnings to improve the company, but it can be difficult when we try to recommend reviewing procedures there may be some resistance. This is often due to limited manpower and needing extra time to implement things."

Business resilience manager, aviation, Hong Kong

"We carry out post-incident and after-action reviews depending on the incident. I think identifying the lessons is easy and distributing those lessons out to people is relatively easy, but ensuring they're implemented and measuring if they have been successfully implemented is one of the challenges we're facing."

BC and incident manager, public sector, UK

"For me, the importance of a robust lessons process is often underestimated, particularly the difference between lessons identified and lessons learned. You have only learned a lesson when an intervention to reduce the likelihood of reoccurrence has been fully implemented."

Head of civil contingencies, public sector, UK

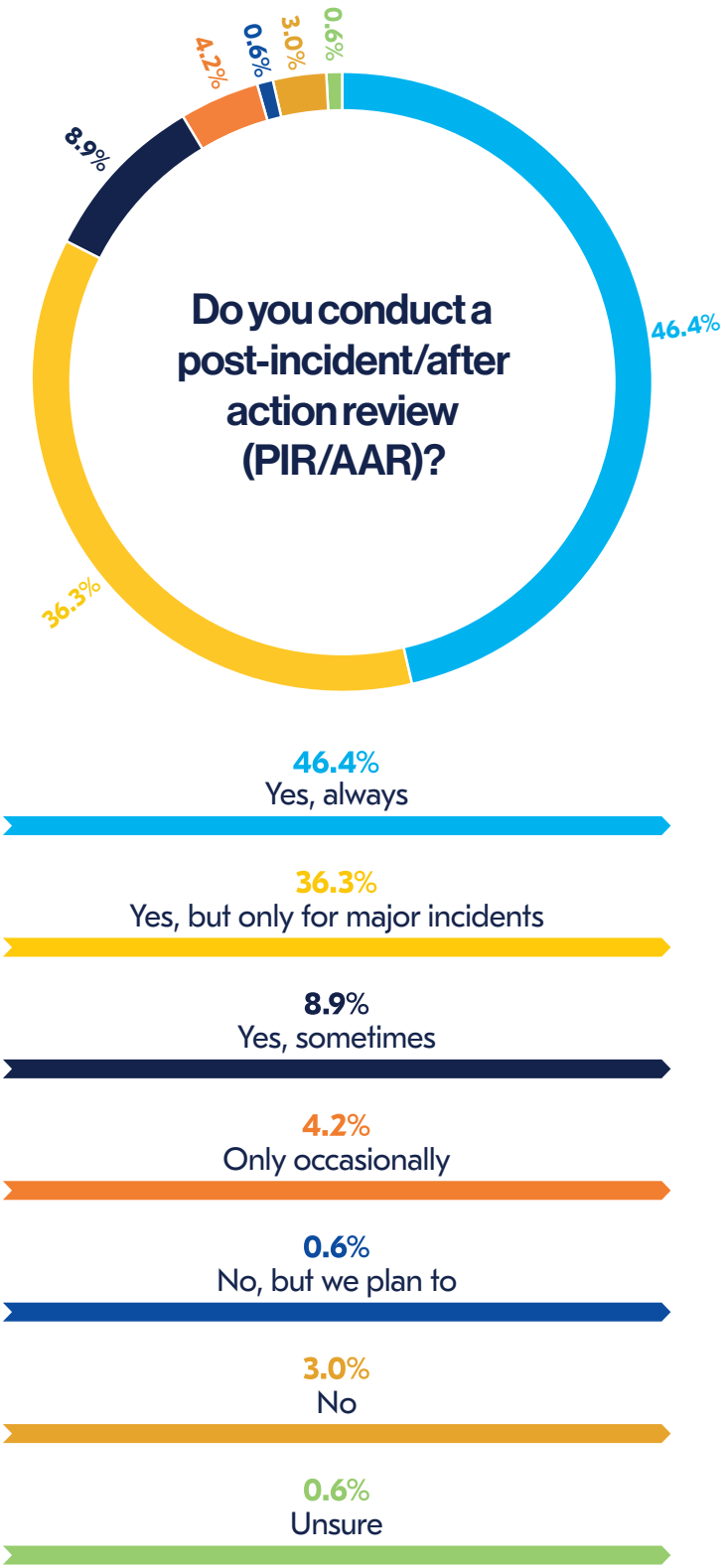


Figure 12. Do you conduct a post-incident/ after action review (PIR/AAR)?

The data on departmental representation in post-incident reviews reveals interesting insights into how organizations prioritise different areas when analysing and learning from incidents. The highest representation is seen in senior leadership, with 79.2% of reviews including executives. This suggests that top management is highly engaged in post-incident processes, a trend that is consistent with last year's findings.

Business continuity and IT departments also have significant representation, both at 74.4%. This reflects the critical role these departments play in maintaining operations and managing technical infrastructure during and after an incident. This is in line with the crisis drivers analysed previously, which featured cyber-attacks and IT incidents among the main concerns for organizations. The connection between digital threats and business continuity has evolved over recent years, to the point that there is now a widespread agreement on the need for BCM team involvement in resolving cyber related disruptions along with the IT and cyber security teams.

The choice of operations and security, represented by 67.6% and 65.8% of respondents respectively, emphasises the importance of having a wide array of skills available to address different types of crises. Having different specialised teams is a recurring theme throughout the report, which starts with the identification of crisis drivers and leads to the need for cross-cutting collaboration across several units. Therefore, the principle of collaboration between management disciplines — expressed in international guidelines and standards — is more relevant than ever.

Interestingly, risk management does not rank in the top five areas of PIR, despite the importance to compare and contrast risk assessment and mitigation strategies with the actual development of a crisis. This is consistent with last year's data, where risk management ranked fourth at 60.5% (2024: 64.0%). Similarly, the communications teams are not being represented as much as their IT and BCM counterparts, with only 62.8% of respondents stating they are part of post-incident conversations.

Other departments that are often not featured in the post-incident review include health and safety at 60.9% representation, human resources at 58.5%, and legal at 55.4%. These low percentages underscore the need to build on current collaboration levels and feature considerations on personnel-related issues and legal ramifications after a crisis.

Digging deeper into the qualitative answers provided by respondents provides a more in-depth explanation of the data. Most respondents state that choosing who to include in a PIR depends on the nature of the event and the teams that were involved. One professional pointed out that they "invite responders who were impacted, and others as needed to the PIR. There isn't a default invite list, as many incidents do not affect all teams across the business. We capture corrective actions during the PIR and assign them to the appropriate business areas, which may include areas not initially invited to the review. All PIR reports are shared with the Operational Resilience Steering Committee." This comment was echoed by another statement: "It depends on the situation. The crisis management team is consistently represented throughout. The post-incident review is shared with the governance group after the incident, where additional areas are represented."

Which departments are represented in a post-incident review?

