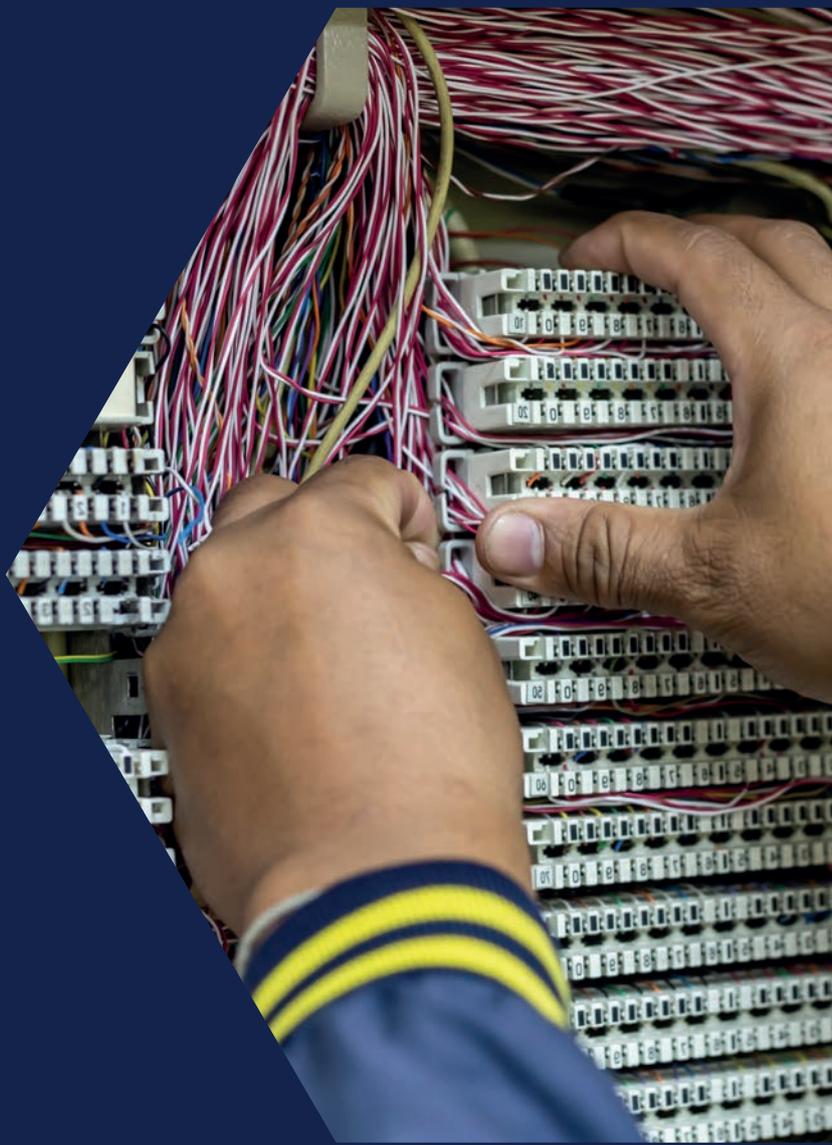


Emergency and Crisis Communications Report 2023



Contents

- 5** **Executive summary**
- 12** **Section one:
The toolbox**
- 41** **Section two:
Triggers and execution of plans**
- 59** **Section three:
Key challenges during a crisis:**
- 66** **Section four:
Building resilience**
- 71** **Section five:
Looking ahead**
- 74** **Annex**





Foreword

We are pleased to present the seventh edition of the *BCI Emergency and Crisis Communications Report*. We would like to thank F24 for their continued support of this vital report in the BCI's Thought Leadership portfolio.

This year's report shows a discernible shift in the way organizations are managing their emergency and crisis communications. New technologies are becoming a game changer in the way organizations communicate, collaborate and act in a crisis scenario. Whilst the first and foremost criteria required of an emergency communications solution remains contacting staff quickly and efficiently, practitioners now expect much more of their tools. They want back-up communications services to be available as part of their solution, they are asking for geolocation services to help locate staff in remote environments, and they want teams to be able to collaborate effectively throughout a crisis – even if electricity and communication networks are down.

Practitioners are also changing the hardware devices they use to interact in a crisis. To manage crises effectively and nimbly, the best way of doing this, for most, is by using the device which they always have on them in person: their smartphone. Interestingly, as smartphones are now essentially mini tablet computers, there is a significant drop-off this year in the number of organizations using tablets in a crisis scenario. Desk phones are also continuing their demise.

We are further noting that organizations are seeking to mature their emergency and crisis communications strategies as they finalise their new working practices. For organizations who still have a lot of staff working on site, walkie-talkies and radio communication still have their place. For those who have staff working in multiple locations, a more sophisticated emergency communications solution becomes essential. We have also noted an increased interest in satellite phones this year.

However, whilst technology has gone a long way in creating solutions which help practitioners to manage crises more effectively through collaboration and through information rich dashboards whilst also offering the ability to communicate when networks are down, plans still fail. Organizations frequently lack the ability to elicit a truly effective response because staff do not receive regular training on tools and processes, they do not take part in sufficient exercising, managers fail to update contact information, or contact information is housed in spreadsheets on various computers.

Encouragingly, we have seen an uptick in the volume of training and exercising taking place this year, and we are seeing investment in dedicated tools and technologies rise as reshuffled workspaces look to find tools that better match their new ways of working.

We hope that this report provides a useful benchmarking document for organizations who already have a tool in place and, for those who do not, provides an awareness of the range of options needing to be considered when employing a new emergency and crisis communications system.

We would once again like to thank F24 for their continued sponsorship of this report and also offer our sincere thanks to everyone who completed the survey or participated in interviews for the report. Data is only one part of the analysis process and the interviews help us to really understand the issues faced by practitioners in their day-to-day roles.

Rachael Elliott

Head of Thought Leadership
BCI



F24

Foreword

2022 was a year that put the resilience and preparedness of companies to test perhaps more intensely than ever before. Following the challenges and disruptions caused by the COVID-19 pandemic in the previous years, there was a hope that 2022 would bring a more stable business environment. However, 2022 presented quite a few new as well as unexpected crises like the war in Europe, disrupted supply chains, inflation, and the climate crisis. In the face of the state of permanent crises, it becomes more important than ever to have effective emergency notification and crisis management systems in place and to anchor resilience as a fundamental element in the company strategy.

In the light of these developments, we are happy to see companies recognizing the situation and acting proactively.

One important aspect is the significant rise in the number of companies applying software-based solutions during a crisis: With 70.5% of organizations using digital tools or software to manage their emergency communications during crisis scenarios, the share has reached a new record high. Observing this continuously rising trend over the last years, one can even speak of a long-term shift in perspective: The deployment of digital solutions has become a fixed component in managing emergency situations. Nowadays it is rather unusual to not use any specialized software.

Another finding in line with this trend is the continued rise of Software-as-a-Service (SaaS) solutions, which is now used by 81% of organizations who use software in emergency communications. A further positive message is that more and more companies put emphasis on emergency communications training to enhance their preparedness in the event of a serious incident. The frequency of training is rising, with more than a third of organizations (36 %) carrying out training twice a year or more - an increase of over 10 percentage points in comparison to last year (24%).

Quick and reliable means of communication during

a crisis are other integral parts of effective crisis management. For over two-thirds of companies, the most popular method to communicate during a crisis (apart from email) were enterprise messengers (66.1%). The extensive use of those should be treated with care in the light of recent events: Regular outages of prominent business and private messaging tools occurring in 2022 once more underline the severity of consequences if such an outage would happen during a crisis. This should provide food for thought and motivate responsible individuals to re-think and evaluate alternatives.

Taking a closer look to the sort of events which triggered emergency communication plans in the past year, the most common events range from weather-related events over IT or telecoms incidents to cyber-security incidents and data breaches. Given the increase of cyber threats and an accelerating climate change, these threats most likely won't become less relevant in the future and once more emphasize the importance of having an intact notification and crisis management system in place.

On an overall perspective it is encouraging to see also proven by this report that an increasing number of companies are taking these developments seriously by implementing appropriate measures to strengthen their resilience. We at F24 are committed to support businesses on their road to resilience by delivering reliable and state-of-the-art software solutions. We are happy to continue our partnership with the BCI and support their research as a long-term sponsor, trusting that organizations globally benefit from the latest data by understanding the state of companies' emergency notification systems and preparedness. I am confident that this report will serve as a valuable resource for anyone looking to enhance their emergency strategies and improve their notification systems, ensuring the safety and well-being of their employees as well as protecting their values. Having that said, I'm wishing you an inspiring time reading the report!



Benjamin Jansen

Senior Vice President Sales ENS/CM
F24



**Emergency
and Crisis
Communications
Report 2023**
Executive
summary

Executive summary

The number of organizations using digital tools to manage their emergency communications continues to increase: The shifting of organizations' working environments post-pandemic has accelerated the digitalisation and sophistication of tools. This acceleration in technology uptake within organizations was also noted with crisis management applications as organizations continue to move away from the physical crisis room towards virtual environments.

The use of Software-as-a-Service solutions (SaaS) continues its drive as the incumbent software type and is now used by 81% of organizations who use software in emergency communications, the highest ever: Employee mobility, the increased need for collaborative tools and the requirement for multiple devices being used within corporate settings means SaaS solutions are dominating. Less than 1 in 5 now use installed software for their emergency communications.

Mobile phones remain the most popular device to manage emergency communications – but are tablets waning from corporate popularity? With mobile phones now offering access to corporate emergency communication tools through SaaS, they remain the most popular device used in emergency scenarios – although laptops are only marginally behind. The popularity of tablets has fallen dramatically this year, however. In last year's report, they were the third most popular device and more than a third of organizations used them in emergency scenarios. This year, their usage has fallen by ten percentage points which puts them as more unpopular than desk phones.

Extensive use of enterprise communication tools throughout the pandemic has driven investment in digital tools within crisis management: Over two-thirds of emergency communications teams are now using enterprise software to communicate during a crisis. This year, a third of organizations are employing emergency communications management software – a figure likely to increase over the coming year – and 24.6% a secure messaging app which is dedicated for use within emergency situations. Organizations are demanding more from their tools than ever before: features such as collaboration, risk management and information corroboration are increasingly being featured as standard within emergency communications solutions.

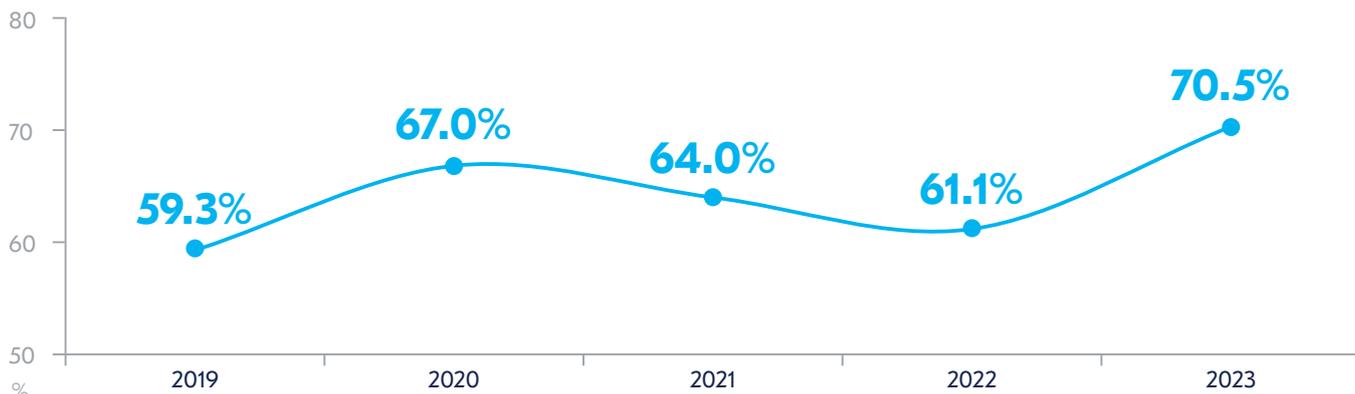
There has been a slight drop in the achievement of expected response levels when executing an emergency communications plan: This year, 74.3% of organizations are achieving their expected response levels compared to 78.5% in 2021 when attainment of expected response levels was at its highest. Whilst the drop is only marginal, it could be down to organizations lowering their expected response times, as well as an increase in incidents in the past year. Adverse weather, the area where practitioners reported most activations in the past year, was the cause for initiation of crisis management plans in nearly half (49.4%) of cases.

The human factor remains the most common cause of failure of emergency communications plans: Most organizations are executing their crisis management plans between one and five times a year, with 46.5% of organizations mentioning information (mostly done through spreadsheets and manual procedures) as the most common cause of failure. A lack of understanding from recipients is once again in second place, pointing towards insufficient training and exercising taking place, as well as a no or limited integration with HR contact systems.

Usage of emergency notification/crisis management tools reaches a historic high

70.5% of organizations are now using digital tools or software to manage their emergency communications within crisis scenarios.

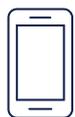
Usage of emergency notification/crisis management tools or software within organizations 2018- 2023



Mobile phones have consolidated their position as the device of choice to manage emergency situations

Almost 98% of organizations use mobile phones to handle emergency situations. Desk phones continue their demise in popularity, and tablets have plummeted in popularity by 11 percentage points.

What devices are you using to manage emergency situations?



95.9%
Mobile phones



94.0%
Computers/
laptops



27.7%
Walkie-talkies/
radios



25.2%
Desk phones



23.6%
Tablets



21.0%
Satellite phones

Software-as-a-Service (SaaS) usage has registered an all-time high

Software-as-a-Service (SaaS) continues to increase as the incumbent method of deployment for emergency and crisis communication software with more than 4 in 5 organizations choosing it over an on-premise tool.

What kind of software/tool are you using?



81.4%
Software-as-a-Service solution



18.6%
On-premise installed software

The capacity to alert and organise a high number of people very fast remains the most valued feature of an emergency communication tool

Nearly nine in ten organizations highlight the need for a tool that allows them to collaborate during an incident (2022: 71.5%)
 Current geopolitical tensions and the intensifying of global weather-related events has created a heightened emphasis on the importance of this capability.

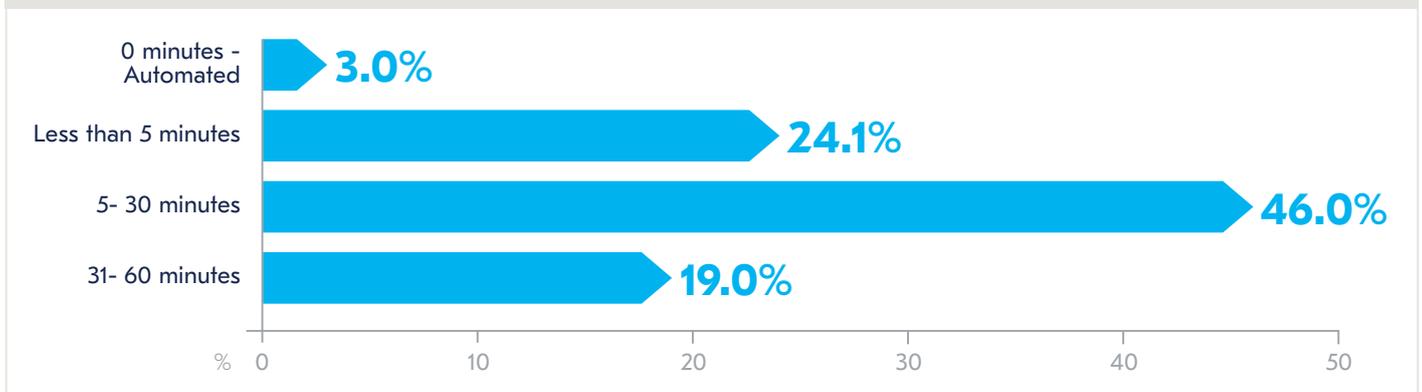
In which areas does your software/tool support you? (top ten responses)



Organizations are getting faster at activating their emergency communications plans

92.1% of organizations are able to activate their emergency communication plans within 60 minutes (2022: 81.7%) with 73% of those organizations being able to do so within 30 minutes (2022: 69.9%).

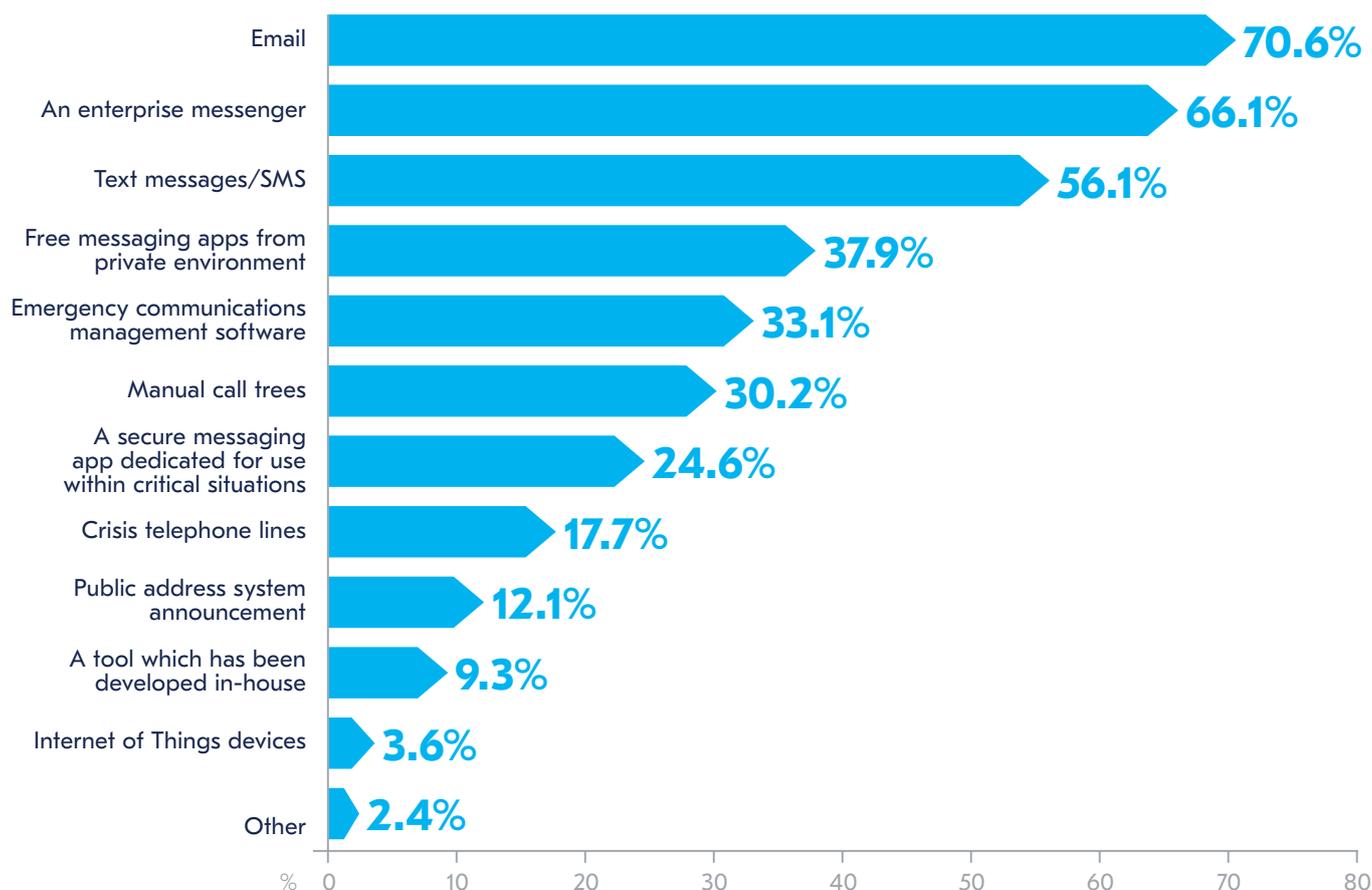
Having a plan: Activation times under 60 minutes



Enterprise messengers are the most used software tool within organizations during a crisis

There are now multiple tools being used for crisis management purposes. However, the most popular method of communication (outside email) is using an enterprise messenger solution to communicate during a crisis. The increase in technology uptake highlights how emergency communications solutions are now a principal target for funding by senior management.

What methods of communication do you use to communicate internally during a crisis?



Technology increases the speed of activation for their emergency communications plan

1 in 3 organizations using emergency communications tools can activate plans within five minutes compared to just 1 in 14 for those without. At 30 minutes, 77% of organizations with tools will have been able to activate their emergency communications plan compared to 49% who do not.