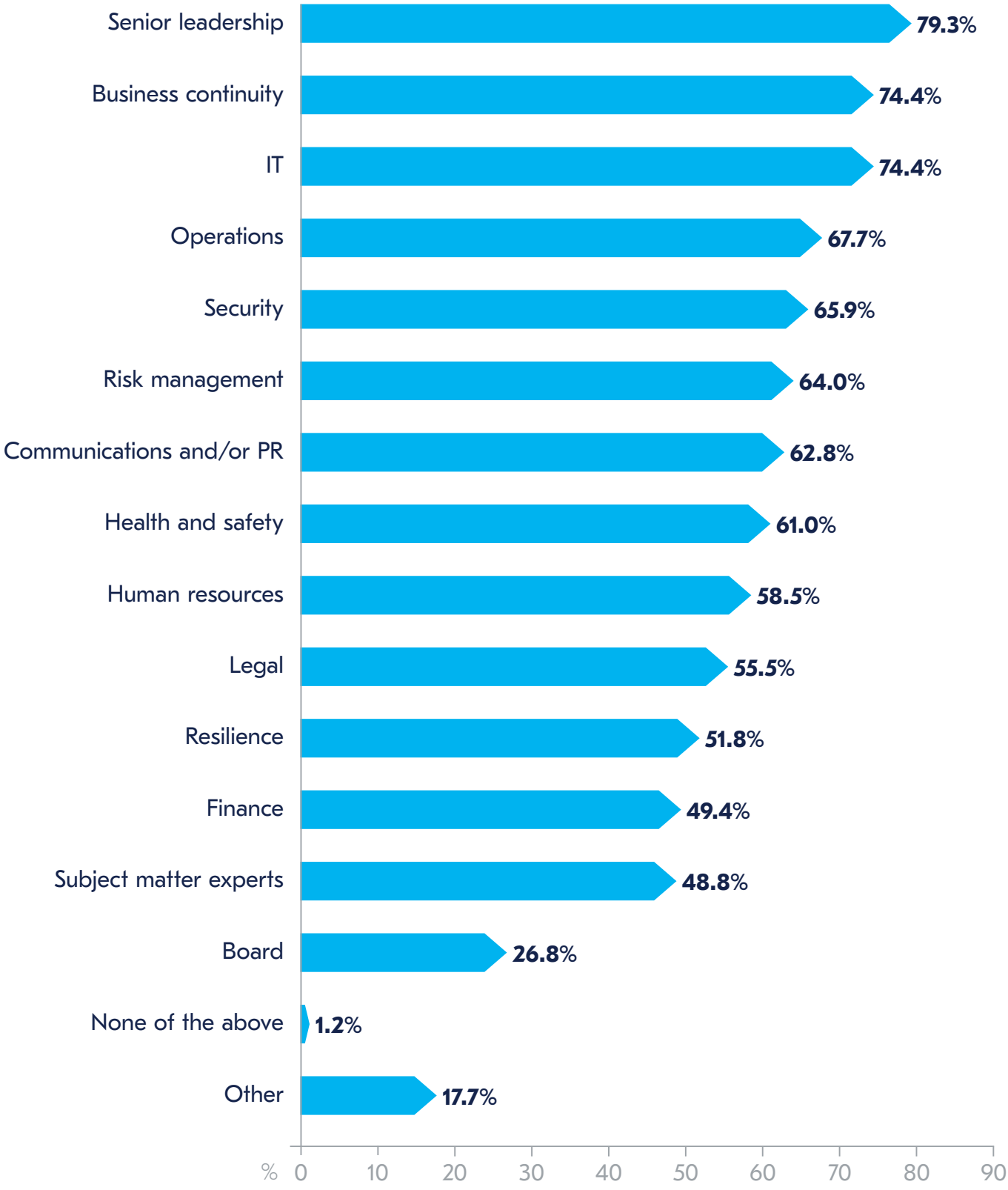


Figure 13. Which departments are represented in a post-incident review?

Technology's role in crisis management

Technology's role in crisis management

- Despite the widespread use of technology, a significant portion of organizations still rely on traditional communication methods like call trees, highlighting their continued relevance alongside modern tools. This balance underscores the value of straightforward communication methods during crises, as well as the need to provide a layered approach to crisis communications.
- The emerging trend of using virtual crisis rooms and dashboards shows a shift towards specialised tools designed to streamline crisis management. These tools are increasingly recognised for their role in enhancing situation control, decision-making, and team coordination, though some organizations remain sceptical or prefer traditional methods due to perceived complexity or cost. There is considerable interest in integrating AI into crisis management, with potential applications seen in data analysis, real-time monitoring, predicting crises, automating response protocols, and scenario generation. While AI is expected to enhance situational awareness and decision-making, concerns about its current performance, biases, and ethical implications highlight a cautious approach to its adoption.

Current data on the role of technology in crisis management reveals a significant uptake of technological tools and systems over the past 12 months. Nearly half of respondents (46.4%) indicate that technology played a major role in their crisis response efforts. The preference for tool dedicated to crisis management confirms a trend that has transformed the discipline through the years. Currently, professionals can rely on cutting-edge digital solutions that leverage advanced communication platforms, data analytics, and automated systems to enhance decision-making and response efficiency.

Another 33.7% of organizations report that technology contributed to some extent, suggesting that while technology is helpful, it may not be fully integrated into their crisis response strategies. These organizations might be using technology selectively or in conjunction with more traditional methods. As in last year's report, despite innovation, there is still room for the adoption of more traditional techniques in crisis management.

A smaller portion, 13.3%, indicated that technology played a limited role in their crisis response, suggesting either a lack of access to advanced technological tools or a preference for manual processes. It might also reflect industries where technology has less applicability in crisis situations. Lastly, 6.6% of respondents stated that technology played no role at all in their crisis response. This group might be operating in environments where technological solutions are either unavailable, underutilised, or deemed unnecessary.

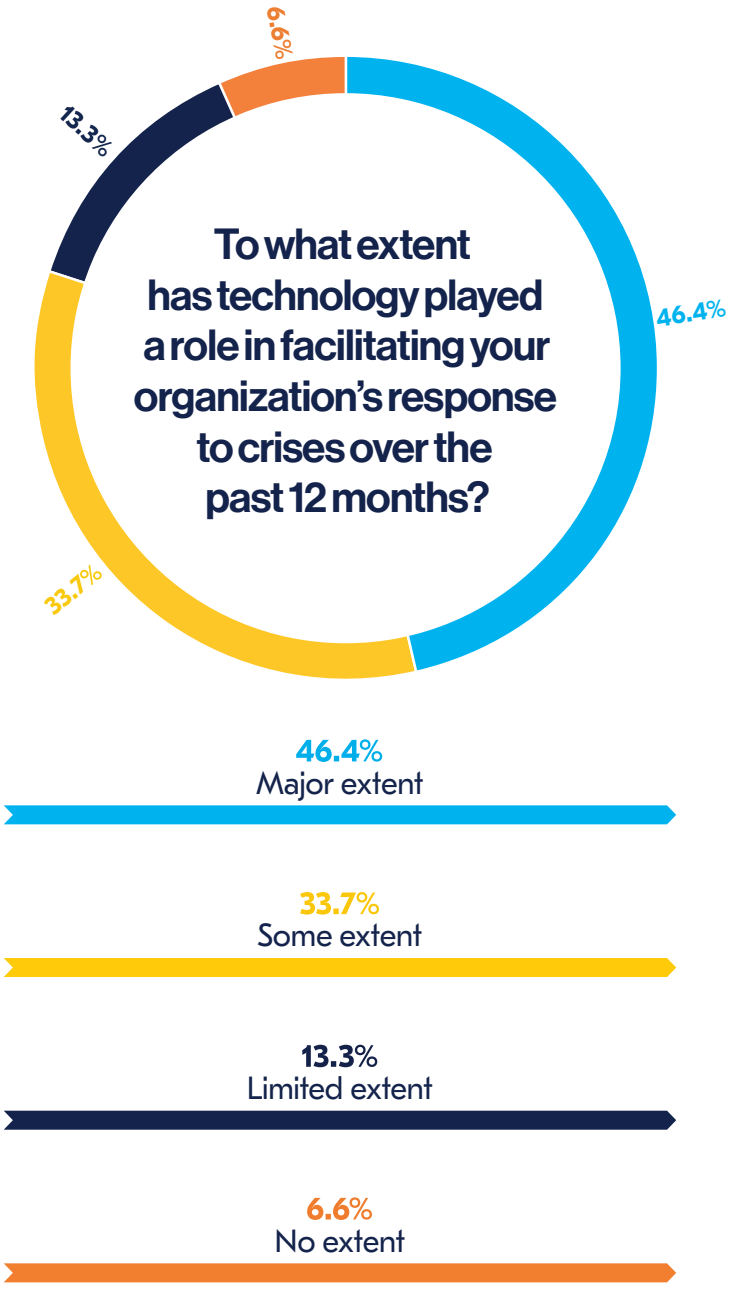


Figure 14. To what extent has technology played a role in facilitating your organization's response to crises over the past 12 months?

The 2024 report highlights once more the trade-off between highly customised on-premises solutions and the more agile and flexible tools that include software-as-a-service (SaaS). This often depends on the size, business model, and financial availability of an organization, since customised software tends to be more expensive and more reliable when considering factors such as network stability and information security. However, having such a vital tool depending on a delimited geographical premise may represent a risk to the organization, since it is more easily subject to physical damage or lack of access. In addition, the increasing uptake of remote work may contribute to a preference for communications tools that can be used on multiple devices and are not strictly connected to one location.

Still, the most popular choice among respondents remains enterprise software (73.7%), confirming last year's trend. This preference for enterprise platforms underscores their critical role in facilitating communication and coordination during crises, supporting the notion that such technology has become an integral part of the crisis management process as well as providing ease of use to users who will be operating software on an interface which is used daily.

"In the past we relied on teleconferences for communication, but we've moved into videoconferencing and using systems such as MS Teams and Webex."

Senior emergency manager, health sector, Ireland

"It is mainly the use of Teams that has enabled us to get the crisis management team together very quickly. We also use WhatsApp for immediate notifications."

BC and incident manager, public sector, UK

Some organizations use free messaging tools in crisis situations and, while some use them in combination with dedicated, secure apps, 48.8% of organizations still use free messaging apps, for their versatility, accessibility, and cost. These apps provide rapid, informal channels for real-time updates, complementing the more structured enterprise solutions.

Still, professionals still value the more traditional methods of communication, such as call trees, which are employed by 44.5% of respondents. Despite the rise of modern digital tools, call trees remain relevant, suggesting a continued value in straightforward, direct communication methods during crises that helps avoid overreliance on a specific tool.

Moving to emerging solutions, virtual crisis room and dashboard technology (25.6%), dedicated crisis management tools, and collaboration apps (both at 22.6%) illustrate the shift towards specialised platforms designed to enhance crisis management efficiency. These tools offer centralised management and improved coordination, aligning with the increasing adoption of tailored technology solutions for emergency scenarios.

Furthermore, specialist apps and social networking sites (each at 22.0%) occupy a more niche but significant role in crisis response. These tools serve specific functions, from targeted communication to broader engagement, reflecting a nuanced approach to integrating technology in crisis management.

Social networking sites should, of course, be used with care as an information source, and verified news sources should be used, wherever possible, to back up information. However, during an unfolding incident, social media feeds can help to provide real time information about how the crisis is unfolding. There are, however, some tools which are continuing to wane in popularity due to changes in the way we work. On-site communication screens, for example, are fading in popularity due to the increasing propensity for remote working. This particular technique has fallen to 22.0% this year, down from 28.5% in 2023. Public address systems have seen an even sharper demise with just 17.1% using it as part of their crisis management technology portfolio compared to 24.7% in 2023

Which tools and technology have you used within the past year as part of your crisis response?

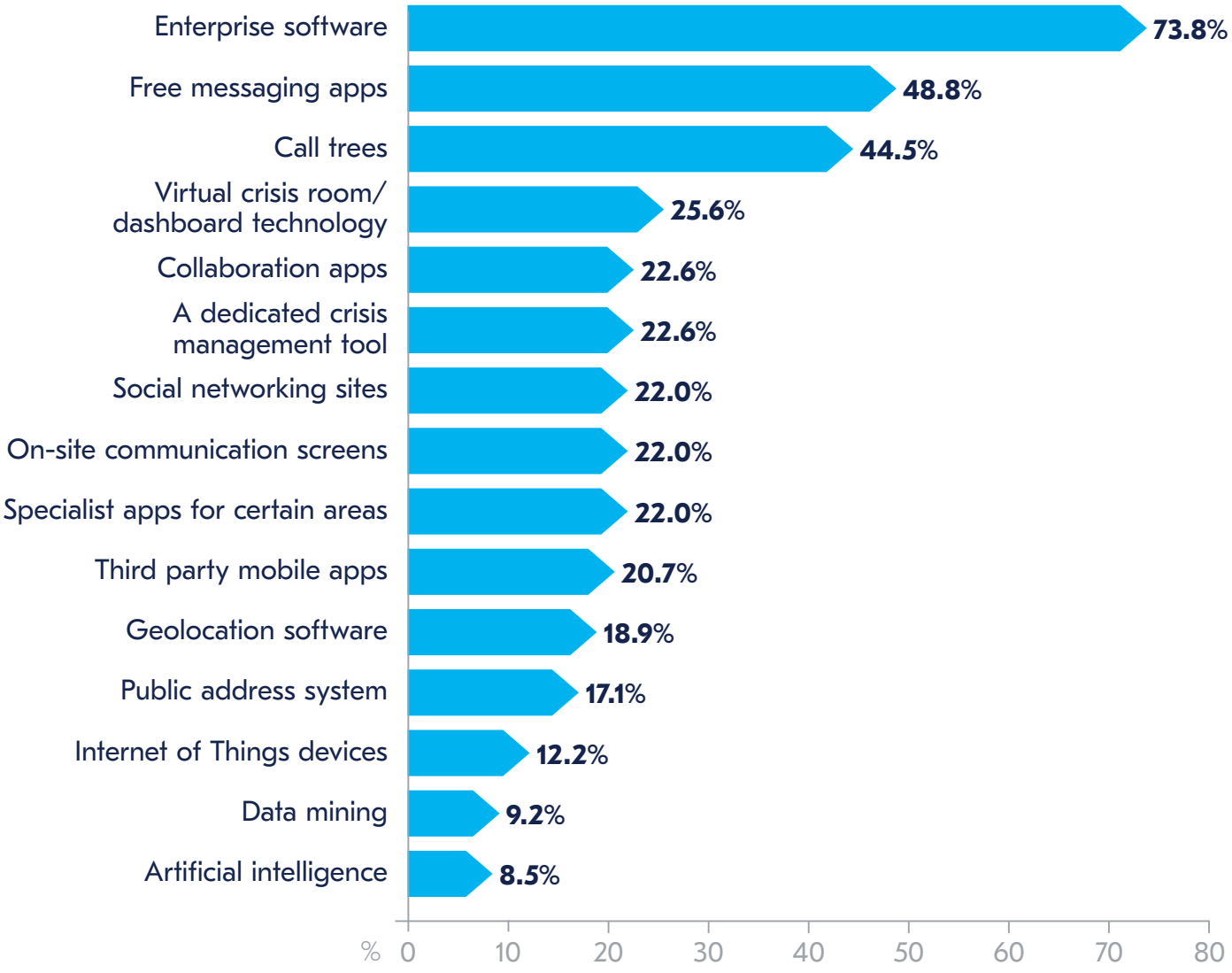
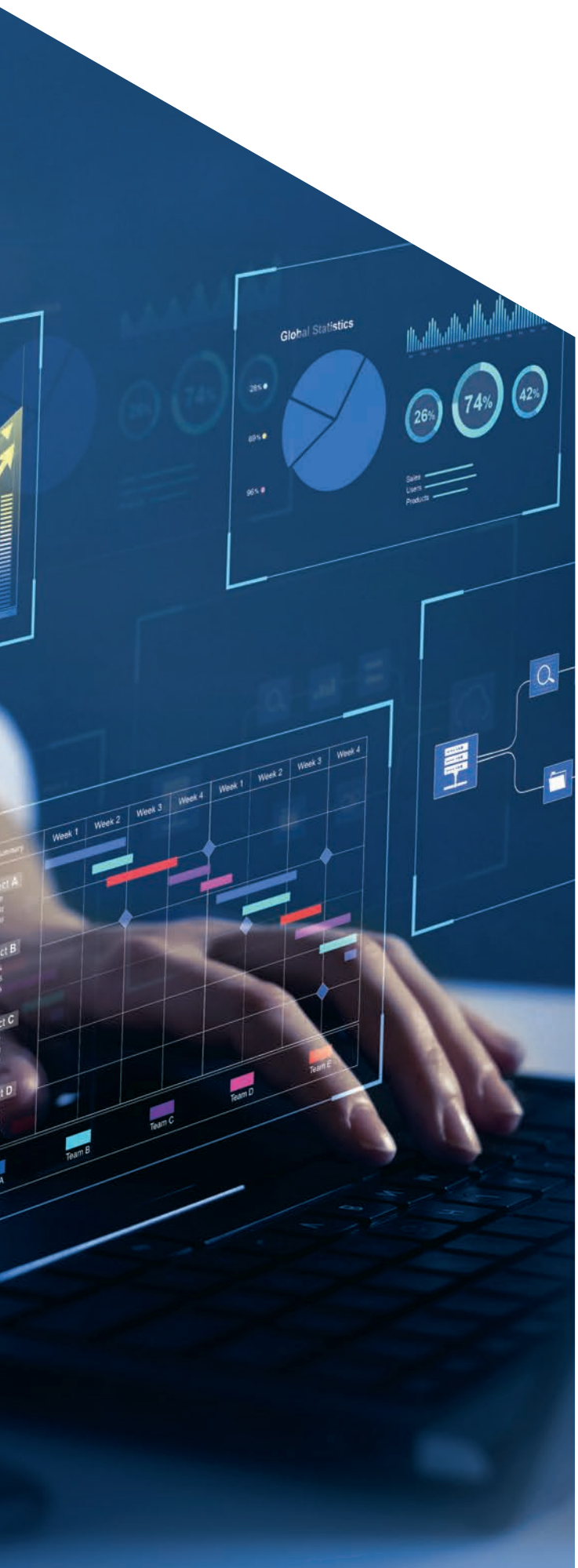


Figure 15. Which departments are represented in a post-incident review?