	Organizations using emergency communication tools	Organizations not using emergency communication tools	% difference for those using software vs those who do not
Organizations capable to activate plan within 5 minutes	32.8%	7.1%	+25.6%
Organizations capable to activate plan within 30 minutes	77.2%	48.6%	+28.7%

The human factor continues to be the prime reason for an emergency communications failure

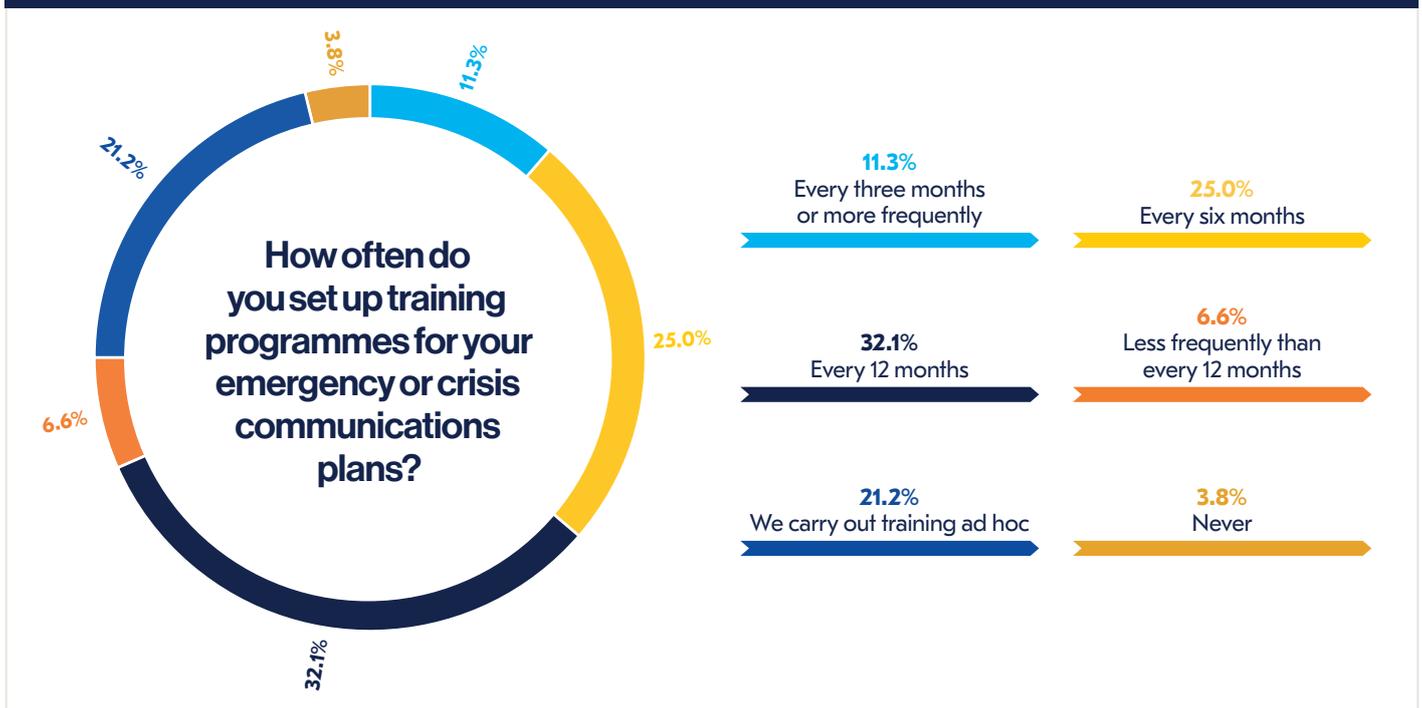
The lack of accurate staff contact information is the most commonly cited reason for emergency communications plan failure. However, with manually updated spreadsheets still the incumbent method of storing staff contact information, it is not surprising that this is the primary reason for plan failure.

If you failed to achieve your accepted response levels, what caused the failure? (Top nine responses)



There has been a significant increase in the importance attributed to training and exercising within organizations

More than a third of organizations carry out training between two to four times a year, a contrast from previous reports where once a year was the norm.



Emergency and Crisis Communications Report

This year's BCI Emergency and Crisis Communications Report showcases how 2022 has been a year of re-establishment of emergency and crisis communications policies within organizations. Over the pandemic years, organizations remodelled working practices with remote working rapidly becoming the *status quo* for many. These changes have spurred organizations to remodel their emergency and crisis communications strategies to make them fit to new working practices and, in many cases, has prompted investment in new products and services. This report seeks to help organizations benchmark how their tools, plans and procedures compare to peers, but also to encourage debate and showcase best practice for the design and implementation of crisis management plans.

2022 was a time of numerous crises: organizations were still battling the consequences of COVID-19 but most were finally opening up to the idea of business as usual (whatever configuration that may have taken for each organization). However, the war in Ukraine reminded us that peace is not guaranteed, especially as other geopolitical issues become more relevant to the operation of organizations. Weather-related events have been a big challenge for many, with some countries being subjected to wildfires and extreme flooding for the first time ever. Meanwhile, an increase in cyber attacks has been keeping organizations on their toes, and, lately the effect of the cost-of-living crisis is a factor that many organizations are having to deal with. As noted in the BCI Resilience in Conflict Report 2022¹, the current working environment of organizations is multidimensional and, because of that, many are now choosing to follow an all-hazards approach to crisis management.

This year's report has identified many positive trends in emergency and crisis communications: technology uptake to manage communications in a crisis is higher than ever, and the main tools chosen by organizations are Software-as-a-Service (SaaS) solutions which have enabled organizations to activate their emergency communications plans faster and more efficiently. In turn, organizations are demanding greater functionality from their tools as collaboration becomes an essential component of organizations' needs, particularly as crisis rooms are increasingly becoming virtual set-ups and remote/hybrid working patterns consolidate.

However, some problems remain: The main point of failure for an emergency communications plan continues to be due to the human factor, rather than technology failure. However, there are encouraging indications that institutions are stepping-up their training and exercising programmes and are seeking to better embed new technologies within their organizations to help reduce human error in the use of said tools.

Nevertheless, some of the legacy problems remain. Institutions are still having difficulty ensuring staff contact details are up-to-date, and data silos frequently remain. The wide use of spreadsheets as the tool of choice to store personnel data is not only ineffective but can lead to data breaches.

As we enter 2023, we are cautiously looking at a future where the acute organizational impacts of the pandemic subside and new challenges emerge. However, with challenge there comes opportunity, and this report shows the appetite for new technologies in the emergency communications environment such as Internet of Things (IoT) is greater than ever. Because of this, we are expecting to see organizations continue to embrace and utilise technology to help ensure emergency and crisis communications are as resilient as the plans that support them.

1. Elliott, R & Riglietti, G (2022). BCI Resilience in Conflict Report 2022. The BCI (November 2022). Available at <https://www.thebci.org/resource/bci-resilience-in-conflict-report-2022.html> (Last accessed 2 February 2023)

Section one: The toolbox





Section one: The toolbox

- Organizations are now employing digital tools to manage their emergency communications within crisis scenarios at the highest levels ever seen.
- Software-as-a-Service (SaaS) solutions have grown to a historic high, asserting its importance within emergency management situations and the broader business environment.
- Emergency communications are increasingly being handled from mobile devices with mobile phones now the primary tool for managing emergency communications.
- Professionals are going “back to basics” in terms of desirability criteria from their tools: 86% of respondents view the ability to alert and mobilize a large number of people very fast as the primary factor for using an emergency communications tool (up 14 percentage points on 2022).
- Physical crisis rooms are being rendered obsolete for some organizations with virtual/hybrid arrangements increasingly becoming the norm. Nearly two-thirds of respondents currently use a virtual crisis room.

Emergency and crisis communication tool usage is at its highest level ever

This year's report demonstrates that the use of tools and/or software for the management of emergency situations is at a historic high: 70.5% of respondents report using crisis management tools or software to manage such contexts. This represents an increase of 9.3 percentage points from last year.



Usage of emergency notification/crisis management tools or software within organizations 2018- 2023

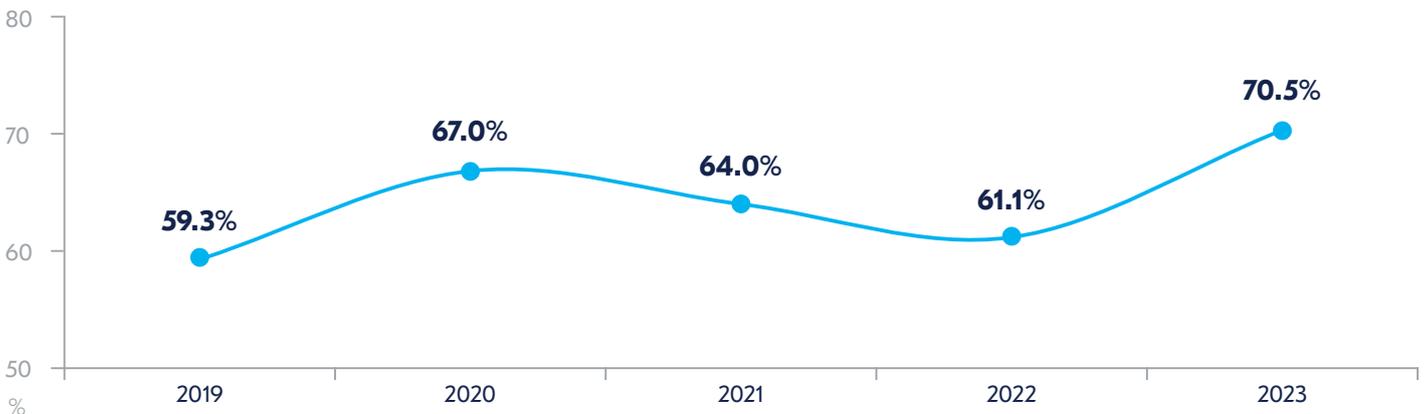


Figure 2. Usage of emergency notification/crisis management tools or software within organizations 2018- 2023

Over the last five years there has been a steady increase in the number of organizations using SaaS solutions rather than on premises installed software. The COVID-19 pandemic and the resultant mass movement of staff to remote environments has driven an increased appetite for two-way communication tools and a decrease of on site and/or one way communication instruments. Using SaaS solutions means it is easier to access emergency communications tools via a multiple range of devices and locations meaning it provides organizations with more flexibility, negates issues with legacy systems and allows updates to be made via the cloud. An interviewee from Trinidad and Tobago explained how their risk exposure to weather related events pushed them to acquire a crisis communication tool.

“We are located within the hurricane belt, and the earthquake line as well. We are on one of the fault lines across the Caribbean. These are two big things that could affect us at any time, but earthquakes could be very sudden and very destructive. So those are two things that we had in mind when acquiring an emergency mass communication notification tool. It’s actually operated out of the UK so it’s obviously remote and we can still get the service even if we have any issues with the Internet and cloud software on our side.”

Health and Safety Manager,
Infrastructure, Trinidad and Tobago

“If I go back to the pandemic, we find ourselves in a unique position with everybody working from home. We were able to use a communication platform to contact colleagues around the country if there was an issue with our major IT platforms or if there was a VPN issue. We were able to use the platform during the summer to communicate with colleagues who may have been struggling in the extreme heat to make sure they were okay and notify them that office space was available if it were struggling at home.”

Operational Resilience, Financial & Insurance
Services, UK

Current operating environments have seen a consolidation of hybrid working patterns. These new working conditions have increased the need for collaborative solutions and the data shows that SaaS is the best option to use due to its multiplatform functionality. Organizations find themselves trying to ensure staff can maintain the use of emergency communication tools in distant locations and in most cases without a computer/laptop close by. Because of this, 81.4% of organizations have incorporated SaaS as their communications tool of choice, relegating the use of on premises installed software. An interviewee from the financial & insurance sector explained how easy it was to communicate during a crisis using software, whilst an interviewee from Australia spoke how their organization uses technology for crisis management.

“Our emergency notification system or ENS tool is used all the time. It’s a major part of our emergency response communication strategy and we use it predominantly when we are dealing with an incident, an emergency or a crisis. Our IT teams also accesses the emergency notification system when normal communication methods (e.g. email outage) are not available. We have a number of people that we’ve trained in supporting us to use that tool around our network. Our people receive these messages to their work or personal devices via a link. Not unlike any business, we are dealing with a lot of issues to do with phishing, and, when people are receiving links these days they are fearful of clicking that link. We also educate our people not to click links, so we are moving towards the service provider’s app, so then our people will be confident this message is coming from us and they can access/respond accordingly. Once the app is installed our people can receive communication that way rather than, at the moment, through the link.”

Global Senior Manager Business Continuity,
Professional Services, Australia

“We can send crisis communications to multiple devices including mobile phones (text/voicemail), home phones, and desktop alerts to colleagues on their laptop/desktop. If it is still up and running it will pop up on the screen automatically. We can use one or multiple points at the same time.”

Operational Resilience, Financial & Insurance Services, UK



Figure 3. What kind of software/tool are you using?

SaaS is not only capable of deploying a solution across multiple devices, it also enables a faster speed of response and activation of crisis communication plans. In 2023, 78.2% of organizations who used SaaS as their tool of choice were able to activate their emergency communication plans within 30 minutes, compared to 58.6% of organizations using on premises solutions.

Issues with internal collaboration between IT and business continuity/resilience were a regular feature in comments. A respondent spoke how regular updates for their communications solution were issued, but as they were *“maintained locally by Service Owners”* they were *“not guaranteed to be up to date.”* In this particular case, a SaaS solution may help to solve this specific issue.

Throughout the lifespan of this report, there has been an increase year-on-year in terms of the proportion of organizations which use SaaS technology. This trend has continued this year with 81.4% of organizations now using a SaaS tool compared to 77.2% in 2020. This trend is likely to keep growing because of the benefits it brings to organizations from a flexibility, resilience and business continuity perspective. General growth in the SaaS market is also adding to this trend, with BMC reporting global expenditure on SaaS solutions rose from \$145.5bn in 2021 to \$171.9bn in 2022 – a growth of 18.1%².

2. Shiff, L. & Kidd, C. (2021). The State of SaaS in 2022: Growth Trends & Statistics. BMC Blogs. BMC.com.(online) September 17th 2021. Available at: <https://www.bmc.com/blogs/saas-growth-trends/> (last accessed 30 January 2023)

The instruments of crisis management

When exploring the devices organizations use to manage a crisis, mobile phones remain the most commonly used device, with 95.9% reporting they use them for managing a crisis situation. This figure has marginally increased year-on-year and cements the mobile phone in its position at the top of the table. Computers/laptops remain in second place with 94.0% of respondents using them to manage an emergency scenario; a half percentage point increase year-on-year. The aforementioned data shows how the enhanced functionality of mobile devices coupled with the expansion of multi-platform SaaS solutions means mobile phones have become the natural tool to facilitate the management of emergency responses. An interviewee from France explained how their organization used multiple instruments for crisis management within the organization.

“Our current software solution is mainly for mass communication. In this sense, it’s quite effective. But in the case of in-house security use only, currently we use the radios or our mobile phones as the main tools.”

Business Continuity, IT & Telecommunications, France

After these top two devices, there are no others with such universal usage. However, the range of devices which are still being used shows other communications devices still have their place within emergency communications plans.

What devices are you using to manage emergency situations?

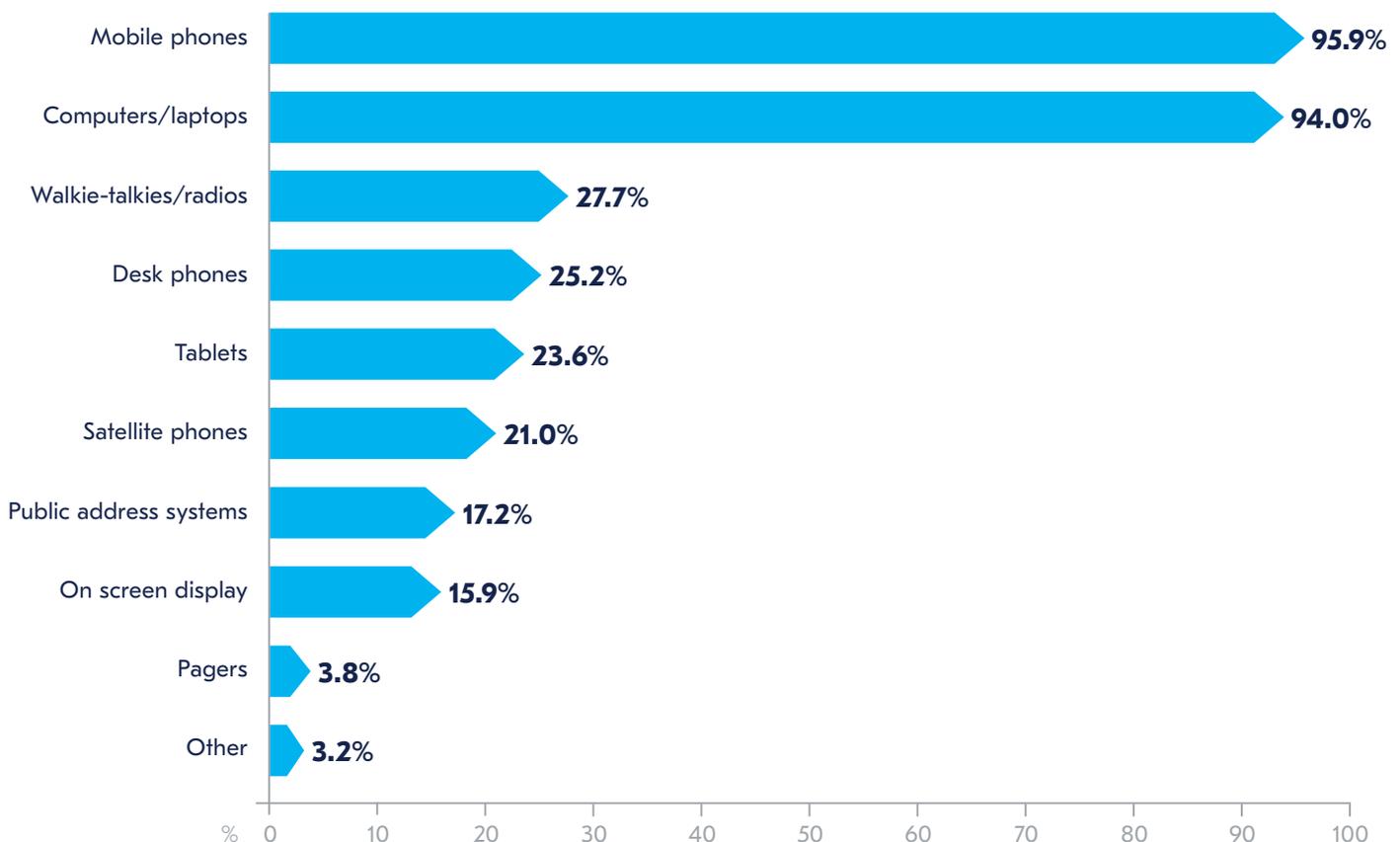


Figure 4. What devices are you using to manage emergency situations?

The overall use of walkie-talkies and radios has dropped by a negligible amount, but they have climbed one place in the table to become the third most commonly used device. After these devices saw a notable decline in their use during the pandemic as organizations turned to remote working, their use has increased as organizations move fully or partially back to on-site environments.

Evolution of the use of Walkie Talkies within crisis management plans 2020- 2023

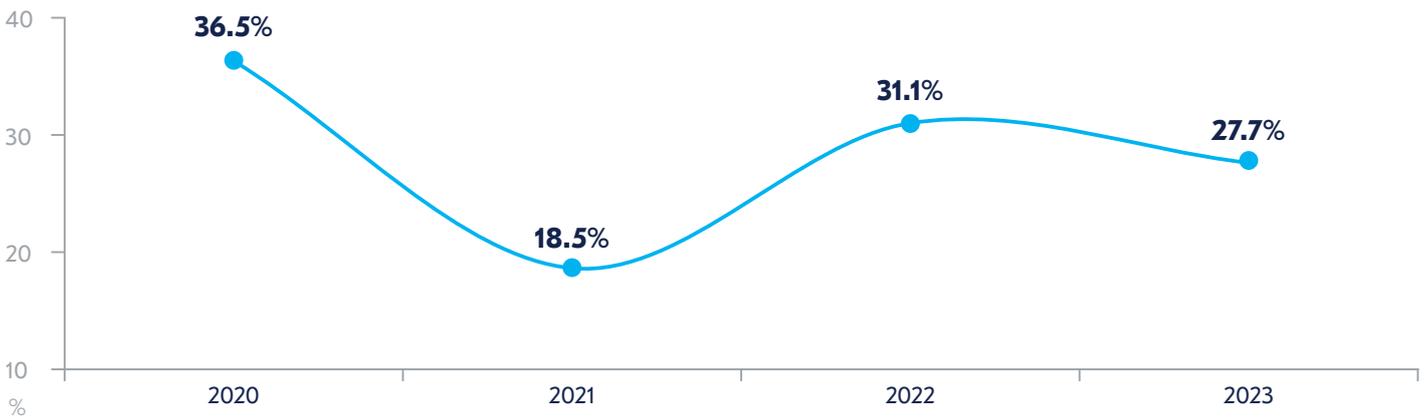


Figure 5. Evolution of the use of Walkie Talkies within crisis management plans 2020- 2023

An interviewee from France explained how his organization considered walkie-talkies an important part of their crisis communications policies.

“Like many organizations, when designing a crisis management plan, we consider imminent danger to the people and to assets. An important contribution for this emergency response approach is based on the actual physical security component of the organization. This area is doing the work through security guards, which are external services delivered by a dedicated service provider, for each of the sites that we have. Of course, since we need to communicate with them, sometimes it’s a matter of minutes. We had to put in place clear communication channels, so we use standard walkie-talkies. We use radios as well, which are very useful when the corporate communication infrastructure is down, because this is a parallel communication element put in place to address this emergency response. If we have a fire happening in our data centre for example and every communication is down, a parallel walkie-talkie solution helps us to communicate.”

Business Continuity, IT & Telecommunications, France



Interestingly however, there has been a pronounced decline in the use of tablets: their usage has fallen by 11 percentage points from 34.6% in the 2022 report to 23.6% in 2023.

Such a fall is synchronous with the overall downward trend in the tablet market. This decline is explained by many factors such as tablets being replaced by laptop/tablet hybrids (e.g. the Microsoft Surface Pro or the HP Spectre), a lack of tablet-specific updates being released, as well as changes to the operating environment. Supply chain issues, for example, have led to a mass shortage of electronic components. The tablet market has also been shaken up by the increased functionality of smartphones. Such devices have become bigger and more functional and, as a consequence, are being used in the place of tablets.³

Evolution of the use of tablets within Emergency Communications environments 2019- 2023

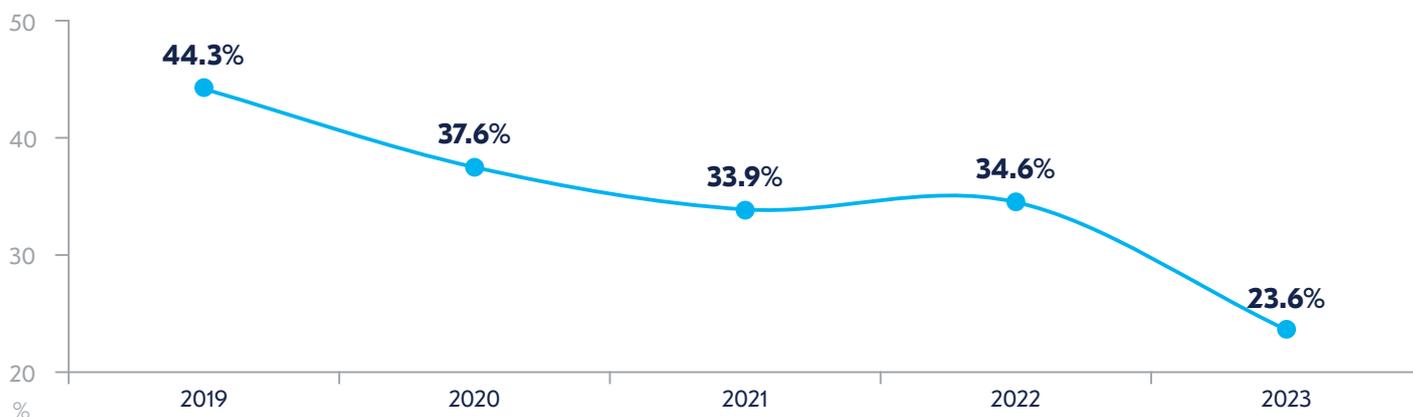


Figure 6. Evolution of the use of tablets within emergency communications environments 2019- 2023

Other methods of communication that declined in use this year are desk phones (25.2%), public address systems (17.2%), and on-screen displays (15.9%). However, although usage is low, public address and online displays are still in use in organizations that work mostly on site. An interviewee from Kenya explains how his organization still uses public address systems:

“Within the building, we have broadcasting outlets where we are able to communicate special messages. And I think this works best in emergencies that require a quick evacuation. It becomes easier to be able to broadcast a message than sending out an SMS or a call tree. Because of our challenge of actually using the manual call trees, then the public address system really works best.”

Group Head of Business Continuity Management,
Financial & Insurance Services, Kenya

³ Brooks, A. (2023) The decline of the tablet market, Top Ten Web Hosting Sites (online) January 8th 2023. Available at: <https://toptenwebhostingsites.com/blog/the-decline-of-the-tablet-market/#:~:text=For%20many%20consecutive%20quarters%2C%20the%20tablet%20market%20has,that%20includes%20Apple%2C%20Samsung%2C%20and%20Huawei.%20What%20happened%3F> (accessed: 17 January 2023)

Brown, A. (2022) The tablet market is on the decline again, Android Headlines.(online) August 4th 2022 Available at: <https://www.androidheadlines.com/2022/08/tablet-market-decline-q2-2022.html> (accessed: 17 January 2023)

Abdullah (2022) Demand for tablets in the global market declined in the first quarter of 2022, Gizchina.com. (online) April 30th 2022 Available at: <https://www.gizchina.com/2022/04/30/demand-for-tablets-in-the-global-market-declined-in-the-first-quarter-of-2022/> (accessed: 17 January 2023)

Organizations are starting to dispose of desk phones and transitioning to a web-based voice over IP solution (such as those supplied by Zoom, 3cx, or Microsoft), where there is no need for a physical telephone anymore. This trend is a more cost-effective option for most organizations, but with it opens up the possibility of being affected by downtime as they are dependent on the Internet rather than traditional copper wire connection to function; increasing vulnerability and lowering resilience. Nevertheless, with copper wire telecommunications being grandfathered in most geographies by 2030, organizations that still rely on this technology to function as part of their emergency communications plans should look towards alternatives now. For the UK, analogue communications are set to be turned off in 2025, Japan has a target of 2024, whilst Australia and New Zealand plan to complete the process imminently.

Pagers have also seen a slight decline of nearly 2 percentage points since the last edition of this report, yet they still maintain a prominent place within some niche markets. For example, people working within the healthcare system indicate that these devices' resilience and reliability coupled with the superior infrastructure available and the enhanced connectivity of these tools means they remain an essential component of their communication plans. It is important to remember that some tools, which some may consider as dated, can be crucial to others in an emergency situation – particularly when network availability differs so greatly between geographies. However, even in the health service, there is still a recognition that this type of tool will soon become obsolete.

"In the emergency ambulance domain, there is a lot of engineered resilience in the system and crews have fallback procedures to the point they do not need technology, other than receiving a notification of where to go. There is currently a national programme for the refresh of the emergency communications infrastructure being deployed. So we're moving from analogue radio to digital radio. We're recognizing the end of life of paging and enabling priority service over 2G, 3G, 4G, 5G."

Line of Business, Health & Social Care, New Zealand

There is a device that has been holding its place within emergency planning through many editions of this report. Satellite phones are employed within 21.0% of emergency communications plans, particularly in areas where there are connectivity issues or mobile networks are non-existent. Their use has increased dramatically over the last two years: when comparing the 2021 and 2022 report, there was an increase of 7 percentage points year-on-year, and this increase has increased further in this year's report. The conflict in Ukraine, increasing global tensions and adverse weather events around the world have reminded many of the importance of maintaining communications at all times, particularly in areas with little to no network coverage. An interviewee from Australia explained how satellite phones are very much part of their crisis management plans.

"We've only got two satellite phones in the firm so we share them accordingly with any local office within that region that's in an area of conflict that has enough triggers to demand potential loss of network access. If necessary due to time or urgency, we would also consider purchasing additional phones. Satellite phones, while we haven't used them so far, are very much a part of our strategy."

Global Senior Manager Continuity,
Professional Services, Australia

However, even for those who do use satellite technology, problems can still arise. An interviewee highlighted how many emergency communications apps had limited or no functionality when paired to a satellite connection which rendered certain apps obsolete.

"We use a satellite system for the Internet, it's more powerful and more functional. It facilitates hyper speed Internet in difficult, remote, locations. However, I need to have more tools to communicate when we have another crisis, and I hope that some of the big companies, some of the apps, start to function with satellite connection, because it is impossible to work with them because of the low bandwidth."

Crisis Management Advisor,
International Organization, Switzerland

Application of emergency communications tools

In which areas does your software/tool support you?

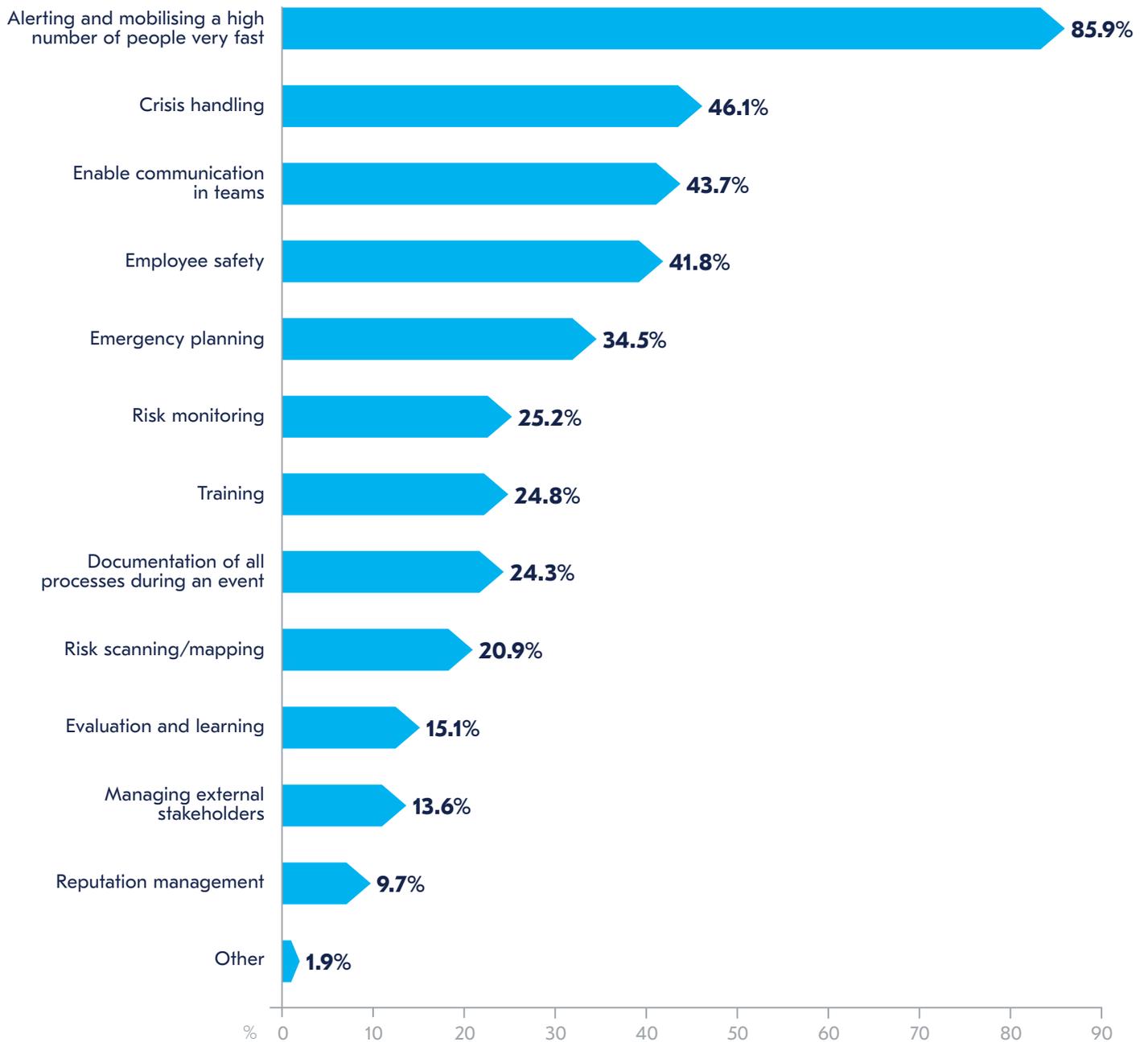


Figure 7. In which areas does your software/tool support you?

The next section evaluates the areas where organizations are seeking their emergency communications tools to support them. The main usage given to such instruments is to alert and mobilize a large number of people very quickly: more than four out of five organizations use their tools for this purpose (an increase of 14.4 percentage points since our last report). Maintaining communication within organizations is a central element of crisis planning, and it is unlikely that this will change in the future. Emergency communications tools can help to enable this effectively, by providing functionality such as tiered alerting, alerts to multiple devices and also enabling communications in a communications blackout. In this edition of our report, there is a heightened awareness of the need for tools dedicated to the aforementioned purpose which again has been driven by increased geopolitical instability and a growth in weather-related events. An interviewee mentioned the importance of mobilising people very fast, within the Ukrainian context.



“Our massive one-way communication protocol is important. For example, if we have a massive event in Ukraine we send out a communication. We also work with our team in Ukraine, our regional team in Budapest, but also we send out and a communication for information of all staff worldwide because like this we cover the duty of information which is one pillar of our duty of care policy.”

Crisis Management Advisor,
International Organization, Switzerland

An additional area where organizations are supported by their emergency communications tools is crisis handling (such as task management, reporting and updating): 46.1% of our respondents expressed that this is now one of their main uses within critical situations. A respondent commented on how their *“organization relies on multiple software applications within crisis handling: one for BC planning (plans, BIAs, risk assessments, IT/DR, and ERM) and another for emergency alerting and communications”* demonstrating how the expectations of emergency communications solutions are now far more than the traditional alerting system.

Another use commonly expressed by respondents is the ability to enable communication within teams, in order to collaborate in crisis response. This option was selected by 43.7% of respondents, and it is also demonstrated in the context of crisis rooms moving to hybrid/online settings. The increased use of collaborative technologies was labelled as critical to the success of an emergency communications strategy. Interviewees highlighted how two-way communication was now an intrinsic part of the emergency and crisis communications strategies.

There is a notable increase in concern about employee safety, and lone workers in particular. With many organizations now moving to hybrid environments, the likelihood of workers being alone in offices is greater than it has been previously⁴. As a consequence, safety is now being considered as an integral component of many organizations' emergency communications plans with 41.8% of organizations using emergency communication tools to deal with this matter (2022: 37.7%).

Emergency planning (34.5%), risk monitoring (25.2%), training (24.8%) and documentation of processes during an event (24.3%) registered medium interest within organizations. However, comments from interviewees registered that there was a lack of knowledge of these particular components being available in emergency communications tools which suggests these may be areas of unexploited interest which organizations have yet to fully realise. Areas which respondents identified as having less need by organizations are reputation management and managing of external stakeholders, with these options at the bottom of the list. Indeed, the latter two requirements concern external stakeholder management and such tasks are likely to be better addressed through specialist tools and communication experts.

⁴ Morris, C. (2022). Lone worker numbers are rising. What are you doing to keep them safe? O2 Business Blog.(online) September 9th 2022 Available at: <https://businessblog.o2.co.uk/2022/09/09/lone-worker-numbers-are-rising/> (last accessed 31 January 2023)

A third of organizations do not use any specialist tools or technologies

Close to one in three organizations have yet to explore the benefits of specialist emergency or crisis communication tools within their organizations, with some believing tools are not applicable to them at all.



Figure 8. What is the main reason for you not having or not planning to have a tool/software for emergency communications/crisis management?

When respondents were questioned about the motives for not using an emergency communications platform, the primary reason given was the lack of budget (34.8%) – which takes the first spot each year. Budget is a common problem, particularly for smaller organizations who may not perceive there is a need to invest in a multi-functional emergency communications system. Some respondents discussed how they had performed a cost benefit analysis for management to show that extra investment is likely to lead to longer term savings.

On a similar note, 15.7% of respondents said their company was too small for such a tool. If this is the case, organizations should nevertheless ensure they have a tried and tested plan in place to communicate with all staff in case of emergency and should consider exploiting the communication capabilities of in-house technologies such as Microsoft Teams or Slack. An interviewee spoke about their lack of budget and complications when trying to acquire a specialist tool whilst an interviewee from Kenya acknowledged the risks of not having an emergency communication tool:

“We don’t currently have a specialised emergency notification/crisis management tool or software basically for an economical reason, because the software in the market is designed for the big corporate sector, and they have a price that we can’t reach. Also, as an international organization, each country that we operate in has a different law, a different privacy policy, which has created some problems for us. Now we are talking to another company about their products, at the same time that we are thinking about a self-design tool, having our own tools will allow us to better manage and share sensitive information. Nowadays with social media, our communication time is faster than private sector or even mass media.”

Crisis Management Advisor,
International Organization, Switzerland

“We currently have not automated our emergency communication process. It’s manual. This means we use the old traditional call tree approach where we have a call register of all the staff with their contacts. Being a very big organization, there’s a lot of layering of departments. We find that our call trees frequently require a lot of updates even on a monthly basis and therefore, given the magnitude of that workaround, it’s quite hard to actually be able to keep up and to have up-to-date information. And therefore the risk with that is that we have staff who will not be able to receive the necessary information in terms of a crisis or a situation that requires them to give feedback.”

Group Head of Business Continuity Management,
Financial & Insurance Services, Kenya

In third place (13.5%) was the organization not perceiving the benefit of using a specialist tool. In this case, if the budget is there and the practitioner feels the organization would benefit from such a tool, showcasing the additional benefits of a tool (such as those specified by this report) could help to convince management that it is necessary. No capacity/specialized personnel and a complex implementation process were some of the other reasons stated for not implementing technology in this area. Again, these last two options were typically selected by those in smaller organizations which did not have the required specialist knowledge available in-house.

Nevertheless only 3.4% of respondents said that they were based entirely remotely so there was no need to contact staff onsite, meaning that despite the extensive move to remote and/or hybrid working conditions organizations have not steered away from having such a tool in place and recognizing its importance.

Interestingly, analysis of the 15.7% in the “other” category showed that the majority of those who selected the option are actually in the process of looking to implement a solution and/or have a lack of information on the applicable tools available. Moreover almost all organizations within this “other” label are in the process of employing a solution, highlighting the importance of speaking with industry and community peers to explore the opportunities available.

The interviews for this report showed that many organizations have a tool but are not able to use it or implement it correctly. In this regard, an interviewee from the Netherlands said they were not using all the functionality of the tool that was available, whilst another from the US explained the intricate work that had to be done in terms of organizational culture when implementing a tool, in addition to different departments requiring the tool to be used for different purposes.

“We do have plans and we do have a tool, however we are not using the functionality available through our tool at the moment. We can warn people, but only if they are in the office or if they have email available. That’s how we would inform people right now if there is an emergency situation going on. So that’s really depending on people being either in the office or having email at their discretion.”

Business Continuity Manager,
Financial & Insurance Services,
Netherlands

“I inherited a critical event management system that the institution has had for five years. However, because of the way that it was introduced and the reason it was introduced, it hasn’t really penetrated the whole organization. It’s only been used in two major centres, and these are managed reasonably separately. They have their own management teams that have adopted that critical event management software system in entirely different ways. They do use it for critical events, but one hospital uses it a lot more for other events than the other one. Across the organization, bearing in mind we have 78 other facilities, the critical event management product hasn’t been used for critical event management at all. We have a tool but we’re only using it for a limited amount of its capabilities across all of our system.”

Resilience Director, Healthcare, US

“Our critical event management system was originally purchased by IT for specific purposes, and it was never adopted universally because the way the culture of the company worked at that time. So there is no universal approach to how the tool is used or even how the tool is accessible. It’s a lack of ownership issue. I don’t think anybody actually owned the project at an enterprise level so we never investigated the opportunities to utilize its functionality. We need someone to say ‘this is how we should be implementing this’, and then make it happen.”

Resilience Director, Healthcare, US

Organizing collaboration and the move to virtual environments

When examining the topic of collaboration within organizations' core crisis teams, respondents highlighted the importance of appropriate collaboration and interaction within core crisis teams in order to elicit a quick and effective response. Such interaction has come even more to the fore now as physical crisis room environments are becoming virtual.

"As part of the COVID response, we've actually taken that as the cue to invest in working from home. It's just good resilience, future pandemic proofing, better continuity provisioning if we lose a major office. We do not have excessive people, so hybrid is the way we work. But it's also addressing the fact that New Zealand has the triple threat of earthquake, volcano, and tsunami for most regions. So it's giving that resilience in operations as well. So for us, we've actually downsized office space, we couldn't actually physically return to all on site working."

Line of Business, Health & Social Care, New Zealand

The way in which institutions manage collaboration within their crisis teams varies from organization to organization according to their own requirements and needs. 62.8% of respondents said they currently have a virtual crisis room or an online collaboration tool dedicated to crisis management, whereas just 23.9% choose physical crisis rooms and a further 13.2% who stated not having a crisis room at all. Again, the latter category largely consisted of smaller organizations. Although the question was asked slightly differently last year, 54.9% of respondents claimed that they used a physical crisis room in the 2022 report — a figure which has more than doubled year-on-year⁵.