The rise in popularity of virtual crisis rooms and dashboards is indicative of the growing recognition of their importance in modern business operations. These tools are becoming essential for organizations in a context where there is a shift to remote and hybrid working styles. The old model of a physical crisis room is becoming obsolete in some organizations. The data suggests that the primary use of these tools is for situation control, decision-making processes, and team communication, with 40.5% of respondents highlighting these aspects. This underscores the multifaceted utility of virtual crisis management tools, as they not only help in managing the immediate situation but also enhance communication and streamline decision-making across teams. An example of this is the ability to assemble teams fast, having a global representation in the room, being able to have subject matter experts as part of the team (regardless of where they are in the world).

Another option available is "off the shelf" virtual crisis rooms. These are pre-configured digital platforms designed for managing crises and facilitating collaboration during emergencies. Some of their advantages include tools like real-time chat, video conferencing, and document sharing to enable seamless teamwork, ease of information sharing, scenario simulation options, ease of task management allocation and strict access control that ensures only authorised individuals can access sensitive information.

However, it is noteworthy that 27.6% of respondents indicated that they do not use or would not use such tools. This could suggest a lack of awareness or a belief that traditional methods suffice for their needs. For some organizations, the perceived complexity, or the initial cost of implementing these tools might outweigh the benefits. Some concerns about virtual crisis rooms could be concerns about confidential information becoming public, opening up an organization to a cyber-attack at a time of crisis, lack of ability to connect in the event of a power, platform, or telecoms outage.



However these concerns can be addressed as some virtual crisis room technologies are protected against screenshotting (protecting user's privacy, power backup supplies could be available to team members in case of an outage, extra cyber security measures could be out in place to safeguard the technology used when in a crisis.

Interestingly, when assessing the impact of virtual crisis management on internal efficiency, a significant portion of respondents (24.1%) acknowledged that these tools have enhanced their efficiency to a good extent, while 13.6% believe the impact is significant. This is a strong indicator that, for many, the adoption of virtual crisis tools is paying off in terms of operational effectiveness.

The data revealed relatively low levels of scepticism, with 6.8% of respondents feeling that these tools have only made a small difference, and 3.7% even reporting a reduction in internal efficiency due to the use of technology. This confirms last year's trend, where a similar subset of respondents expressed doubts regarding the adoption of virtual crisis rooms. This might point to cases with implementation challenges, such as insufficient training, poor integration with existing systems, or resistance to change within the organization.

"We have virtual crisis management rooms if it is the middle of the night and we need to do something quickly, but if it is during the day, if possible, we'll have physical teams meet. There is a balance for it. I think you need to make sure that you use virtual meetings at the right time for the right purposes. When it moves into the recovery phase, business continuity people prefer to work from their own desks."

CEO Private sector, UAE

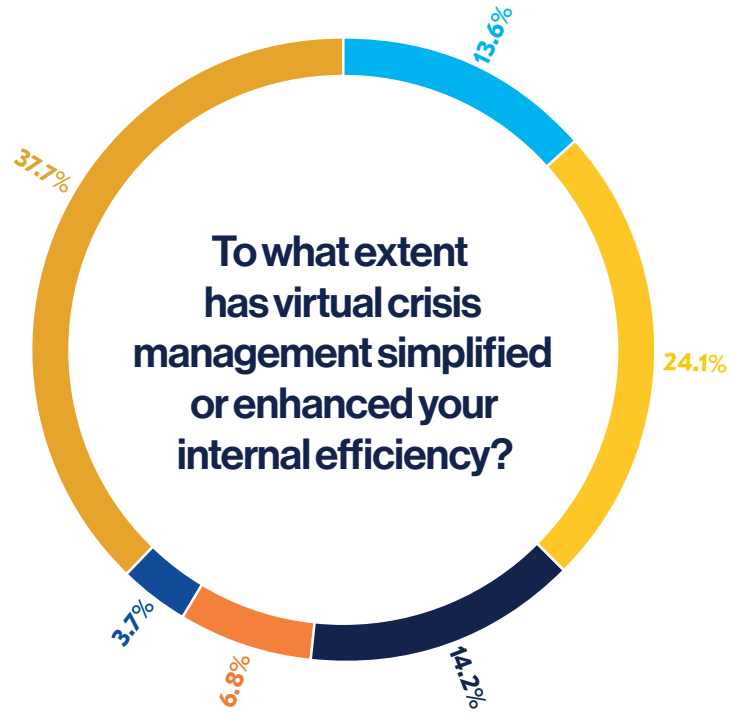
Delving into the specific tools used by participants provides valuable insight into the practical applications of virtual crisis management solutions. Tools like PowerBI and Microsoft Teams are prominently used to enhance situation control, decision-making, and communication. For instance, pre-staged files for teams, including playbooks, are used to speed up triage and recovery efforts.

Continuous communication during a crisis is critical, and organizations are choosing various platforms for this purpose such as Teams, virtual whiteboards, short status updates, and WhatsApp. These tools facilitate real-time information sharing and coordination among teams, ensuring that everyone is aligned and informed. However practitioners should be wary as some platforms faced scrutiny over its data privacy practices and lacks end-to-end encryption, making it vulnerable to security breaches and unauthorised access to sensitive information.

Interestingly, some participants noted a preference for tools that work offline, suggesting a need for solutions that are reliable in all circumstances, including those where internet access might be compromised such as walkie-talkies, satellite phones, or local radio systems.

Moreover, situational control and decision-making processes are sometimes influenced by individual leadership styles. This points to the importance of tailoring crisis management tools to fit the unique dynamics of each organization. Other participants mentioned using proprietary tools to remotely access shared situational awareness and track key issues.

Figure 16. Virtual crisis room/dashboard are currently growing in popularity and are in high demand. What do you use/would you use this kind of tool for?



13.6%
To a significant extent

24.1%
To a good extent

14.2%
To some extent

6.8%
To a small extent

3.7%
Not at all, we have found using technology has reduced our internal efficiency

37.7%
N/A

Figure 17. To what extent has virtual crisis management simplified or enhanced your internal efficiency?

The survey data indicates significant interest in using AI across various aspects of crisis management. Respondents see strong potential for AI in areas such as data analysis and decision support (72.5%), real-time monitoring and alerts (70.6%), predicting potential crises (56.2%), and automating response protocols (49.7%). According to participants, AI could enhance situational awareness, provide critical insights during crises, and enable faster, more informed decision-making. Additionally, AI's ability to analyse data and identify patterns could help organizations anticipate crises, while automation could streamline response execution, reducing human error and increasing efficiency. Communication and coordination during a crisis (44.4%) is another area where AI is expected to play a crucial role, particularly in ensuring timely and accurate information dissemination across teams and stakeholders.

> **"We are not currently using AI to help with crisis management, but there are undoubtedly opportunities to do so in the future."**
>
> Head of civil contingencies, public sector, UK

However, qualitative feedback from respondents offers a more nuanced perspective. Some participants mention specific use cases, such as preventive communication and coordination for risks including climate-related ones, and maintaining current configuration data, dependency analysis, and mapping products to processes. These applications show AI's potential to support proactive and organised crisis management.

On the other hand, there is also scepticism and caution. Concerns about AI's current performance, biases in databases, and the ethical implications of relying on AI in critical situations were expressed, with one respondent noting that AI tools have shown "very poor and questionable performance" to date. This reflects a broader hesitation to fully embrace AI without addressing these significant challenges. Trust and reliability emerge as central themes, with some respondents undecided on how or whether to integrate AI into their crisis management strategies, emphasising the need for proper feedback cycles and validation mechanisms to ensure AI's effectiveness and ethical alignment.