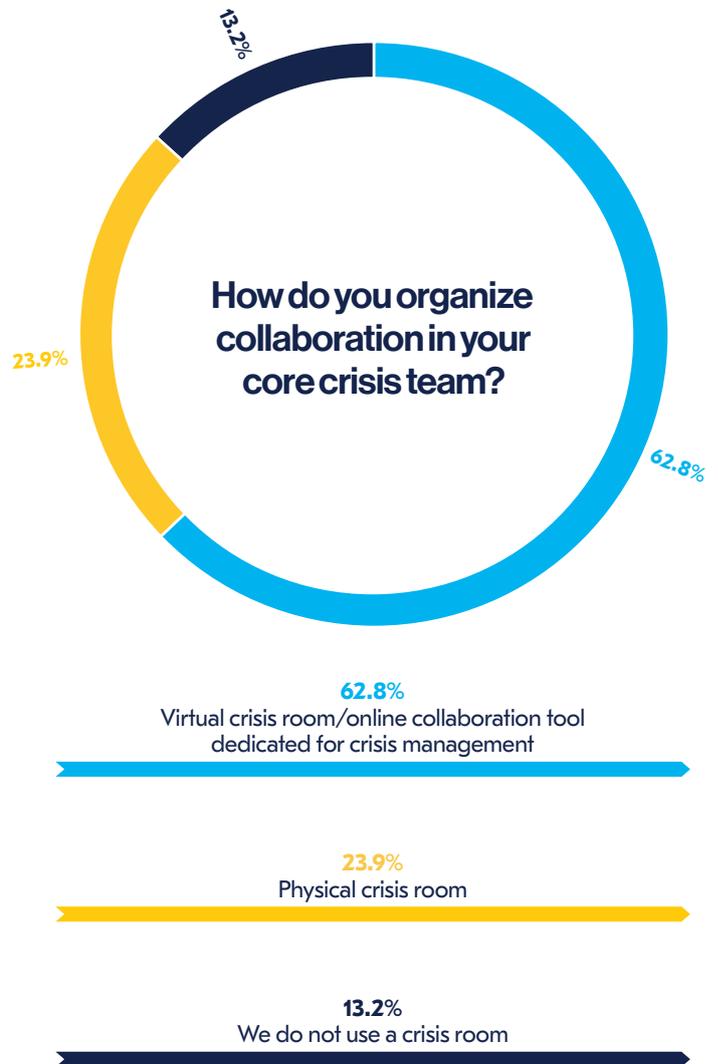


Figure 9. How do you organize collaboration in your core crisis team?

⁵ Elliot, R. and Lea, D. (2022) Emergency and Crisis Communications Report 2022 (Online). Available at <https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html> (accessed: 17 January 2023)

At the moment, the majority of institutions organize collaboration through virtual/hybrid schemes. Such an environment is likely to be the best fit for most organizations when also considering the evolution of collaborative technology and the tremendous shift witnessed in working patterns over the last four years. Physical crisis rooms are now becoming obsolete for some organizations and the virtual tools now available help core crisis team members not only make collaborative decisions across different geographies in a crisis situation, but can encourage ongoing communication and sharing of best practices, policy updates and results from training and exercising.

“Within our service desk we have a person designated as the SPOC every day; a single point of contact. Immediately we’ve identified an issue, he will or she will enable The War Room, there will be a dedicated Teams channel for that. And we just open a video session through SPOC, so anyone can call in there, live messaging is put through the there and we record the events through Teams. In our recent issue, that was not an option because we didn’t have Internet connectivity, so we immediately stepped back. The War Room became physical, we’ve got a large whiteboard already installed, so it became more of a huddle, less of a ‘from your desk’ situation. For me as duty manager, I would stay in The War Room for the duration of the outage or would be present in the service desk area. So over the next seven days, if I couldn’t join via Teams, I would just have to transit to the office. Duty managers can’t be more than one hour from the office and that’s about my average trip.”

Line of Business, Health & Social Care, New Zealand

What methods of communication do you use to communicate internally during a crisis?

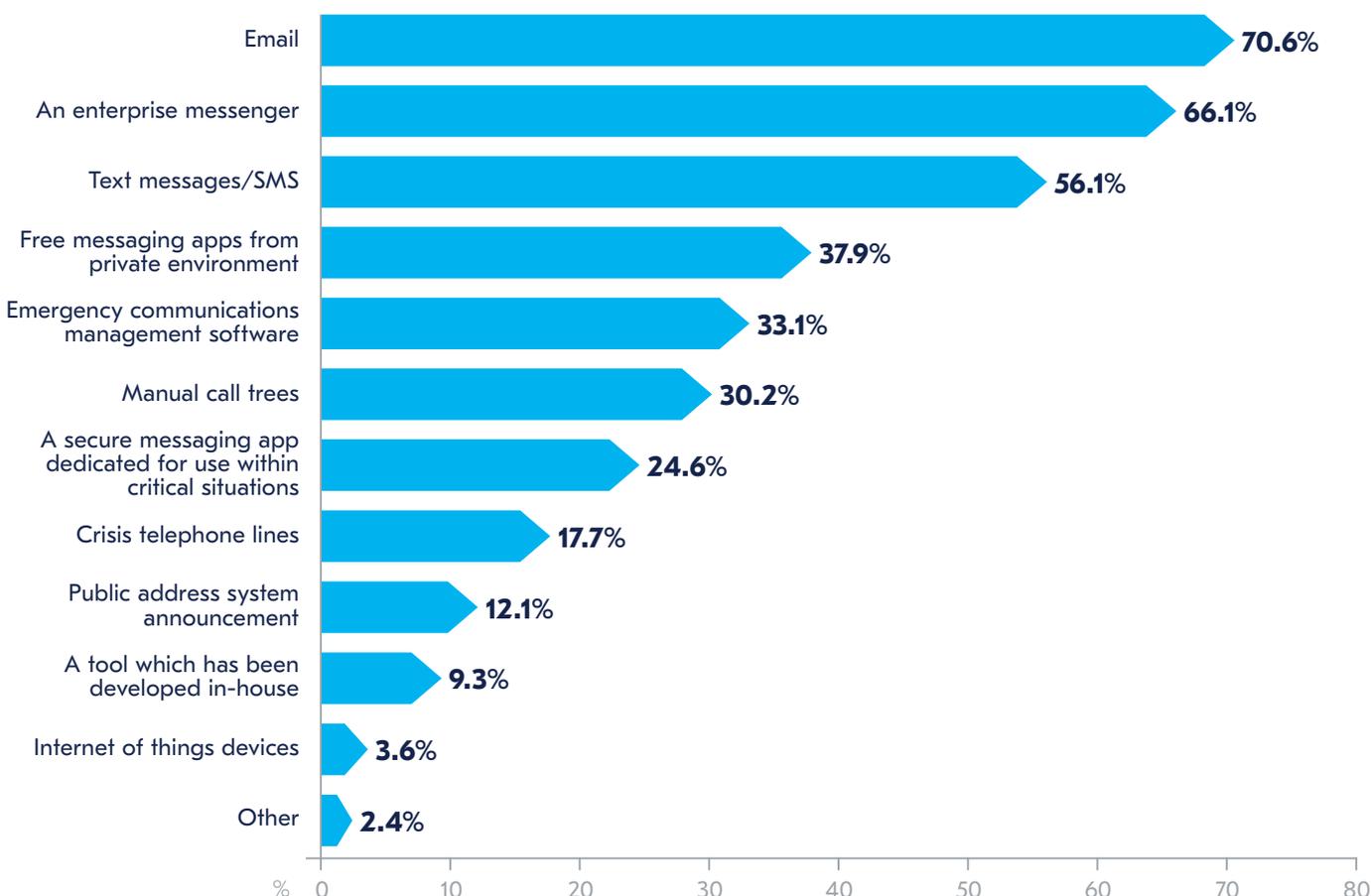


Figure 10. What methods of communication do you use to communicate internally during a crisis?

When studying the methods of communication that organizations use internally during an emergency situation, there is an increased focus in the use of various solutions simultaneously. It has previously been acknowledged in several BCI reports that this represents an attempt to increase redundancy and contingency within emergency communications plans. Indeed, layering and/or overlapping of tools and methods of communication within emergency communications scenarios are now becoming incumbent practice. In this regard, an interviewee explained how they use multiple methods of communication to ensure an effective response.

“We also use our emergency notification system to instruct response teams on next steps to communicate as a group. For example, we would send out an emergency notification to advise response teams to access the group chat on WhatsApp, or join a video chat in 10 mins on Teams. This is a super quick way of getting attention of the response team members and altering them to the unfolding event and to take action.”

Global Senior Manager Continuity,
Professional Services, Australia

Emails are, once again, the most widespread mode of communication with 70.6% of organizations using email to communicate in a crisis. However, it should once again be highlighted that using email as the sole mode of communication in a crisis is ill-advised: in the case of a cyber-attack, for example, email systems may become unstable or fail to function at all. In addition, email delivery depends on a working Internet connection, and most organizations have no method of identifying if a message has been read. Finally, communicating the importance of an emergency message in email can be difficult to do.

The second most popular option (66.1%) is the use of enterprise tools such as Teams, Slack, or Skype; used in 66.1% of cases. In the 2022 report, it was discussed how the popularity of this type of solution came to light as a result of the pandemic and organizations quickly switching to collaborative tools (such as Microsoft Teams) to communicate. Such tools are not failsafe, however. As recently as January this year, an outage of Microsoft Teams affected millions around the world showing that either a back-up solution should be employed and/or the use of an independent communication platform which is dedicated to crisis management considered⁷.

Evolution of the use of enterprise messengers within emergency communications 2020-2023

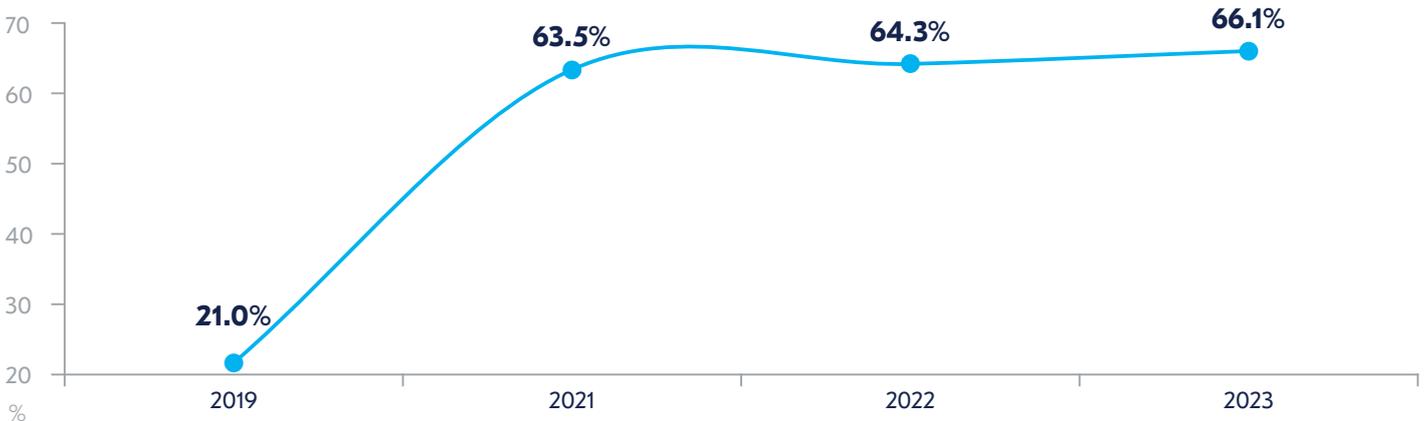


Figure 11. Evolution of the use of enterprise messengers within emergency communications 2020-2023

6 Elliott, R., Lea, D., (2021) Crisis Management Report 2021 [Online]. Available at: <https://www.thebci.org/resource/bci-crisis-management-report-2021.html> (accessed: 17 January 2023)

7 Bickerton, J. (2023). Microsoft Teams Outage Affects Millions Around the World. Newsweek. 25 January 2023. Available at: <https://www.newsweek.com/microsoft-teams-outage-affects-millions-around-world-1776339> (last accessed 13 February 2023)

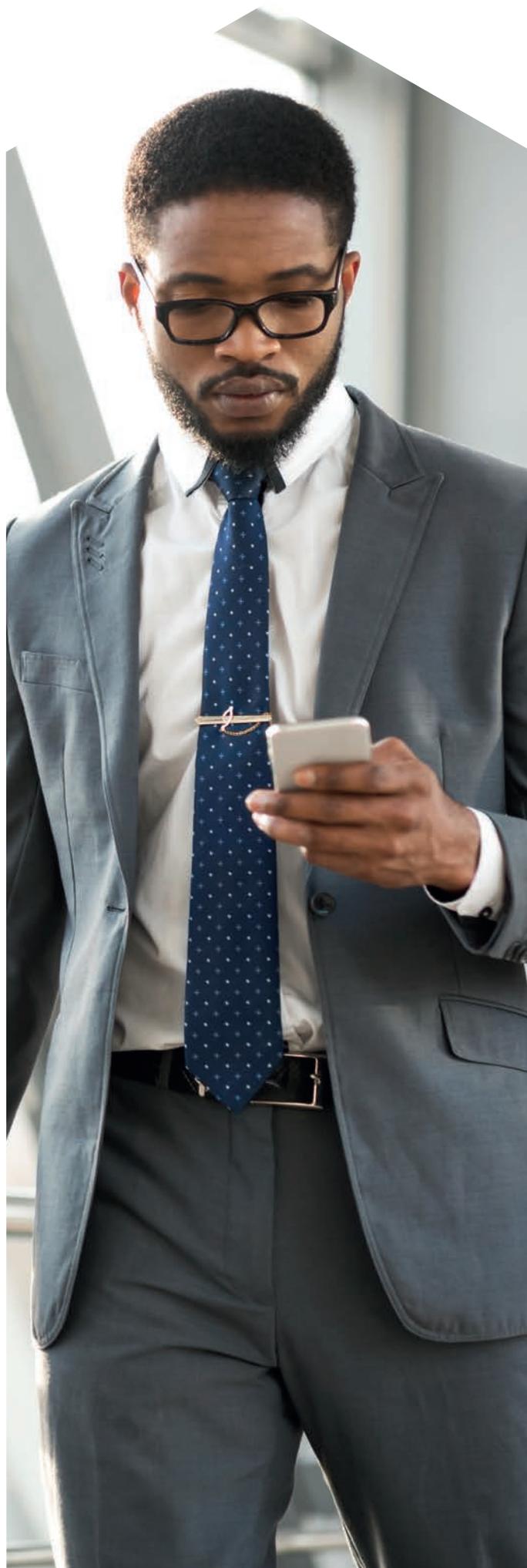
“Some people will have corporate devices, some people just are happy to use personal devices with business applications, some people may not. We just don’t know. So that’s the thing, if I choose to send a broadcast message, I don’t know what personal device people have. For me, it’s also interesting, when I worked in a government-based job, I could rely on the fact that everyone would essentially form their work around Microsoft Outlook and email would be a reliable delivery mechanism, but as I’m an NGO in this role, a lot of people base themselves through Teams. So if I send a broadcast email I no longer have confidence that the email will find everyone a) because they might not have appropriate devices; and b) because they may stay in Teams and not bother with Outlook more than once or twice a day. So that I think for a crusty like me, Outlook is my kind of happy place. But people younger than I are now, Teams is where you need to be now.”

Line of Business, Health & Social Care,
New Zealand

Text messages/SMS have taken the third spot this year as one of the most used methods of communication during a crisis with 56.1% of organizations making use of this option. Despite newer technologies (such as WhatsApp or Teams) becoming the incumbent messaging solutions within some organizations, text messages can prove to be a more reliable method of communication as messages can be sent and received in areas of low bandwidth through the GSM network and do not need an Internet connection to function.

“We can send crisis comms to people’s mobile phones, to their telephone voicemail, to their home phones, to their laptops if they’re working, to their desktops, if it’s working, so they pop up on the screen. So we can use one or multiple points at the same time. So we will send it using the app and it will come up as an SMS on their phone.”

Operational Resilience,
Financial & Insurance Services, UK



Nearly two in five organizations still rely on free apps as emergency communications tools

There has been a four-percentage point increase y-o-y in the usage of free messaging apps such as WhatsApp or WeChat to communicate in an emergency scenario. Usage figures increased from 33.9% to 37.9% and, whilst disappointing, it is still far below the 45% of organizations who reported using such apps in the pre-pandemic period.

Using such tools are often deemed as insecure in terms of information security. Indeed, WhatsApp has been labelled as one of the most hacked messaging apps, making it an insecure option not only for everyday communications but specially for real time crisis communications⁸. Also, as in the Microsoft Teams case discussed above, WhatsApp remains vulnerable to outages: in October 2022, a major outage caused tens of thousands of users to lose access to the platform⁹.

Furthermore, using free apps commonly means there is no audit trail showing if staff have received and read messages, and, if staff have turned alerts off, they may not receive the message in a timely manner — particularly if a message is sent out-of-hours. Others are likely to use free applications for personal use too which can mean notifications are missed or staff are not alerted to the importance of a message. An interviewee explored the issue of organizational culture as an issue when operating an emergency communication tool:

“So it’s not only about the tool but also about changing the mindset. How do we ask the teams to look to their mobile phones the moment we send a message out? And then you really hear people saying, “No, it’s weekend, I don’t look at my company phone,” Or, “I don’t look at professional messages.” And that’s also a change in mindset. So it’s not only the tool, but it’s also the people who need to change their mindset. But of course, since the fact that many people are working remote, we need to rely on mass notifications tool more than ever before.”

Business Continuity Manager EMEA, Manufacturing, Belgium

For some organizations however, such apps still not only retain a place within organizations, but have been widely applied within corporate environments and within institutions. This is particularly the case for smaller organizations who do not have the budget for a more advanced solution, or those who use applications for non-emergency use or “watercooler” chat that might take place during an incident (e.g. which coffee shop staff are mustering at or team-to-team chat). However, despite the challenges that free apps have in the corporate environment, their usage is likely to gain more popularity over the next year. There was widespread reporting in January 2023 that WhatsApp was going to allow users to connect to the service via proxy servers so they can remain online if the Internet is blocked or disrupted by blackouts¹⁰. The latest news, combined with its cost, convenience and universality will all help to continue to drive use within organizations.

8 Crises Control (2021). WhatsApp for emergency communications is a bad idea. Crises Control. 21 January 2021. Available at: <https://www.crisis-control.com/blogs/why-using-whatsapp-for-emergency-communications-is-a-bad-idea/> (last accessed 17 January 2023)

9 Toh, M. (2022). WhatsApp suffers major outage. CNN Business. 25 October 2022. Available at: <https://edition.cnn.com/2022/10/25/tech/whatsapp-outage-service-down-intl-hnk/index.html> (last accessed 13 February 2023)

10 McCallum, S. (2023) WhatsApp to enable messaging in internet blackouts, BBC News. BBC.(online) January 5th 2023 Available at: <https://www.bbc.co.uk/news/technology-64175966> (Accessed on 17/01/2023)

An interviewee explained the approach in regards to the use of WhatsApp within their organization:

“Although, officially, WhatsApp is not an approved communication tool within our company, everybody is using WhatsApp and it works very well in the environment where we have the, let’s call them “the non-wired associates.” These are employees without a corporate phone. We communicate with them very efficiently via WhatsApp. For example, last year there was a big weather storm coming and it was going over a part of Europe where we have a number of manufacturing plants. We had to close a few of these locations to protect our people, mainly because it was also dangerous to go outside on the roads. Our efficiency rate reaching them via our dedicated tool was 20% versus around 80% via WhatsApp.”

Business Continuity Manager EMEA, Manufacturing, Belgium

Evolution of the use of WhatsApp within emergency communications 2019-2023

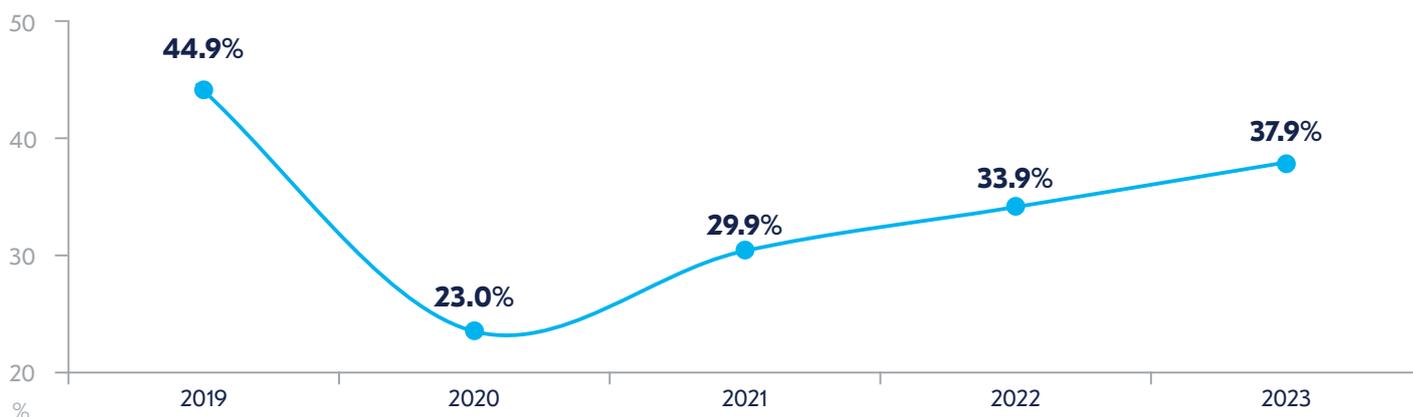


Figure 12. Evolution of the use of WhatsApp within emergency communications 2019-2023

Dedicated emergency communications management software and secure dedicated messaging apps are also two widely used communication methods, with emergency communications management software being used by a third of organizations (33.1%) and secure messaging apps used by a quarter (24.6%). Such technologies have advantages over their free alternatives for the reasons outlined in figure 10.

“I use amateur technology because in essence, we don’t want to be stuck with some software that maybe in some of our contexts won’t work. We started with a technological process update. Later we detected that the proposed solution wasn’t working with the satellite connection. Most of the time, we work in a country where you have an Internet satellite connection. We are very difficult! And for this reason, we decided to take a dramatic approach and use some of the solutions that are easy, less costly, but also very impacting in the life of our colleagues. This is our approach.”

Crisis Management Advisor, International Organization, Switzerland

Organizations using free solutions are unhappy with their tools, whilst those using dedicated solutions are the happiest

When analysing core collaboration, the right solution for each organization is unique. This is reflected in the ways organizations arrange collaboration and the tools used for this purpose. However, with cost frequently the deciding factor, organizations are finding that tools are not fit for purpose and this year satisfaction levels have fallen. Only 40.5% of respondents answered they were happy with their solution, with the remainder either unhappy or registering some degree of dissatisfaction. The percentage of those happy with their current arrangements increased to 16.2% (2022: 13.4%) whilst 43.3% said they were “somewhat happy” with their solution (2022: 44.0%).

When considering the type of tool used and the levels of satisfaction, there was a stark difference between the levels of satisfaction. For those using free messaging apps, less than a third (28.5%) were unequivocally happy with their solution, whilst 40.3% of those using an enterprise messaging solution had the same view. The only solution with more than 50% satisfaction was for those using dedicated messaging apps (53.3%). With just 11.7% saying they were not satisfied, this shows that whilst free messaging apps can be a good solution for some, the superior options available through enterprise solutions and dedicated apps lead to higher satisfaction levels. Indeed, dissatisfaction with free tools was more than double than of dedicated applications. Free applications are also unlikely to be personalized to organizations’ requirements, as well as not providing user support.

Are you happy with your tool of choice?

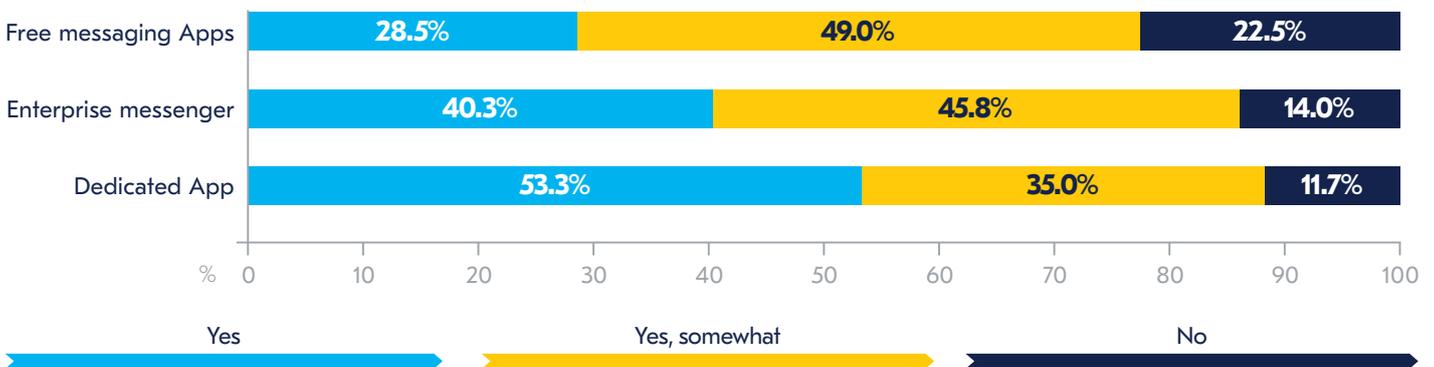


Figure 14. Are you happy with your tool of choice?

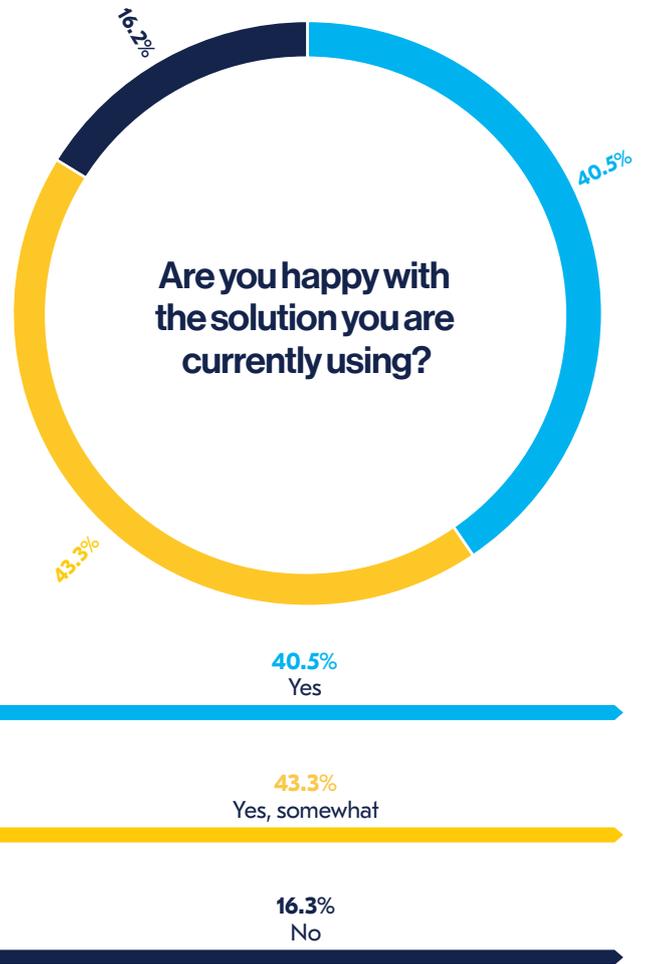


Figure 13. Are you happy with the solution you are currently using?

For those respondents who claimed they were only “somewhat happy” with their method of communication, the concerns raised were almost identical for all three solutions: a desire for better integration with alerting scenarios, a need for more functionality and problems with battery life drain on devices. One interviewee discussed how this battery life drain was a problem, whilst another discussed how a problem with their solution was two apps failing to communicate effectively with each other.

“We have two apps but they don’t communicate with each other. So on one app, we have an alert system which allows us to communicate, but this is limited to the management team, and then we have to go to another tool, to communicate widely to the whole organization.”

Business Continuity Manager EMEA,
Manufacturing, Belgium

“I’ve got a work app on my work phone and I’ve noted battery life got nobbled by it. When I would normally get a four-day charge, now I get about a day and a half, I think because of the global location system. So yeah, it’s reduced the battery life, but it’s very good in context, we’re all happy with it. I have a long experience of health applications to work for the local hospital for many years, and sometimes it is a case of fine-tuning in light of experience. My feedback to the organization was ‘Hey, wonderful thing. Just noting, my phone does not last as long, which reduces my resilience. If I lost power, I’m going down from four days to one.’”

Line of Business, Health & Social Care, New Zealand

When asked about “other” reasons, one respondent said that *“there was no integration between their crisis alert and crisis management tools.”* This was a problem raised more than once and shows how important it is for solutions (where possible) to have the ability to integrate with existing applications such as Apple iOS apps or the Microsoft Office suite of products. Another reason indicated by respondents was that tools were not being used to their full potential. One respondent explained how they *“have all the functionality needed, but the application is not used to its full potential.”* Such problems can arise when, for example, the application is bought and installed by IT, but the business continuity manager is not given full access to the tool to a) test its capabilities and b) personalise the tool to the crisis management requirements of the organization. This highlights the importance of ensuring regular contact is made between the product buyer/owner and those resilience professionals who will be managing the crisis communication plans.

In relation to enterprise messengers, a respondent said that *“MS Windows-based notification is compromised if the two-factor authentication function is not available due to lack of Internet access.”* The same respondent also pointed out that their organization *“has differing communication protocols for clinical and corporate issues.”* This makes the usage of any chosen tools even more challenging and either requires two separate apps which can integrate with each other, or purchasing a solution which is fit for all purposes.

Meanwhile, another respondent stated that *“the tool used does not facilitate wide scale scenario or situation data collection. It’s simply used to pulse information out from a centralised source to employees. It is unidirectional.”* As mentioned previously, organizations are moving more towards two-way collaborative communications solutions for the management of emergency communications and this particular note of dissatisfaction again shows a disconnect between how the resilience professional believes a solution should be employed vs differing organizational requirements.



Two interviewees also spoke about problems with different data protection policies within different jurisdictions.

“We are looking at different countries with different data protection rules and so on, so this is always a challenge for those who would like to be informed, but don’t have a corporate email or mobile phone. This is the problem with every emergency tool you buy on the market, it’s that you cannot connect a person if they are not linked within a corporate network. So that’s a little bit the problem that we have with every tool. Even if we send text messages, I can only send text messages to whoever has a corporate mobile phone. But again, you will not reach those who don’t, so that remains always the same issue.”

Business Continuity Manager EMEA, Manufacturing, Belgium

Some organizations have been able to personalise enterprise messaging systems and embed them within the functionality of a dedicated solution. However, many found they were not able to do this as the required expert knowledge, human resources and/or IT resources were not always available. However, whilst some organizations may look to develop in-house software, it is not always the best route to take. A respondent commented on this particular aspect: *“We have jointly developed a pan-Essex solution for local government and emergency services which involves sharing data. A single partner feels unable to share data, which significantly reduces the solution’s efficacy.”*

Another problem cited by an interview was that of data privacy and adhering to GDPR in terms of data storage. This was particularly relevant to a large multinational organization where data requirements differed according to each jurisdiction.

“Most of the solutions available in the market consist of putting the data in their cloud. We are obliged due to the GDPR to make sure that the cloud is physically in the EU. Quite a large number of the tools, especially the ones not developed by an EU member state, have their cloud located outside their countries, including in the US and maybe even countries like China and others. This is discarded by us from the beginning because of legal compliance issues.”

Business Continuity, IT & Telecommunications, France

Tool requirements

The previous section showed how some practitioners are unhappy with the tools they have for their emergency and crisis communications, and much of this is because there is a gap between the business requirements of a tool and the reality of the product that is available. Respondents were asked to scale eleven functionalities of emergency communications tools to gauge the most crucial functionalities.

Despite the talk about collaborative communication, one-way communication is the function which most practitioners now see as “critical” for organizations. “One-way mass communication” heads the table for the first time since the question was adopted into this survey in 2018. 48.6% of respondents chose this aspect as critically important for their alerting and emergency communications plan. Within a context of fast-changing challenges such as weather-related events, geopolitical tensions in different areas of the world (for example, the war in Ukraine) and local issues (such as power cuts), the capability to inform all relevant parties of the existence of an imminent situation and encourage them to keep safe has become critically important for organizations.

Whilst collaborative communications are vital – particularly in today’s interconnected world – getting a message out quickly to all those affected (and potentially affected) by an incident can become a matter of life or death in certain situations.

Interestingly however, when considering both the “critical” and “very important” options within the scale, one-way mass communication moves to fourth place and the podium is dominated by more collaborative aspects of emergency communication tools. In the current context of remote and hybrid working environments, emergency communication systems should ideally include some degree of collaboration within their functionality.

Technology is also expected to help facilitate expert teams to collaborate easily and in real time, and enable the constant exchange of information to help in the decision-making process. More than a quarter of respondents rated these two options as “critical” or “very important” within their organizations.

Functionality of emergency/crisis communication tools: “Critical” and “Very important” Aspects (top four)



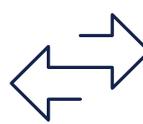
77.2%

Effective communication with remote teams



75.8%

Enable expert teams to collaborate easily and in real time



75.7%

Constant exchange of information to enable decision making



71.3%

One-way (mass) communication

Figure 15. Functionality of emergency/crisis communication tools: “Critical” and “Very important” Aspects (top four)

This analysis shows that whilst one-way mass communication is the most critical aspect of a tool, the collaborative and information-sharing aspects are those which are likely to become crucial aspects of the decision-making process when purchasing a tool for an organization.

Last year, the table was headed by constant exchange of information to enable decision making. This year, that option has fallen to third place. However, this aspect of crisis management tool functionality still holds great importance for organizations: 75.7% of respondents said this was a critical or a very important part of their emergency communications tool.

As demonstrated by the growing popularity of choosing collaborative tools during a crisis (technology uptake it as a historical high), being able to work together during an emergency (be that with experts, colleagues or top management) continues to be key to a co-ordinated, multidepartment response and ensures key stakeholders are able to remain informed at all times during a crisis.

How important are the following aspects for your alerting and emergency communications?

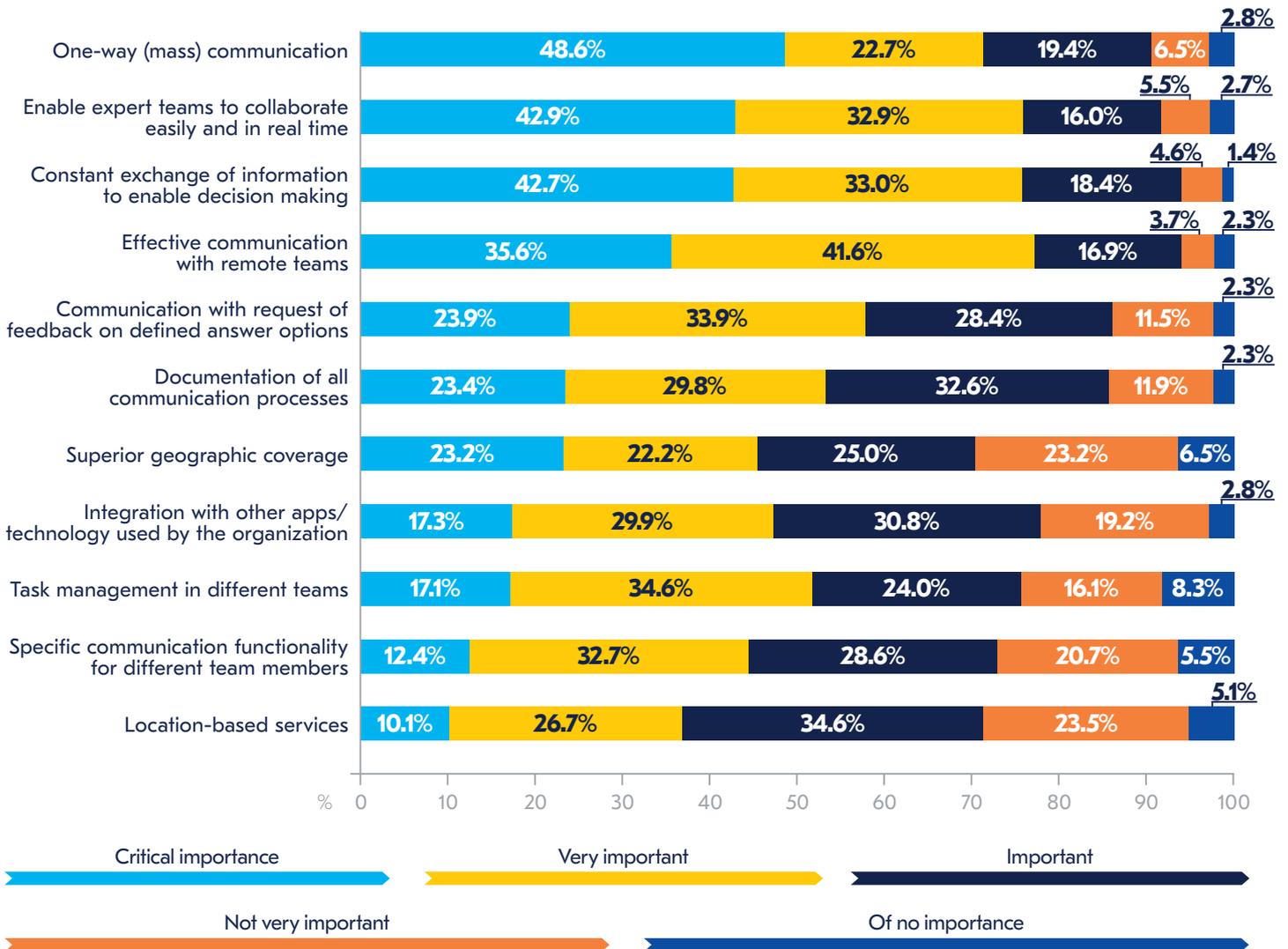


Figure 16. How important are the following aspects for your alerting and emergency communications?

Within the less critical options of emergency communication tools, location-based services, specific communication functionality for different team members, integration with other technologies used by the organization and task management in different teams all appear near the bottom of the table. Interestingly, location-based services was not selected as “critical” by any respondents, despite this particular function being mentioned in interviews as a desirable aspect for locating workers during an incident. A respondent said that “sharing GPS coordinates for emergency services teams” has become more important since the pandemic. Two interviewees also mentioned the issue of geofencing:

“Geofencing is not an issue for us yet. We are able to enforce that, especially across our employees, just to be able to ensure that we do know where they are. It’s for their safety. It’s not an issue for us, however I think as the market matures we will have to search the best way to actually be able to align with new regulations to ensure their privacy is not abused in that particular process.”

Group Head of Business Continuity Management, Financial & Insurance Services, Kenya

“We have recently rolled out an app which people can carry on their mobile phones. It has a broad context, where it geolocates and senses any kind of general incident or emergency. So if there’s significant disruption to the roads through a road traffic accident or land slip, you’ll not get notified of that. Also civil unrest or other environmental issues that may affect your ability to work. It also carries an emergency messaging system, so we can push out.”

Line of Business, Health & Social Care, New Zealand

A developing landscape means evolving tools

Considering all the changes in organizations’ working environment worldwide, it is no surprise that the requirements for emergency communication tools have also changed. On this question, more than half of respondents (51.2%) said that their view of what was needed from their crisis management tools has changed.

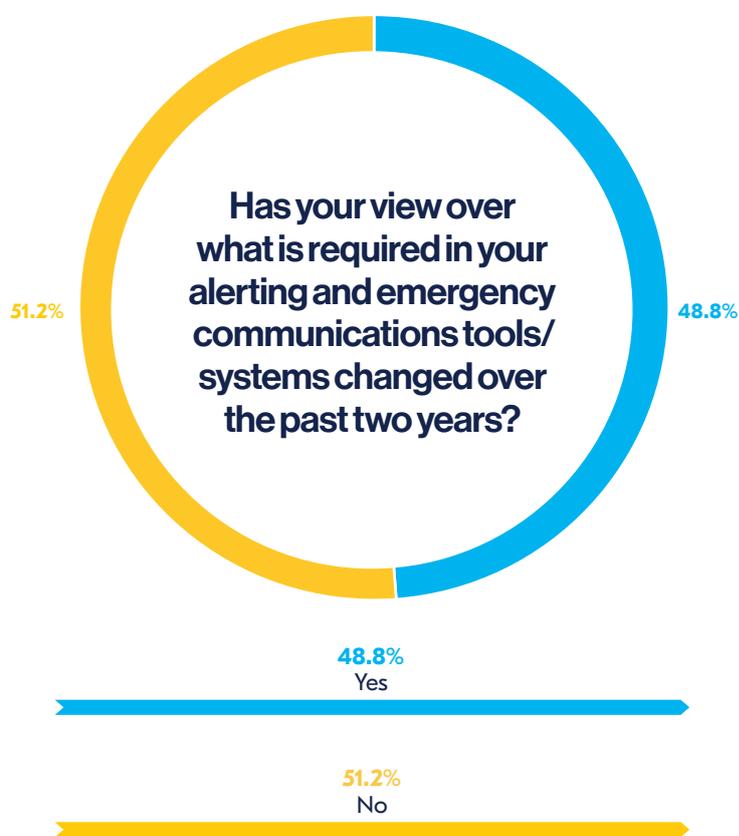


Figure 17. Has your view over what is required in your alerting and emergency communications tools/systems changed over the past two years?

Some organizations had a robust system in place before the extensive changes in staff and the business working environment took place as a result of the pandemic and more contemporary challenges. Respondents commented that they have had to adapt their systems to new environments. One respondent explained how the changes had helped to push through changes to their practices as hybrid working had become the norm: *“remote workers are less of a concern as [we] now operate a hybrid working model and most employees work from home and systems have been updated to accommodate this.”*

However, other organizations had had to shift or redefine their working arrangements and, with that, their emergency communications plans and the tools they will need to execute those procedures. Some of the major changes that respondents highlighted have been themes in the *BCI Emergency and Crisis Communications Report* in recent years: integration and consolidation of existing tools, requirements for instant remote communications and moving away from reliance on SMS/emails and free messenger apps. Six primary themes emerged from the comments made by practitioners:

1 Increased importance of remote communication tools:

There is now an increased desire to have tools which can facilitate real-time communications cross-geography within an integrated system. The ability to be able to communicate effectively to remote staff has become key. One respondent said that *“previously remote communications were less important due to people being located within primary sites.”* Another described how *“remote communication tools [have become] more important, being agile in managing remote teams, which were working together physically before the pandemic.”* Meanwhile, the quotes in the previous section demonstrate just how important tools such as geofencing are, even though it was rated low on the table. Hybrid working has also brought challenges to the communications environment as an interviewee pointed out.

“Hybrid working is a challenge; from a technology perspective you’re relying on colleagues updating their personal data to ensure that we can communicate with them accurately. Historically if you are in the building, you communicate verbally, and put up signage posters in the events with incident information. Now you’re dealing with a workforce that spread across the country, you’re more focused on technology going wrong than a building being unavailable.”