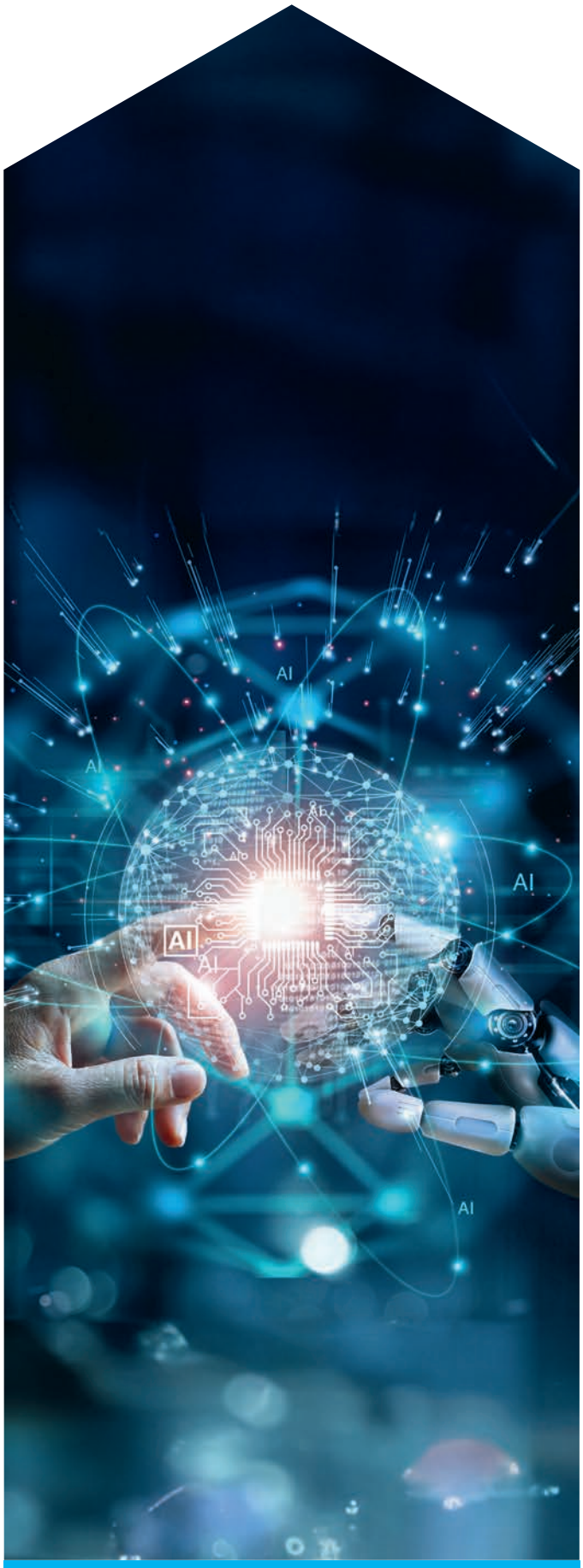
Several respondents are unsure of AI's benefits or believe it is too early to say, indicating that while interest in AI is high, practical adoption may lag behind until these concerns are resolved. Other participants mention more specific applications, such as collaboration with external agencies, scenario creation and testing, automated meeting minutes, and using AI as a backup to validate response and recovery decisions.

"We're bringing in an automation business continuity management tool, which is very useful both in the planning stages and for real incidents."

CEO Private sector, UAE

"We use AI. We input our traditional intelligence in the planning and AI analyses it for us. As long as the information going in is good, it will give us some good options to analyse. It saves us work, but it still needs to be checked by a human."

CEO Private sector, UAE



"We use AI to help design scenarios for simulations."

CEO Private sector, UAE

It is interesting that most respondents have not highlighted the uptake of AI in exercising and crisis simulations, which is a growing trend that is gaining popularity in industry discussions. Generative AI (GAI) is revolutionising crisis management training by creating highly realistic and adaptive scenarios. Unlike static simulations, GAI-driven training presents dynamic situations that evolve in response to participant decisions, closely mirroring the fluid nature of real crises. This technology allows for the generation of scenarios that integrate multiple variables — economic, social, technological — thus providing a more comprehensive and challenging training experience.

With GAI, scenarios can be tailored to various experience levels, offering a bespoke challenge for both novice and experienced professionals. For instance, simulations can adjust in real time based on decisions made by participants, offering insights into the cascading effects of their choices, and encouraging strategic thinking under pressure. Additionally, GAI enables real-time adaptability and provides detailed feedback, fostering a continuous learning loop where participants can refine their skills through iterative practice.

This shift from traditional preparedness to mastery represents a paradigm change in crisis management. By leveraging GAI, organizations can cultivate a deeper understanding of crisis dynamics, make high-risk decisions in a safe environment, and address knowledge gaps that arise from individual biases. This approach ensures that leaders are not only prepared but adept at navigating complex, unpredictable crises, enhancing organizational resilience and response capabilities[15].

What are the areas where you think AI can help you within crisis management?

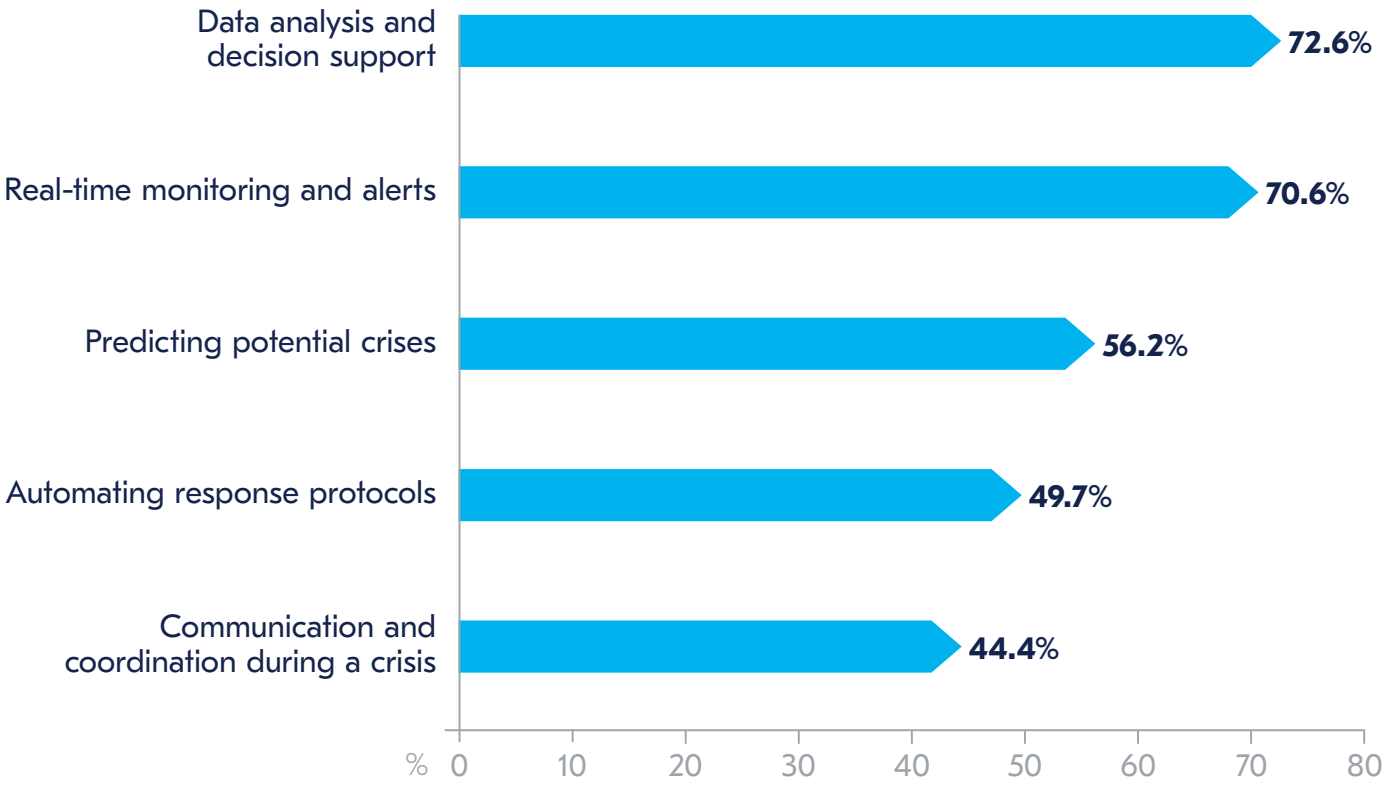


Figure 18. What are the areas where you think AI can help you within crisis management?