Operational Resilience, Financial & Insurance Services, UK

2 More collaboration within organizations:

There is a need to be more interconnected within organizations and to reduce the siloing of information within specific departments. For emergency/crisis communications, this typically means regular communication and information sharing between HR, IT and business continuity/resilience. On this point, one respondent highlighted the need to work collaboratively: *“Needs to link in with central HR records and these records need to be kept up to date. Both are a challenge”*

On a positive note, some organizations have made progress in terms of collaboration. A respondent explained how *“what was once a dedicated tool for emergency and crisis situations only managed by the BCM team is now being expanded more formally to be used by other incident management teams across the organization.”*



3 Move towards more sophisticated tools to manage emergency communications:

Organizations are moving away from reliance on SMS/emails and free messenger apps towards more appropriate and sophisticated tools to manage crises. Some organizations have now made the transition from a free messaging app to an enterprise messenger successfully. One respondent commented that *"comms is rather easier now as we have adopted Teams as our comms tool for the business overall - something that was kickstarted by the pandemic and which may not have happened without the need to be able to work efficiently from remote locations."*

However, having an enterprise messenger is still not enough for some organizations to effectively execute an emergency communications plan. The use of reliable communication tools has become a crucial part of crisis management for some. On this topic, one respondent expressed that they *"really require a better communication tool other than using current email, SMS (WASP) services & WhatsApp groups."* Another highlighted that *"the need for automation and communication procedures"* was key within their organization.

Better integration with other systems has been an issue also highlighted. There is need for tool integration within organizations, and one respondent highlighted *"the need to have these systems interfaced with the BCMS or as part of a BCMS solution as well as traveller tracking and risk intelligence has become apparent, so that there is a one stop shop solution - which allows incident teams to have a more holistic overview when managing a situation."*

Another participant stated that *"The more integrated approach across emergency communications software, interfacing with risk monitoring functionality as well as BC software, is to be encouraged as this would ensure more effective activation, management, documenting and recording of events for incident command teams without some of the gaps in process that can occur when using different systems for incidents that teams more currently use at present. A number of vendors appear to be moving in this direction, some more quickly than others though - as I expect that these developments will come via acquisition rather than development in many cases."*

4 The need to test systems more regularly:

Comments resonated around the point that once a system is installed, it needs regular inspection to ensure updates are installed and it remains fully functional. One respondent said that they had to redefine policies because of new working environments, *"especially preparedness and readiness of strategies for sites, people, infrastructure and applications."*

5 Organizational re-engineering

Some respondents reported that they have had to do a comprehensive review of their emergency procedures and how to work in such scenarios, frequently prompted by an emergency. One respondent said that *“triggered by an increasing crisis frequency, we have reviewed and restructured our entire crisis management system, mainly by having more operational staff in the crisis management team and less top management involvement in the crisis management itself. Crisis management is now nearer to a military “command and control” structure.”*

An interviewee meanwhile talked about the positive impact of the COVID-19 pandemic in the restructuring of the organization's emergency plans

“COVID-19 was really good to help us reinforce the importance of our emergency systems. Previously it was easier for us to use fire wardens or floor wardens to help rally people and get them outside. But now everyone's working in a different location, the emergency response system enables us to contact and communicate with our people regardless of their location and/or time of the day. This change in how and where people work has just made our emergency communication system even more important and more frequently used.”

Another interviewee mentioned the profound changes in organizational culture and re-engineering that happened post-pandemic and how this is still impacting their organization:

“We had a lot of people joining the organization during COVID-19, and it was quite complex to familiarise them with the organization, to understand the culture of the organization, and to teach them what they are supposed to do if they receive a certain communication. Our tools were not enough to give them the necessary knowledge and the practical experience to do that. The system wasn't configured for our needs due to the fact that we don't have the same working culture that we used to have before COVID-19. We're still struggling as an organization to really identify what the best communication strategy is in this post-COVID period to address all the needs of the organization. For example, in the last few weeks, we've been informed by the national authorities that they have put in place a system where they may cut some of the areas from consuming electricity so that the overall electrical grid will be up and running. So, imagine we have people teleworking, and if they are teleworking at home, everything goes down, and it might not be so easy for them to come on site. We need to find a solution to cope with this situation where they don't have electricity, which is quite complex if everyone is not present in the same place. We are trying still to adjust to post-COVID scenarios.”

Business Continuity, IT & Telecommunications, France

6 Cost effective solutions:

A theme that has resonated throughout the report is the desire for a cost-effective solution and this also came through in this particular question. Respondents emphasized the need for a cost-effective solution above all, particularly small organizations who feel a costly solution is not applicable in their situation.

Section two: Triggers and execution of plans





Section two: Triggers and execution of plans

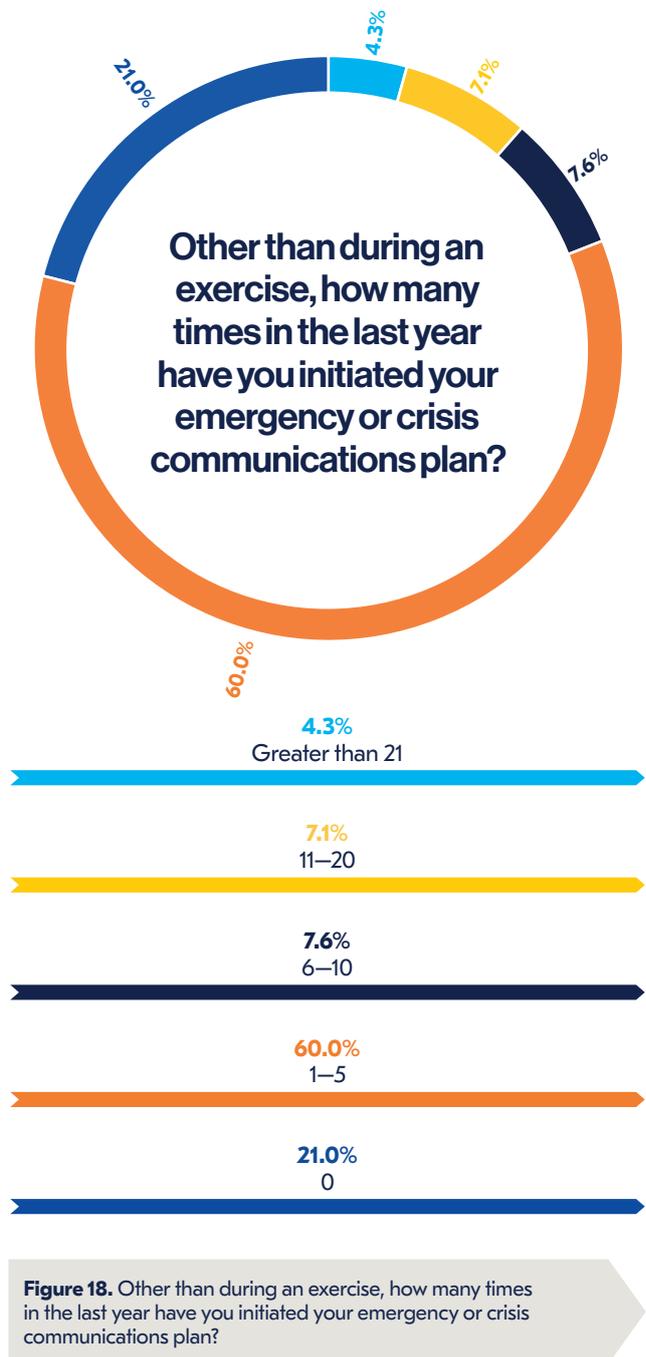
- The main triggers of emergency communication plans are weather related events and IT/ cyber incidents. Disease outbreak only accounted for 28% of cases during 2022.
- 92% of organizations are able to activate their emergency communication plans within 60 minutes, with 73% of those being able to do so within 30 minutes. One in four organizations are now able to activate within the “golden five minutes”.
- Those organizations who use specialist software are able to activate their plans quicker: 77.1% of organizations that use technology can activate their plans within 30 minutes compared to 48.6% who do not.
- Providing information to senior management takes longer and is typically not automated, due to the need to corroborate information.
- Three-quarters of organizations are achieving their expected response levels when triggering their emergency communication plans.

Activating emergency communications plans

When analysing the number of times organizations have had to initiate their emergency communication plans in the last year, numbers are similar to the 2022 edition of this report. 21.0% of respondents reporting that they did not have to initiate their crisis management plans at all in 2022. Whilst non-activation of plans is likely to be seen positively by management, constant reinforcement of the importance of testing and training needs to be highlighted so the organization remains prepared when an activation does occur.

Nearly two-thirds of organizations (60.0%) had to trigger their emergency communication plans between one and five times in the last year, a figure comparable to recent reports. With hybrid working now in place and some organizations reverting entirely to an on-site environment, there has been a small increase in organizations having to activate their emergency plans more frequently during 2022. 7.6% of organizations had to execute their emergency communication plans between six and ten times (2022: 6.1%), and 7.1% of organizations triggered their crisis management plans between 11 and 20 times in the same period (2022: 5.4%).

There has been a marginal fall to 4.3% in the number of organizations that have had to activate their plans more than 21 times (2022: 5.4%). This suggests that the upheaval in organizations during the pandemic period when multiple activations had to be made as a result of staff illness, for example, has started to level off.



Triggers

The main cause of emergency communication plans being deployed within the last 12 months is due to weather. Adverse weather initiated nearly half (49.4%) of organizations' crisis management strategies. With weather related events becoming more frequent as a result of climate change, this trend is likely to continue until organizations begin to incorporate long-term resilience to climate-related events within their resilience plans – something which the *BCI Severe Weather and Climate Risk report* shows that organizations are not yet considering seriously. An interviewee from Kenya spoke about the need to activate emergency plans because of weather related events:

“Recently we had flooding issues which really disrupted the public transport in the area of Kinshasa. In terms of people getting to work, it has been quite a challenge and we had to activate our emergency plans.”

Group Head of Business Continuity Management,
Financial & Insurance Services, Kenya

Last year the table was led by disease outbreak, but this year that has fallen to fifth place with 28.3% of organizations saying an outbreak has caused an activation of plans. Organizations are now used to managing the risks posed by COVID-19, and business-as-usual can now be maintained more effectively – even if the virus is still widespread in communities.

In 2022, an IT or telecoms incident was the second most popular trigger of emergency communication plans (43.3%) which represents a slight increase on 2022 (42.0%). There have been a number of newsworthy outages of IT and telecommunications this year: a Canadian mobile and Internet giant had a 15-hour outage in July 2022 which led to critical disruption to phone lines (including emergency services)¹¹, and the most recent Microsoft 365 outage in January 2023 caused multiple services to go down without warning (including Teams, Exchange and Outlook)¹². With outages rising on a global scale¹³, resilience professionals need to ensure that they can continue to communicate in case of a network outage: sending an email to inform all staff about a network outage might seem like an obvious mistake to avoid, but a number of professionals interviewed how they have received an email from IT about an outage – but only when systems are back up and running again.

Cyber-security incidents and data breaches, closely related with the two aforementioned issues, are in fourth place in the table this year, with 34.4% of organizations citing this as a reason for activating their emergency communications plan. Cyber incidents are likely to remain a primary cause of activations for the indefinite future as attacks continue to grow in quantity and sophistication.¹⁴

11 Honderich, H. (2022). Rogers outage: Why a network upgrade pushed millions in Canada offline. BBC News [online]. 20 July 2022. Available at: <https://www.bbc.co.uk/news/world-us-canada-62174477> (last accessed 2 February 2023)

12 Milmo, D. (2023). Microsoft investigates outage affecting Teams and Outlook users worldwide. The Guardian [online]. 25 January 2023. Available at: <https://www.theguardian.com/technology/2023/jan/25/microsoft-investigates-outage-affecting-teams-and-outlook-users-worldwide> (last accessed 2 February 2023)

13 Uptime Institute, The. (2022). Uptime Institute's 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short. The Uptime Institute [online]. 8 June 2022. Available at: <https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening> (last accessed 2 February 2023)

14 Elliott, R., Lea, D., (2021). Cyber Resilience Report 2021 [Online]. The BCI. Available at: <https://www.thebci.org/resource/bci-cyber-resilience-report-2021.html> (last accessed 23 January 2023)

Main triggers of emergency communications plans in the last 12 months



Figure 19. Main triggers of emergency communications plans in the last 12 months

“Our service supplier noted that a node had failed, and only 12 corporate clients were assigned to that node. So in their world, 12 is very minor. We were a P3 for engineering support. We had a very robust conversation at that point over a much higher priority. As I say, okay, it’s great news for us, we’re one of 12, not one of 200, but bear in mind, that node took down a lot of national resilience to other things where ambulance services might be useful. So we, at that point, aligned and agreed if we escalate to that service provider, they won’t even debate, they will go to the priority we tell them.”

Line of Business, Health & Social Care, New Zealand

In the matter of civil unrest, an interviewee from Kenya explained how this was a very current issue for his organization.

“I think with the current scenario with Eastern Democratic Republic of Congo that we are seeing coupled with the conflict that we have with the M23 rebels in city of Goma are causing quite an impact for us. It’s an active situation right now where we have actually activated our emergency communications plan to be able to monitor closely what is happening on the ground to be able to safely evacuate our staff into Rwanda. It’s an area where, right now, we are really looking at those particular plans that we need to be able to deploy.”

Group Head of Business Continuity Management, Financial & Insurance Services, Kenya

Reasons for activation at the bottom of the list may be viewed as less of a risk than others. However, each organization has a different risk profile and activation reasons will be very different between organization to organization and country to country. Interruption to utility supply, for example, was a reason for activation for only 16.7% of organizations. However, disruption to energy pipelines in Europe means activations are becoming widespread. In the case of civil unrest, a cause for activation in 16.1% of organizations, some interviewees in conflict regions discussed that such activations can be a near daily occurrence. Elsewhere, non-weather-related natural disasters (e.g. earthquake) activated plans for 16.1% of organizations, supply chain disruption and fire to 14.4% of organizations each, armed conflict to 12.8% , and workplace violence to 11.1%.

An incident that does feature on the radar of most organizations, especially of those operating in highly populated areas, is that of accidents related to overcrowding. A recent example of this is the “human avalanche” that recently happened in Seoul, South Korea and sadly concluded with many lost lives. In this respect, an interviewee explained how her organization launched their emergency communications plan to help ensure staff were safe.

“The emergency response is immediate, easy to use and quick to understand if your people are safe and accounted for. For example, in the incredibly sad and tragic crowd crushing incident in Seoul, our office is located in close proximity to the popular area, and our local Seoul office response team was concerned there could have been some of our people caught up within that incident. So we sent out a message to all our local people acknowledging the incident and for them to reply back that they were safe. Initially, we had four people out of our Seoul office that didn’t respond. So we concentrated on reaching them, and we can rebroadcast additional messages out of the emergency system very quickly. In the end there was one person that we couldn’t get hold of. This was about 15 minutes after we sent the first message, so HR then followed up with their tools (eg emergency contacts) to confirm this person was also safe. The emergency system allows us to focus and use our energy to concentrate on ‘exceptions,’ and immediate communications. This was a good example of when we needed to move quickly to ascertain critical information. We would equally use this to communicate, share updates, or alerts to be received to all our people immediately, and as events are changing. So we consider speed of communication and managing exceptions is critical when responding to an incident or emergency.”

Global Senior Manager Business Continuity, Professional Services, Australia



Which of the following triggered your emergency or crisis communications plan in the past twelve months?

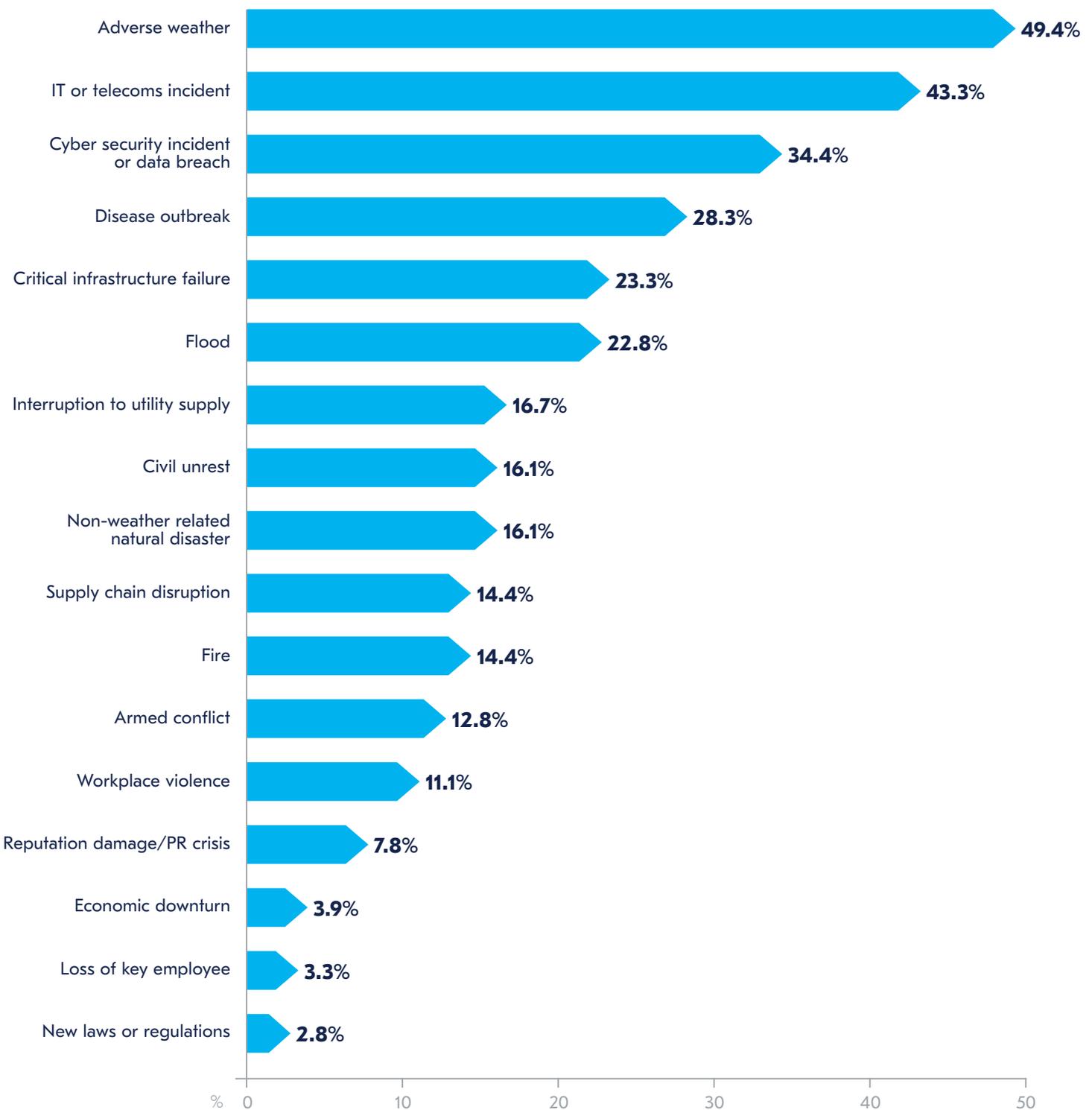


Figure 20. Which of the following triggered your emergency or crisis communications plan in the past twelve months?

Response and timing

Organizations are now faster than ever at activating their crisis management plans. Most organizations can activate their incident response within 30 minutes and, as noted in previous reports, the “golden hour” is rapidly becoming “the golden five minutes” as more organizations are able to activate their plans very quickly. Informing top management is normally achieved within a few minutes of activation, demonstrating the importance of good, agile organizational collaboration.

On average how long does it take to activate your emergency or crisis communications plan?

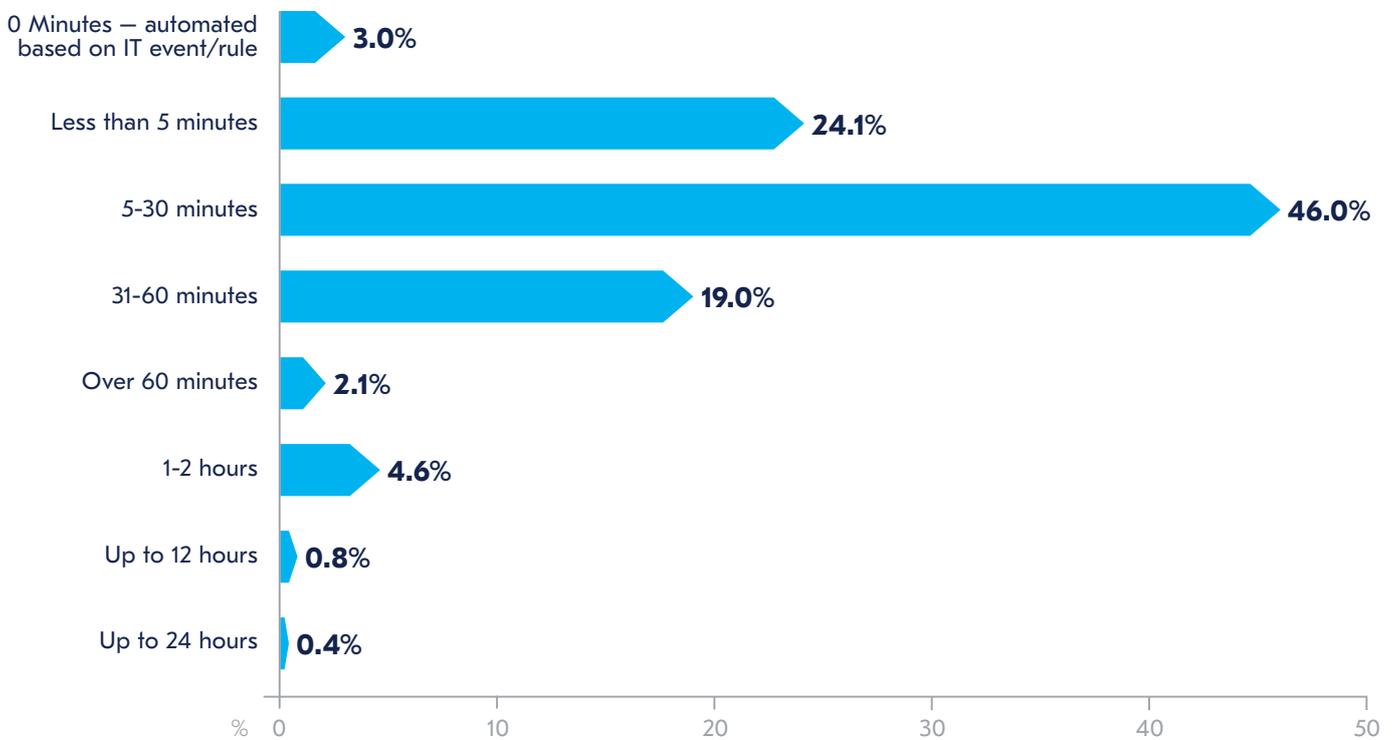


Figure 21. On average how long does it take to activate your emergency or crisis communications plan?



92.1% of organizations are able to activate their plans within 60 minutes, and 73.1% are able to do so in 30 minutes. Indeed, as response times are getting faster and most organizations are able to activate plans within the “golden hour,” many are setting their activation target times lower. Nearly a third of organizations are now able to launch their crisis management plans in five minutes or less, and “the golden hour” is now such an achievable target for most, the “golden five minutes” might now be a preferred target to aim for.

Whilst the “golden five minutes” might be a new aspirational target, it should be noted that there has been a notable decline in the number of organizations able to activate their plans within five minutes. This year, 27.0% of organizations were able to activate their plans within five minutes compared to 40.8% at the height of the pandemic. It was noted at the time that plans were activated less during the pandemic due to low numbers of staff being present in the office and, because of this, plans tended to be quicker to activate. Nevertheless, the number of organizations able to achieve the “golden five minute” target has grown by more than two percentage points this year and, given the progression organizations are making in the sophistication of their emergency communications tools and procedures, it is likely this figure will rise over the next year.

Furthermore, 3.0% of organizations have incorporated automated responses. This number, however low, has quadrupled during the last year and shows that organizations are harnessing technology (such as Internet-of-Things devices) to help with the decision-making process.

Evolution of “the golden five minutes” 2020-2023

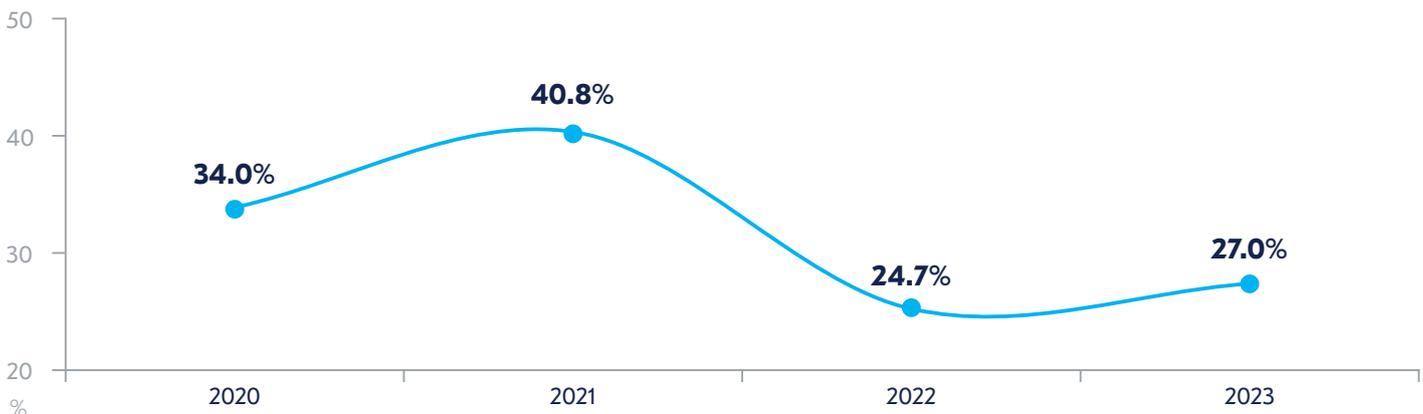


Figure 22. Evolution of “the golden five minutes” 2020-2023

“So typically within five minutes, if there is a technology issue, we’ll either have noted it through alerting or in the case of network down, we’ll just go “Ah, the lights are off, what do we do?” The next 30 minutes it is really confirming the diagnostics and beginning to think about recovery times and getting that into a concise message. Top-level management will be notified upfront, as we may need them to authorize some activity, but there will be a short gap, if any, between that notification and broadcast communications. We do have to think carefully because what we might communicate to corporate side might be quite different to what we might communicate to ambulance side. Corporate might need a richer message with instructions on what to do or what to expect. Ambulance might, depending on the situation, have an automatic response, so we don’t need to tell them or we might just need to tell them how long to keep going in standby mode.”

Line of Business, Health & Social Care, New Zealand

Current crisis scenarios go beyond the situations considered during the COVID-19 pandemic. The risk landscape is now more multifaceted, constantly developing, and more challenging for organizations than in recent years. Indeed, resilience professionals now have to manage not only what is left of a pandemic and its consequences in the business environment, but also manage the impact of increasing climate-related events, growing cyber related issues and geopolitical risks, as well as the day-to-day business risks organizations are exposed to. Furthermore, double- or triple-whammy events are becoming more widespread meaning organizations have to react to more than one incident taking place at the same time. All these lead to making the management of crises and the development of emergency communications plans all the more complex.

Technology is a valuable aid in ensuring the correct messaging can be delivered during a crisis. There is a direct correlation between the speed of response and the usage of tools or software in the management of emergency communications plans. This year, 77.2% of organizations that use emergency communications software are able to activate their plans within 30 minutes, with 33.8% being able to do so in less than five minutes. For those without tools or software, less than half (48.6%) can activate their management plans within 30 minutes and just 7.1% within five minutes.

	Organizations using emergency communication tools	Organizations not using emergency communication tools	% difference for those using software vs those who do not
Organizations capable to activate plan within 5 minutes	32.8%	7.1%	+25.6%
Organizations capable to activate plan within 30 minutes	77.2%	48.6%	+28.7%

Figure 23. Time taken to activate plans for those organizations who do use specialist emergency communication tools vs those who do not

The time it takes to provide information to top management typically differs from the time it takes to activate the plan. 85.0% of organizations are able to do this within an hour, and nearly two-thirds (64.3%) are able to do this in less than 30 minutes.

“What we usually do when we have an incident, by just a few clicks on the button, we can activate our crisis response plans, which is in our business continuity software. But we need a little time to gather and validate the information, to be able to provide feedback to our management team. Usually, it takes 30 to 60 minutes. In real life, of course, what happens is that if there is an incident, it immediately gets notified and our mobile phones don’t stop ringing because, of course, our top management wishes to have some feedback. But what I usually do is say, ‘Listen, let us collect the facts and we will report back to you ASAP.’ It gives us a little bit of breathing time with the local team, to gather all the facts together before we go to our top management team, with some feedback.”

Business Continuity Manager EMEA, Manufacturing, Belgium

Emergency communication plan activation is typically triggered before information is provided to senior management. In order to ensure an incident is not a false alarm, information needs to be verified – as quickly and efficiently as possible – before it can be passed to the top of the organization. When relaying complex information, there is a human element that inevitably will take more time than technology. An emergency communication tool can help to speed the dissemination of this information and also provide a faster pathway to get the relevant information to top management: 68.9% of organizations that possess an emergency communication tool were able to provide information to top management within 30 minutes, compared to 52.1% of organizations that do not use technology within their crisis management plans.

This year has also seen a 0.8 percentage point increase in the organizations’ ability to inform top management within five minutes of activating emergency communication plans. Now 15.9% of respondents report they are able to provide the information quickly, compared to 15.1% in 2022.

However, in 2021 almost one in four organizations were able to provide information to top management within five minutes. This downward trend is likely to have to do with the development of a more complex working environment for organizations and the need for gathering, validating and sharing accurate information, one of the main challenges during a crisis, pointed out by respondents. Indeed, in the 2021 edition of the *BCI Emergency Communications Report*, it was highlighted how senior management were extremely nervous about the “new” virus that was spreading around the globe and were keen to get information on potential outbreaks as soon as they happened. This inevitably led to false alarms and this, coupled with the increase in misinformation and fake news, means management are now requesting information to be verified and corroborated before it is passed on.



Figure 24. On average, how long does it take you to provide initial information on a crisis to top management?

Ready, set... go! Putting plans in action

The average number of times organizations achieved their expected response levels in 2022 was 74.3%. The 2021 and 2022 editions of this report both had answers that were slightly higher, but the 2023 figure is still greater than it was pre-COVID. This is impressive, particularly given organizations have changed their ways of working and many have introduced new emergency communications systems into their workplace environments to better address the new challenges of communication. Some survey comments suggested that organizations are also setting themselves tougher targets to meet and, as a consequence, are finding it more challenging to meet those targets.

Organizations that use an emergency communications tool have better response levels when triggering their plans in real life than organizations that do not use technology to manage crisis scenarios. To exemplify this, organizations that use technology were able to meet their expected response levels 76.0% of the time, compared to 68.0% who did not.

Response levels evolution 2018-2023

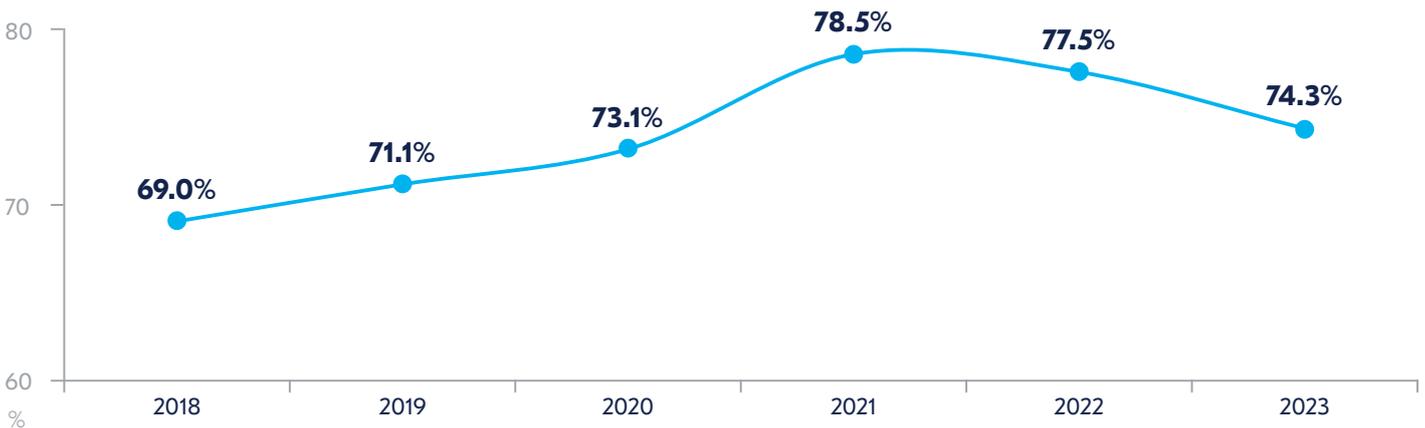


Figure 25. Response levels evolution 2018-2023

Knowing the reasons why emergency communication plans did not achieve the expected response levels is of key importance in order to incorporate lessons learned into plans so the same failures do not occur again.

As noted year-on-year, the primary cause for not meeting expected response levels is not down to technology but is caused by the people involved in the response. This year, almost half of organizations (46.2%) blamed their failure on the lack of accurate staff contact information. The difficulties encountered when engaging with HR for contact information (often due to privacy requirements) has already been discussed, as has the continued tendency to store information in Excel spreadsheets which require manual updates. Meanwhile, a lack of understanding from recipients is in second place this year, suggesting insufficient training is being carried in some organizations to ensure staff know how to react to an activation of an emergency communications plan. It has been noted in this report in the previous two years that training and exercising levels fell during the pandemic: organizations were activating emergency communications with such frequency, extra training and exercising was viewed as too time intensive by management. The continued position at near the top of the table shows that this lack of training and exercising is now having a negative effect on the success of emergency communications plans. With office environments undergoing substantial change in the past three years, organizations should now actively be reviewing, updating and rolling out training and exercising programmes so staff know what to do in their new setting.

In terms of lack of understanding, an interviewee explained his experience with low levels of response and how it was intricacies with technology which were leading to a failure of human response.

“We have the statistics and each time we send a message out, we get very, very low response. One of the elements that came to my attention is that if we sent out a message to email addresses, the people get in the subject of the email the word ‘ext’ (meaning it’s coming from an external resource, not from within our company) and for many people, this is suspicious because they say: ‘Why do I get a company email from outside?’ So they consider it a spam. So we tell them: ‘No, listen, we will try to remove it, but if you see it’s coming from this certain app and our company you still need to open it’. And what we also see is that during office hours we get better responses than outside office hours. In weekends, it’s very difficult to get people engaged to open their emails and to see what’s coming in. So that’s why our emergency response levels, are very low.”

Business Continuity Manager EMEA,
Manufacturing, Belgium

Failure of manual processes were the third most likely reason for organizations not achieving their expected response levels, with a quarter of respondents choosing this response (24.6%). Again, this is another people-related failure, and shows just how much this — rather than technology — is the dominant force in plans failing. The first technology-related failure is found in joint-third place however, with “unavailability of mobile network” cited by nearly a quarter of respondents (24.6%).

Problems communicating the urgency of the response required was ticked by 22.8% of respondents. This is one of the issues which is most discussed by respondents and interviewees, particularly those who do not have a dedicated system in place. The use of Teams or WhatsApp in a crisis, for example, can result in users not taking note of emergency messages due to the platform also being used for other communications. A dedicated solution — which some organizations have created by exploiting the functionality available on enterprise messaging solutions — helps to portray the urgency of the situation due to the channel used.

Another problem related both to people and technology is that of accurate staff roster information. Again, a problem that may originate from the use of spreadsheet software to store contact information, or a lack of regular updates to the emergency communications system from HR. This accounted for 17.5% of responses. Poor implementation was cited by a further 16.4% of respondents, and exemplifies the importance of having in-house expertise or dedicated support from a system provider to rollout and maintain a solution effectively.

Other causes mentioned were staff working remotely (15.8%) and lack of technical expertise in using the process (14.0%). Lower in the list are the more technological issues of internal IT failure (10.5%) and device failure (7.6%). Time zone changes and language barriers were at the bottom of the list; reasons that are reducing year-on-year as platforms become adaptable to global environments and, in many systems, offering support in local languages.



If you failed to achieve your accepted response levels, what caused the failure?

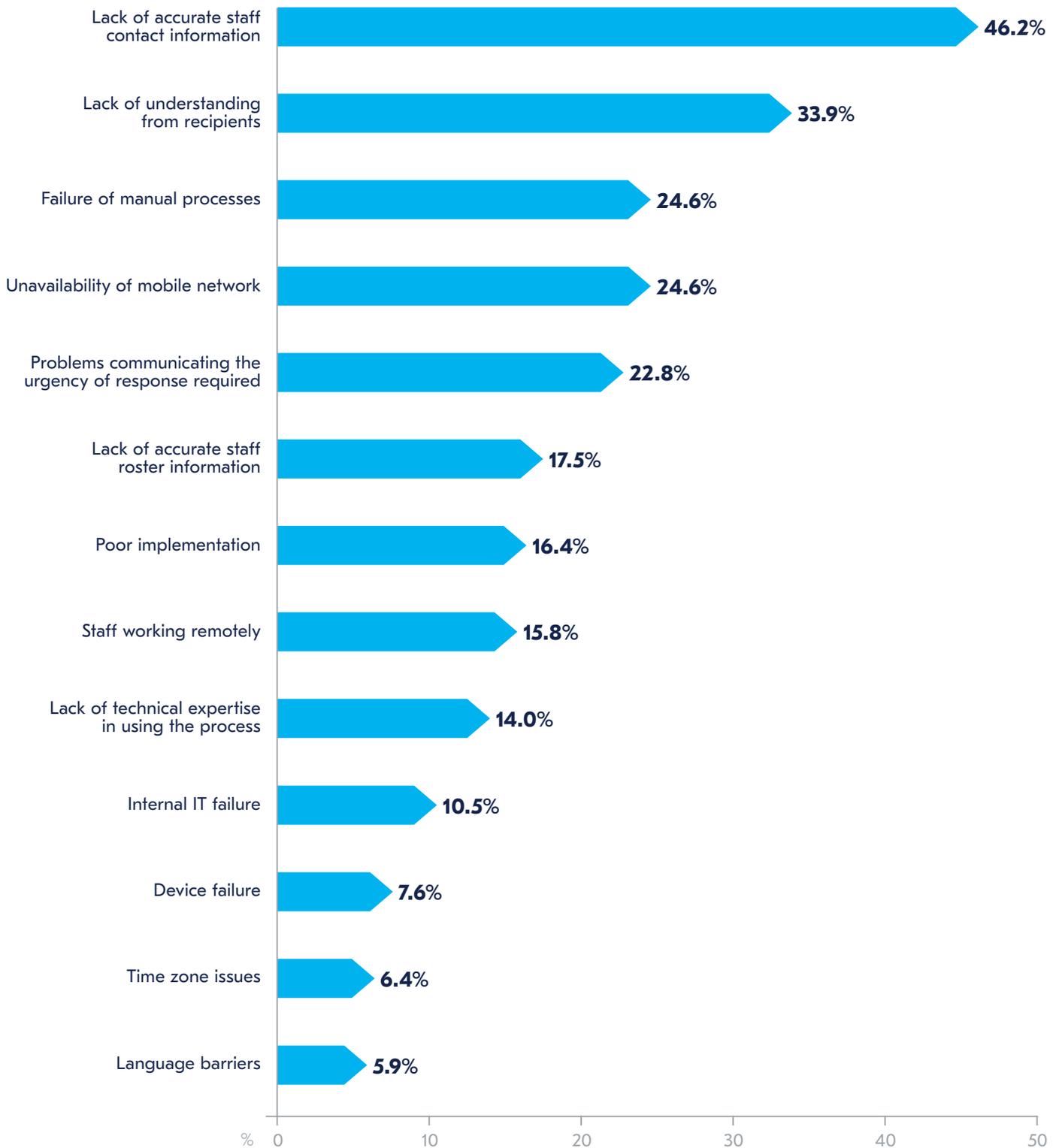


Figure 26. If you failed to achieve your accepted response levels, what caused the failure?

However, whilst a message from an emergency communications solution might portray the importance of the message, one interviewee explained how employees still ignored messages from crisis management tools, often believing they were spam. Such activity suggests insufficient training in the matter which, in this case, was for remote staff.

“To give you an example, if you work in a factory, there is an alarm. You just sound the sirens and everybody hears it and they know how to get out. But if people are working from home, then you need to find another way to connect with employees. And you need to find a tool which is also used by different teams. I mean, in business continuity or in crisis communications, for us it’s easy because we know the tool is there. We use it, maybe not daily, but weekly. So if something comes in, you pay attention to it. People who are not used to getting a message, they are not trained to receive these kinds of messages. For them, it can be considered as spam.”

Business Continuity Manager EMEA,
Manufacturing, Belgium

As mentioned previously, one of the primary reasons for emergency communications plans failing to achieve acceptable response levels is because of lack of accurate staff contact information. In order to delve further into the detail behind this, respondents were asked how they ensured staff contact details were kept up-to-date.

As expected from the results of the previous question, the top two methods for updating contact information are via manual lists (e.g. spreadsheets) (43.5%) and communication with HR (39.5%). Both methods involve manual processes which can mean information becomes out of date, is not compliant with data protection laws, is held in areas which cannot be shared or can result in errors when data is transferred from one source to another. In fact, the manual update of contact information as a method to manage employees’ details has risen by three percentage points compared to the 2022 report. Although a fairly small percentage, the lack of progress in the automation of employees’ data in recent years is disappointing, especially given the progress made in technology.



An interviewee from Kenya explained how data protection issues remained an issue in their organization, but they had found a way around it by creating a “middleman application” that provided emergency systems with limited information, but did not disclose the full data.

“HR is the custodian of information and keeping contact details up to date. At the moment they give us only specific information, they don’t disclose everything, it is just based on the call information that you require to be able to make the engagement. They have created a middleman application that sits in between the main system that is able to house the limited information that we require, without fully exposing all the information.”