Investment in crisis management

Investment in crisis management

- The majority of organizations are anticipating increased investment in crisis management and resilience over the next five years, with a strong emphasis on education, training, and software. This trend highlights a proactive approach to strengthening both human capital and technological capabilities.
- Investment in new technology, such as AI and data mining, is gaining traction, indicating a shift towards leveraging advanced tools for enhanced crisis response. However, there are concerns about over-reliance on technology, with some respondents emphasising the need for redundancy and having back-up manual processes in place to mitigate potential vulnerabilities.
- There is a notable focus on hiring for resilience-oriented roles and improving community resilience, reflecting the recognition that effective crisis management involves not only advanced tools, but also requires skilled professionals and regular collaboration with external partners.

This year's research reflects a clear trend towards increased investment in crisis management and resilience over the next five years, with a majority anticipating either significant or some investment. Specifically, 55.8% of respondents expect investment to grow (2023: 52.7%), a trend which is also in line with the 2023 report, which showed increased attention and dedication towards crisis management. However, the small percentage of respondents expecting a reduction of their budget typically reference economic reasons.

"I think there will be more buy in next year because we managed a number of incidents within the last year. That has meant more understanding of the role from senior management."

BC and incident manager, public sector, UK

"Recent austerity measures led to a decrease in spending on resilience and BC which can be de-prioritised."

Head of civil contingencies, public sector, UK

There is also continuity with the type of investment that professionals expect. Notably, investment in education, training, and exercising tops the list at 84.4% (2023: 79.2%), which is also a recurring theme throughout this year's report. This underlines a growing recognition of the importance of well-prepared and skilled personnel in navigating crises. This is specially relevant as the usage if AI within crisis grows and the need to upskill personnel on this is of the utmost importance.

Training and exercises are crucial for ensuring that teams are not only familiar with protocols but can also adapt to unforeseen challenges. This focus on human capital aligns with the need for dynamic and responsive crisis management, as highlighted by the growing use of generative AI in training scenarios. There is also the need not only to engage personnel on training activities but also senior leadership. In this case, the assistance of AI developing quick, realistic and all-encompassing scenarios can maximise short time slots in busy executive diaries.

Software follows closely with 67.8% (2023: 78.1%), highlighting the attention towards leveraging advanced technologies to manage and respond to crises more effectively. Investment in software can enhance capabilities in data analysis, communication, and decision-making, all of which are vital in crisis scenarios. As mentioned earlier in this report, the use of AI can enhance the preparation (training) and management of crises such as

Infrastructure and staff investments also receive significant attention, with 45.6% (vs 37.5% In 2023) and 57.8% (vs 60.4% in 2023), respectively. This indicates a recognition of the need for robust systems to support effective crisis management. However, hardware, at 18.9% (2023: 25.0%), seems to be a lower priority compared to other areas, which may suggest that while physical assets are important, the emphasis is currently on software and education and training.

Figure 19. Do you believe that investment will increase in crisis management and/or resilience over the medium-term (next five years)?

Please specify where this investment is/will be directed

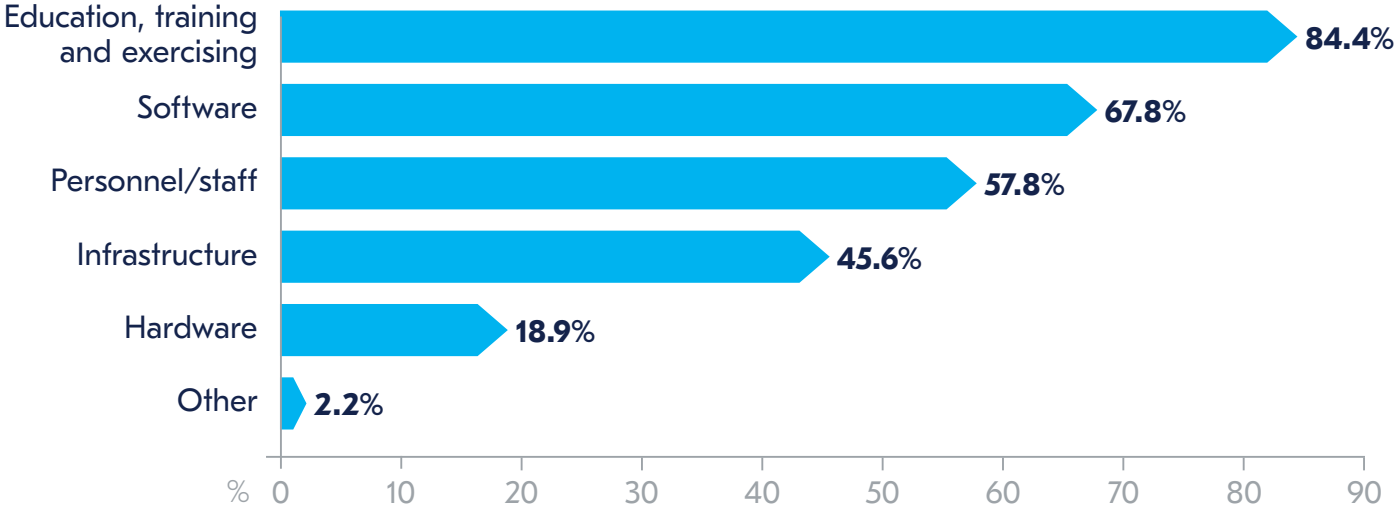


Figure 20. Please specify where this investment is/will be directed

The data suggests that organizations are increasingly aware of the need to adapt their crisis management practices in response to emerging challenges and technological advancements. With 41.3% of respondents indicating investment in new technology such as AI and data mining, it is clear that there is a growing focus on leveraging advanced tools to enhance crisis response capabilities.

This aligns with the broader trend of digital transformation, where technology is being used not just to react to crises but to anticipate and mitigate them through proactive measures like horizon scanning, which 26.5% of respondents highlighted.

Interestingly, 37.4% of respondents expect new hires in resilience-oriented roles, signalling a commitment to strengthening the human element of crisis management. This focus on personnel suggests that while technology is crucial, the expertise and judgment of skilled professionals remains vital. The expectation of improved community resilience, noted by 38.7%, also reflects a growing recognition that effective crisis management extends beyond the organization itself, requiring collaboration with sector peers, local authorities, and other external partners.

Qualitative responses indicate concerns about over-reliance on technology, particularly cloud management and third-party capabilities. Some respondents fear that this dependence may lead to a false sense of security, potentially leaving organizations vulnerable if these systems fail. This concern is echoed in the call for more emphasis on manual processes, redundancy, and air-gapped critical systems to minimise operational impact during crises.

Moreover, there is a clear demand for better integration and interoperability between crisis management and other resilience functions like business continuity and emergency response. This comprehensive approach is seen as key to maintaining effectiveness amidst organizational changes and budget constraints. Notably, some respondents reported no expected changes or even reductions in crisis management funding, which highlights the challenge of maintaining resilience capabilities in an environment of financial austerity.

Overall, while there is a strong push towards technological investment and enhancing human resources in crisis management, there is also a cautious awareness of the risks associated with over-dependence on these new systems. Balancing technological innovation with robust manual processes and ensuring sufficient funding and integration across resilience functions will be crucial for organizations aiming to strengthen their crisis management practices.

Interviewees explained their expectations for the future.

"I would like to see AI support crisis management with update requirements, reminders, automated tasks, and summarising information for large screen dissemination."

Business resilience manager, aviation, Hong Kong

"I expect more investment in AI in the future to bring in automated systems and train people on how to use them to use them properly."

CEO Private sector, UAE

"I see crisis management evolving and linking in with the wider community."

Head of Risk & Assurance, Private Sector, South Africa

"In the future I hope to see the three major disciplines, risk management, crisis management, and business continuity management work more closely together."

CEO Private sector, UAE

How do you feel working practices will change with regard to crisis management in your organization?

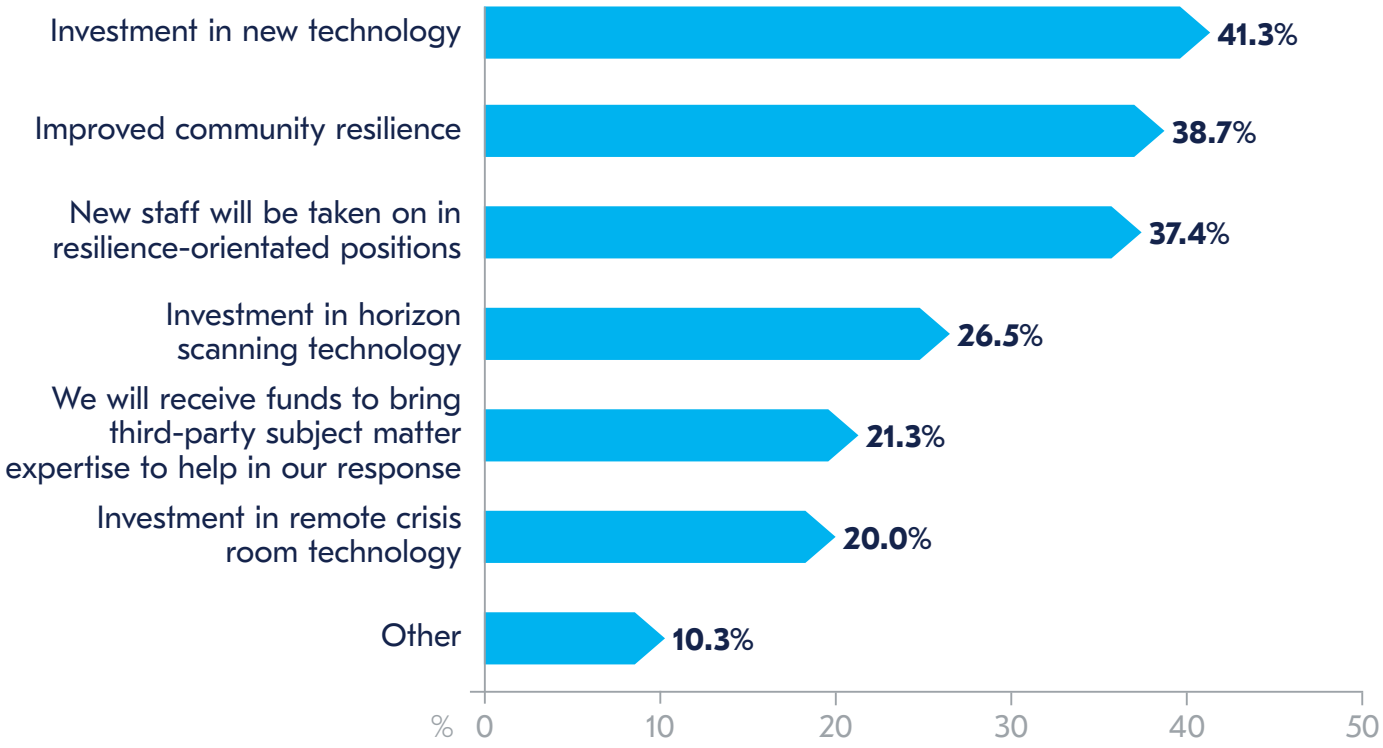


Figure 21. How do you feel working practices will change with regard to crisis management in your organization?

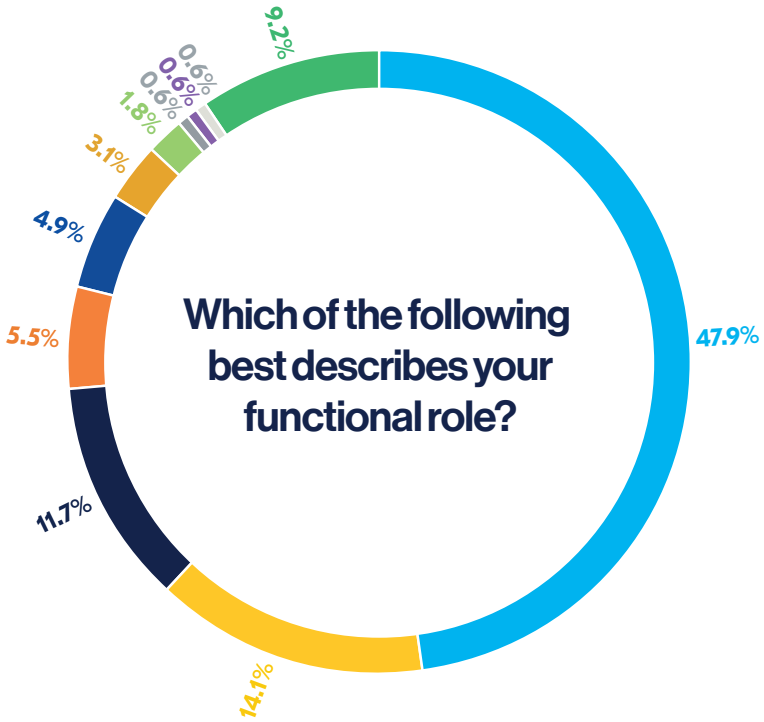
Annex

211
Respondents

38
Countries

15
Sectors

10
Respondent interviews



47.9% Business continuity

14.1% Crisis management

11.7% Risk management

5.5% Top management

4.9% IT disaster recovery/ IT service continuity

3.1% Emergency planning

1.8% Information security

0.6% Health and safety

0.6% Physical security

0.6% Internal audit

9.2% Other

Figure 22. Which of the following best describes your functional role?

33.1% Financial & Insurance Services

13.5% Public Administration & Defence

11.0% IT & Communications

6.8% Manufacturing

4.3% Energy & Utility Services

4.3% Education

3.1% Legal & Professional Services

3.1% Transport & Storage

3.1% Retail & Wholesale

2.5% Health & Social Care

2.5% Telecommunications

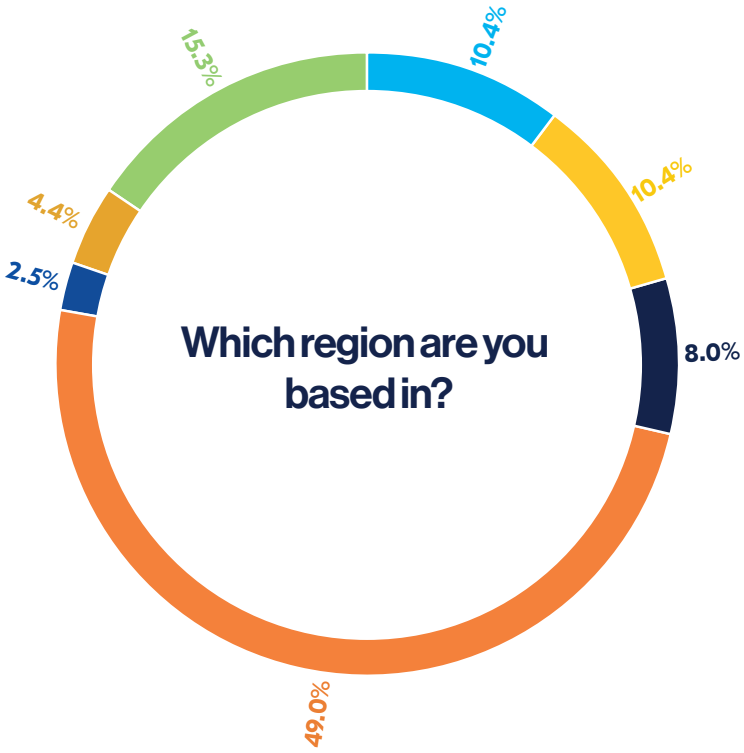
1.2% Leisure and Hospitality

1.2% Support Services

0.6% Engineering & Construction

9.8% Other

Figure 23. What sector does your company belong to?



10.4% Africa

10.4% Asia

8.0% Australasia

49.0% Europe

2.5% Latin America and The Caribbean

4.4% Middle East

15.3% North America

Figure 24. Which region are you based in?

How many countries do you operate in?

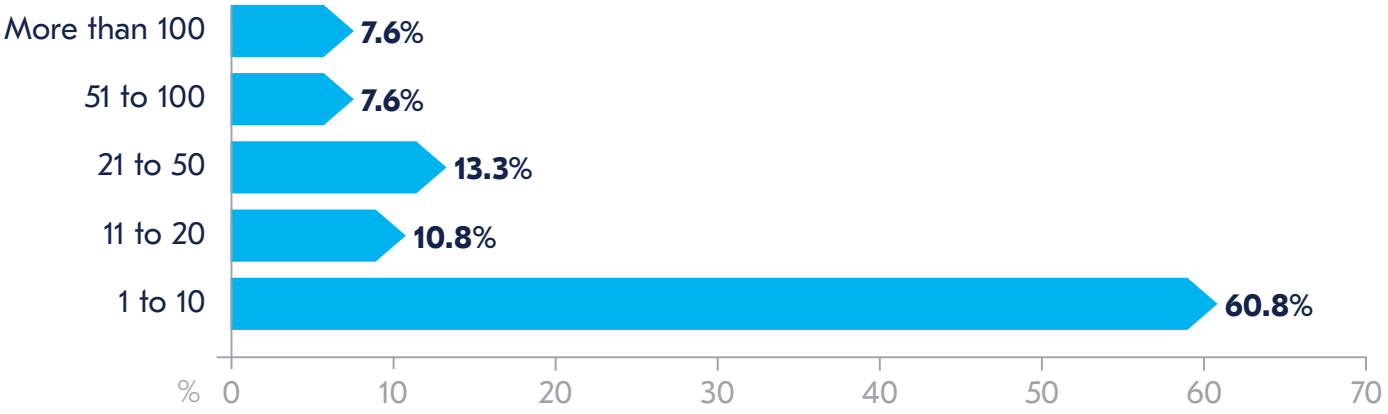


Figure 25. How many countries do you operate in?

Approximately how many employees are there in your organization globally?

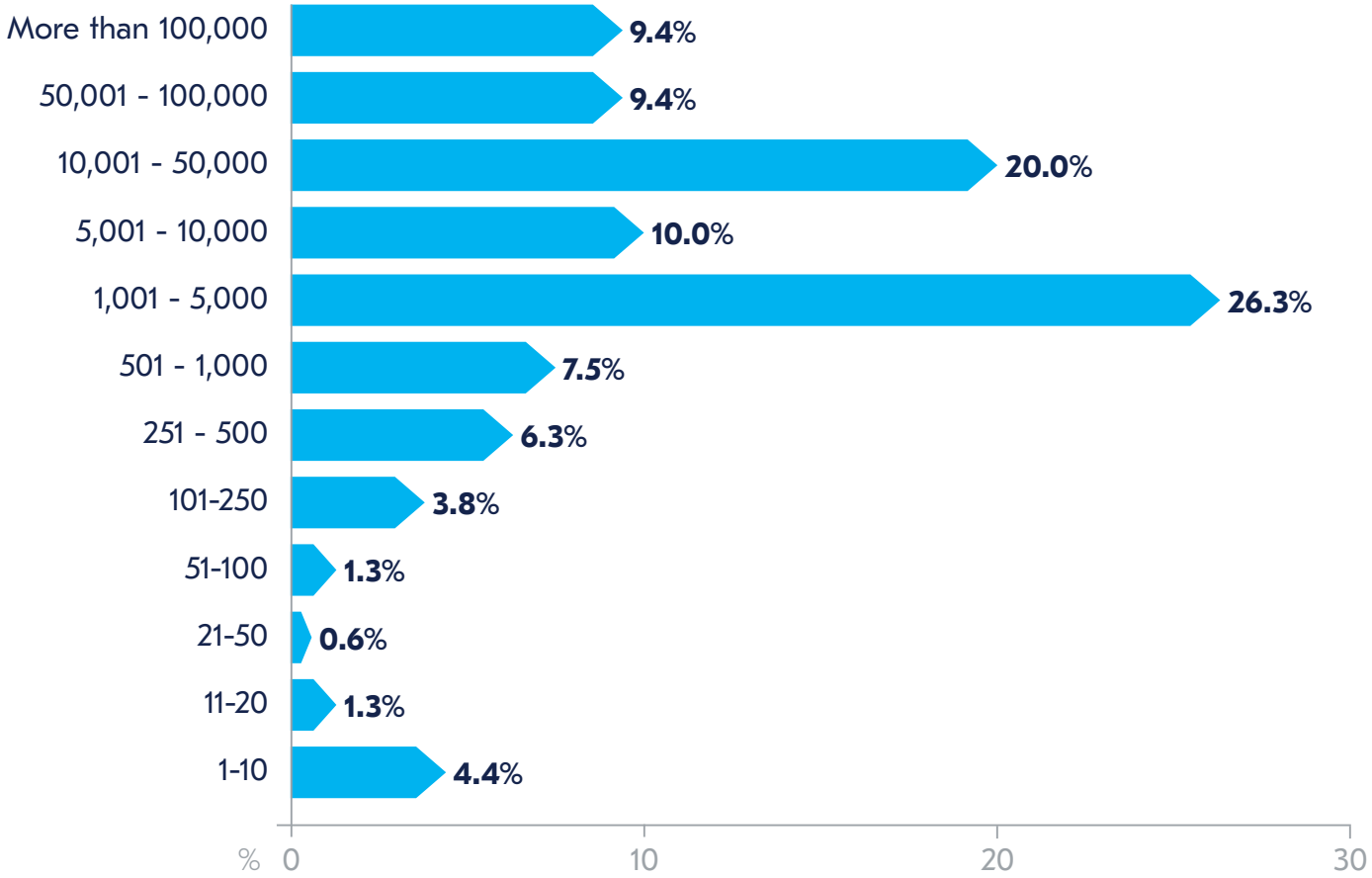


Figure 26. Approximately how many employees are there in your organization globally?

About the authors

Rachael Elliott
(Knowledge Strategist, 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
(Thought Leadership 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

Gianluca Riglietti
(Content Specialist in Business Continuity and Resilience)

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

About the BCI

Founded in 1994 with the aim of promoting a more resilient world, the 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 F24

F24 is Europe's leading Software-as-a-Service (SaaS) provider for incident and crisis management, emergency notification, as well as business messaging. More than 5,500 customers worldwide rely on F24's digital solutions to strengthen their organisational resilience holistically. The highly innovative F24 solutions support customers through the whole value chain: from high-volume business communication and the area of governance, risk and compliance (GRC) through mass and service notification, smart event communication as well as public warning and emergency notification up to comprehensive incident and crisis management.

Contact F24
+49 89 2323638 81 | **www.f24.com** | **patrick.eller@f24.com**
Ridlerstraße 57, 80339 Munich, Germany

References

1. science.nasa.gov/climate-change/extreme-weather
2. www.thebci.org/news/uae-exploring-the-impacts-of-severe-weather.html
3. www.bbc.com/news/science-environment-68897443
4. www.iso.org/obp/ui/#iso:std:iso:22361:ed-1:v1:en
5. skift.com/2024/05/22/singapore-airlines-displays-a-masterclass-in-crisis-communications
6. skift.com/2024/05/22/singapore-airlines-displays-a-masterclass-in-crisis-communications
7. ISO. ISO 22361: Crisis Management — Guidelines. International Organization for Standardization
8. drj.com/journal_main/crisis-management-training-and-exercises-preparing-your-team
9. www.supplychaindive.com/news/adidas-america-fines-400k-osha-warehouse-safety-violations/724723
10. www.thelancet.com/journals/lanwpc/article/PIIS2666-6065(24)00131-7/fulltext
11. www.thebci.org/news/crisis-leadership-report-bci-white-paper-q3-2022.html
12. www.thebci.org/resource/good-practice-guidelines-2018.html
13. drj.com/journal_main/crisis-management-training-and-exercises-preparing-your-team
14. Ibid.
15. theisrm.org/en/the-use-of-generative-artificial-intelligence-as-a-simulation-tool-for-advanced-training-in-crisis-management

BCI 9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK bci@thebci.org / www.thebci.org

F24

bci Leading the way to resilience