Group Head of Business Continuity Management,
Financial & Insurance Services, Kenya

Meanwhile, another interviewee explained that their organization still had to make manual updates as they had two systems in their organization which were not compatible with each other.

“We keep our employees’ contact details up-to-date manually because we have different systems which are not integrated.”

Business Continuity, IT & Telecommunications, France

However, not all organizations make manual updates and 38.5% of organizations do have HR systems which automatically update emergency communications systems — albeit a three-percentage point decrease on 2022 data. Automatic updates allow systems to be updated with human error, and also ensure details within emergency communications systems are as up-to-date as HR records.

A further 17.0% of organizations use automated requests to update contact information via emergency notification systems as a way to keep employees’ contact details up to date. Whilst this is a good method of ensuring employees update their information, it does put the onus on the employee who may not update their information as readily as the system prompts them to. Nevertheless, an interviewee in Australia explained how embedded such a process was in their organization and it worked very effectively.

“Our emergency response tool allows us to ensure every 24 hours it updates all our people’s contact details out of our HR systems. Your personal mobile, your work mobile, your personal email, your work email, it uploads every 24 hours. This ensures that if we’ve had any change to contact numbers/details, or movement in people starting, leaving, moving from office to office or transferring between geographies, every 24 hours we know it’s going to be up to date.”

Global Senior Manager Business Continuity, Professional Services, Australia

How do you ensure contact data of employees, experts, etc. is up to date?

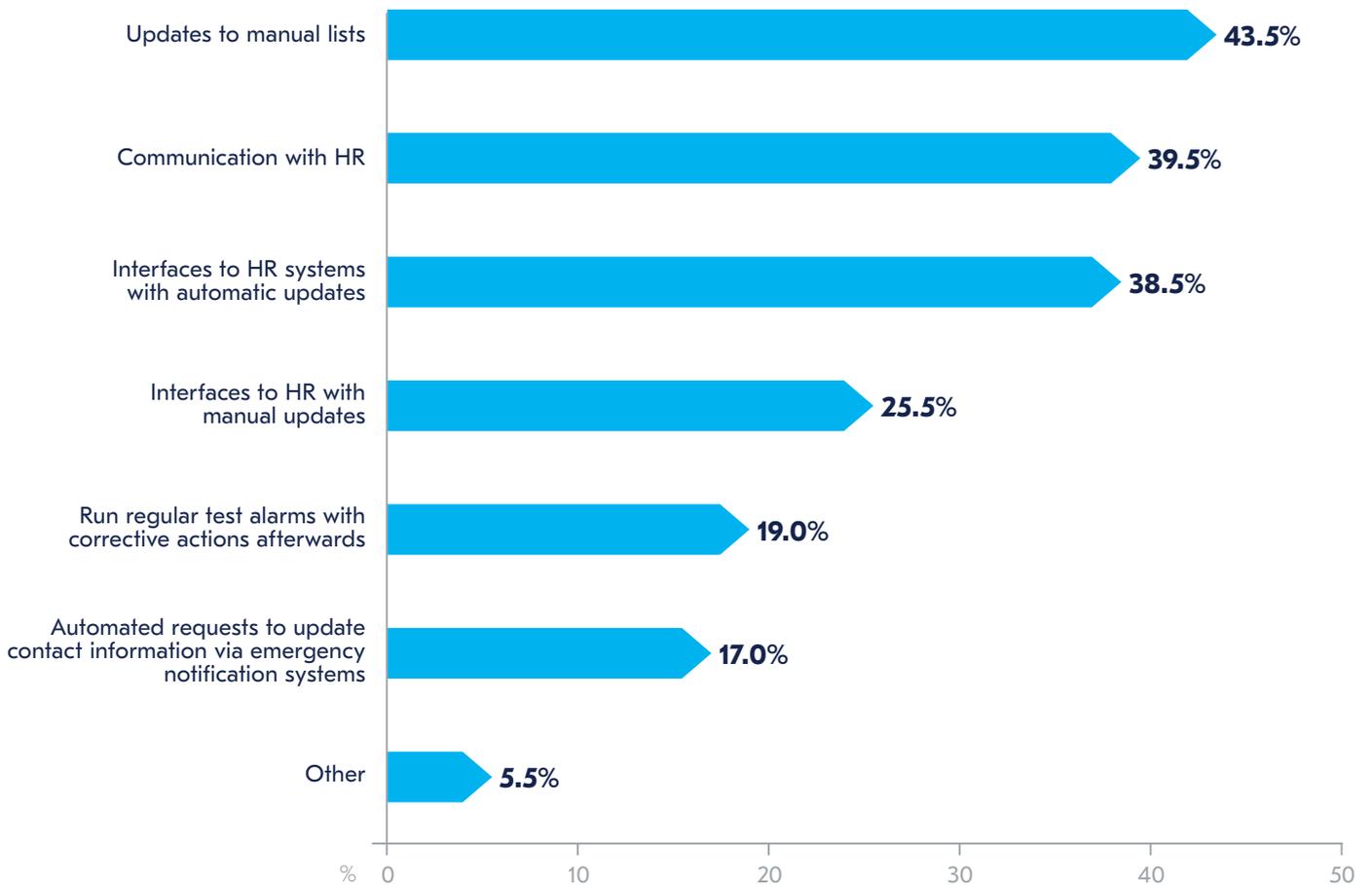


Figure 27. How do you ensure contact data of employees, experts, etc. is up to date?

Section three:
Key challenges
during a crisis





Section three: Key challenges during a crisis

- **The primary challenge during crisis communications is collecting, validating and sharing accurate information and communicating with staff.**
- **“Communicating with staff” and “getting staff to follow planned procedures” are both particular challenges for organizations which point to insufficient training and exercising taking place.**

When respondents were asked what their main challenges were when communicating in a crisis, the same pattern emerges that has been noted in previous parts of the report – that of failure in manual processes. The primary challenge elected by most respondents was that of “communicating with staff” which, as highlighted in the analysis in the previous section, is normally as a result of information being ignored or sent to out-of-date contact information.

However, when considered the first, second and third challenges for organizations, “communicating with staff” falls into fourth position and “gathering, validating and sharing accurate information” comes to the top of the table. This issue has been dominating the concerns of organizations for some time now, becoming a bigger challenge year-on-year as sources of information multiply in parallel with fake news and misinformation spiralling beyond control, making the validation factor a crucial and more complex component when sharing information. Without precise information the crisis management process will almost certainly fail. Because of this, senior management are increasing their demands for validation of information and the amount of information they wish to receive about an incident.

“In terms of effective communication with remote teams, being a very big team we are not all working centrally, some are working remotely and therefore just to be able to cascade everything that is happening within the organization is a key issue for us. Also, In terms of location-based services, it is critical for us because when an incident is affecting one geographical area, you’ll want to really ensure that you have targeted notifications for people around that particular area and people who are planning to travel to that particular location.”

Group Head of Business Continuity Management,
Financial & Insurance Services, Kenya

However, an interviewee explained how issues with communicating with staff can also be a consequence from gaps in the implementation of a plan or from a poor communications plan itself.

“The organization doesn’t have one established way of delivering emergency communication. There are a number of stakeholders involved with that. If you talk to our communications team, they’re saying, ‘Well, we’ve got this app. We use that to tell everybody there’s, whatever going on in three days’ time.’ Nobody’s taken that strategic view of how you deliver emergency communications to actually get people to react to what you are communicating with them and to deliver a message that they are going to take notice of. If I’m in the middle of doing an operation, I’m not necessarily going to be reading my emails or checking my messages. However, I might want somebody in that operating theatre, or just outside of that operating theatre, to say, ‘We’ve now got an active shooter in the building’ . You have to have a specific delivery method that everybody is both aware of and act on when they receive the message. It’s about effectively communicating important messages to the optimal amount of people, in the shortest timeframe really.”

Resilience Director, Healthcare, US

Another challenge highlighted by a high number of respondents is “getting staff to follow planned procedures.” This challenge was voted by 40.7% of participants with 17.1% indicating that this was their first challenge. Again, this issue can be addressed by reviewing training and exercising procedures, and ensuring such training is carried out at least every 12 months and after an incident has taken place if the expected response time was not reached.

“Keeping an overview of the situation” received 38.6% of votes, with 15.0% of respondents saying it this was their first challenge of emergency communications management. This too is related to the issue of “gathering, validating and sharing accurate information.” Within a crisis situation, the conditions are ever-evolving and the issue of collecting accurate factual information becomes difficult.

Communicating with customers and other stakeholders was chosen as the first challenge by 7.3% of respondents. Such communications typically involve the PR and/or external communications team within the process as well, meaning that accurate information is absolutely crucial. One interviewee explained this challenge within his organization.

“Since we have systems that are managed by public authorities, we need to keep them informed. There is a very complex process in place to keep them informed, and it is not quite straightforward because we don’t just say to them on a messenger a couple of words. We need to give them, in a very structured and consistent way, clear information about why this is down, why this doesn’t work and so on. So that’s the reason why it’s a challenge for us to communicate with external stakeholders”

Business Continuity, IT &
Telecommunications, France

What are your key challenges during emergency notification/crisis management?

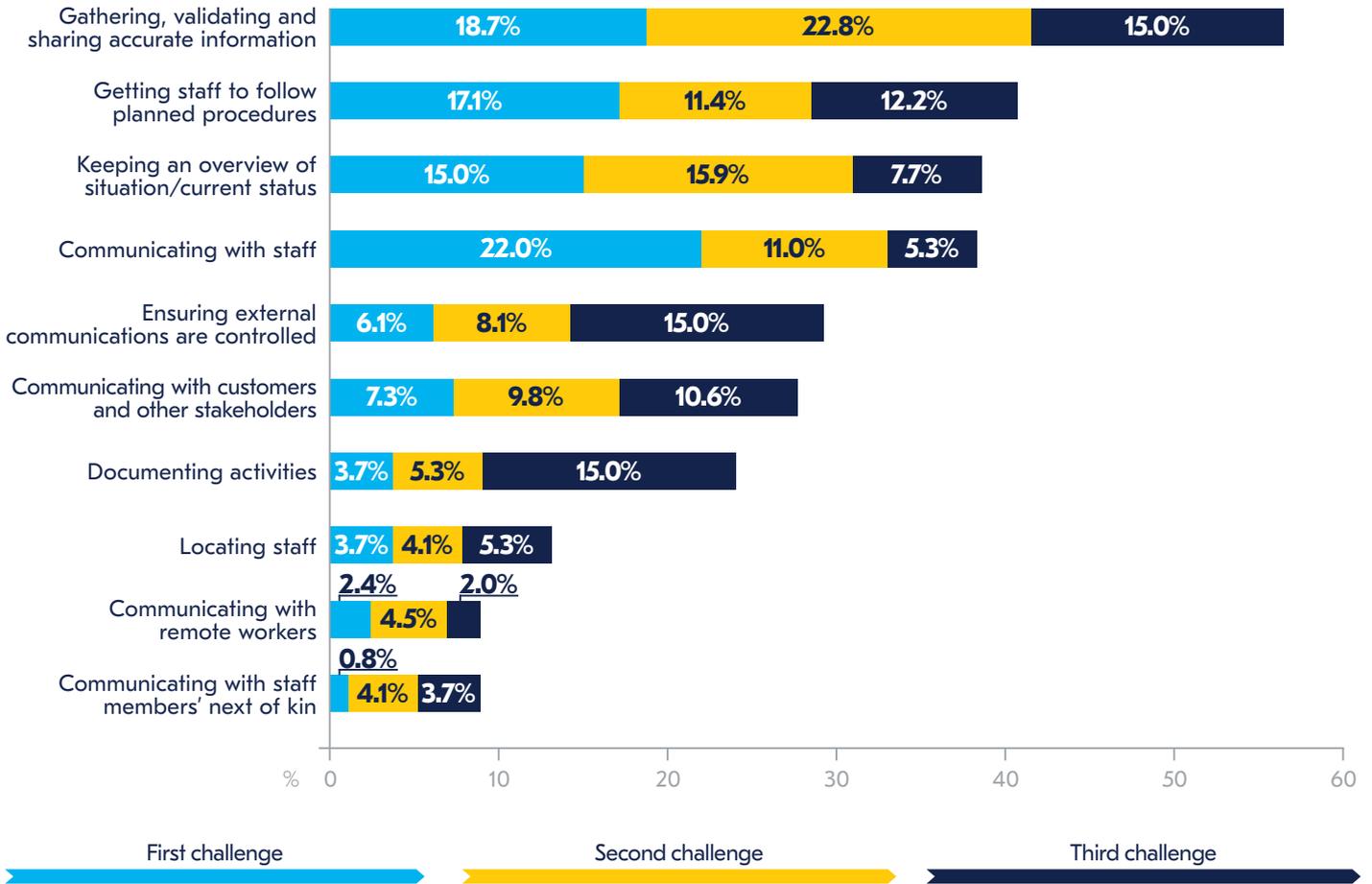


Figure 28. What are your key challenges during emergency notification/crisis management?

A variety of accurate data resources is essential to the effective execution of any emergency communications plan. The importance of obtaining accurate information in a timely manner is also crucial, as plans based on the wrong information could lead not only to the failure of such a program but also, in worst case scenarios, human lives could be endangered. Additionally, reputational damage, loss of revenue and lack of trust from the organization’s personnel could impair the proper functioning of the organization. Obtaining accurate data vs timely data means some degree of trade-off may be inevitable. For example, only using social media as a source for managing an emergency communications plan would be unwise, although using it as an initial source to pick up unfolding information in a crisis can be invaluable. In this case, corroboration with a reliable source or people on the ground would be invaluable.

How do you ensure the acquisition of timely and reliable information when it comes to an incident or crisis situation?

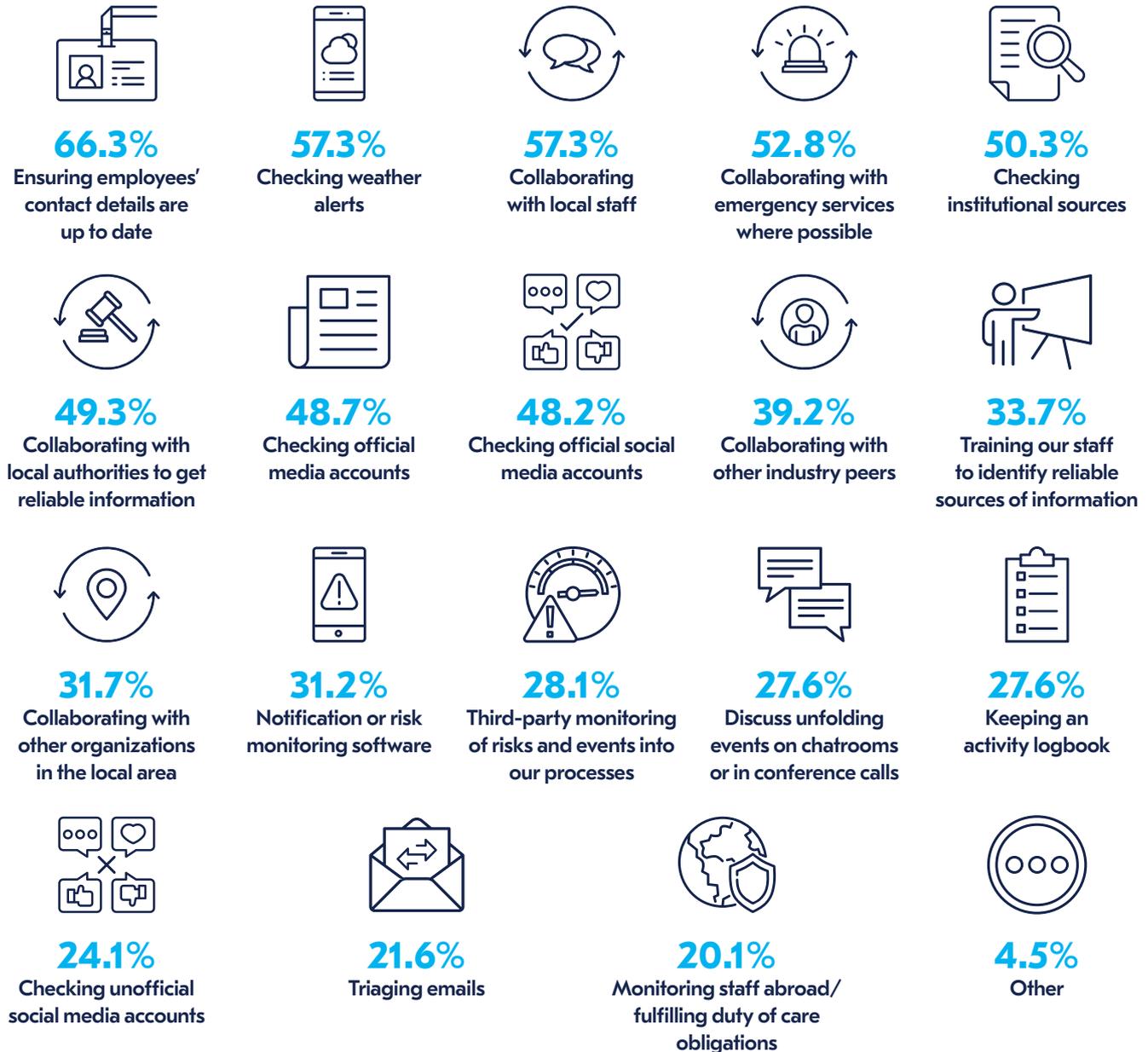


Figure 29. How do you ensure the acquisition of timely and reliable information when it comes to an incident or crisis situation?

Understanding the data sources respondents use in a crisis can provide some insight as to why some of the challenges of communicating in a crisis come to the fore. Indeed, the first question is the best exemplar of these: ensuring employees' contact details are up-to-date is the most popular option for respondents, with two thirds (66.3%) saying they do this. However, even though it is the top option on the graph, it is concerning that a third of respondents did *not* select this, and it goes some way to explaining why communication with staff is the most highly rated first challenge when communicating in a crisis.

Checking weather alerts (57.3%) is in second position. Most organizations will be carrying out this monitoring using free data sources, although those in areas exposed to extreme weather are more likely to use mapping tools to establish if any of their – or their key suppliers' – operational sites are likely to be affected by bad weather conditions. Investing in corporate weather forecasting tools is a trend which is on the increase: a recent report by Market Growth Reports puts the current value of the global corporate weather forecasting market at US\$618.9m and expects it to more than double by 2027 to US\$1,208.7 million – a CAGR of 11.8% between 2022 and 2027¹⁵.

Other factors point to good practice in organizational and community resilience to ensure information can be gathered correctly: collaborating with local staff (57.3%), collaborating with emergency services when possible (52.8%), collaborating with local authorities (49.3%), collaborating with industry peers (39.2%) and collaborating with other local organizations (31.7%) were all popular methods for information gathering. Meanwhile, checking institutional sources (50.3%) and checking official social media accounts (48.2%) were also popular forms of information gathering. Interestingly, around a quarter of organizations are using unofficial social media (24.1%) and/or informal collaboration methods such as chatrooms (27.6%) as part of the information gathering process. As mentioned above, using methods such as this do require corroboration (where possible) but can provide up-to-the-second updates to unfolding situations.

Respondents were also asked if they had any automated alert systems in place and nearly three out of five organizations do use technology in this way. In terms of the automated alerts that they were using, answers centred around a number of key themes: social media, emergency services, weather, IT/cyber and geopolitical events.

Some respondents explained how their organizations were managing this automation via a centralised source which was typically the centralised crisis management team and/or IT. One respondent said that *"IT has their automated monitoring of sites, software, cyber threats"* whilst another explained how *"threat alerts [were] managed through our crisis management and communications SaaS. Internal Teams monitor social media. IT does systems monitoring."* Meanwhile, an interviewee described an elaborate – and effective – system they had in place for information gathering.

"We gather information through groups where they are part of particular forums that have been constituted just to be able to ensure information is flowing through. In Kenya, we get this through what we call KBA. KBA actually brings all these security partners together just to be able to look at the threat landscape and actually cascade information, anything that impacts organizations. That's how we are able to get the information just to be able to action on it. We then have a control room where this information filters before it's actually channelled through. We have a 24/7 team that actually does this for us."

Group Head of Business Continuity Management,
Financial & Insurance Services, Kenya



15 The Expresswire (2023). Weather Forecasting for Business Market Size 2023-2027 Key Geographical Regions Analysis by Top Key Players with New Report. Market Growth Reports (online) 15 January 2023. Available at: <https://www.marketwatch.com/press-release/weather-forecasting-for-business-market-size-2023-2027-key-geographical-regions-analysis-by-top-key-players-with-new-report-2023-01-15> (last accessed 7 February 2023)

Some organizations however, continue to use a wide range of sources to ensure they get the right amount of information. One respondent explained how *"communications has social media monitoring, third party social media monitoring for specific threats, weather and news alerts, based on locations and an app for earthquakes"* whilst another explained how they use a range of applications and devices to manage their situation: *"We use social media monitoring, weather alerts, travel risk management vendor/tool; supply chain risk management tools"; "We use app-based notification services offered by Australian Bureau of Meteorology and state-based emergency services such as 'NSW Rural Fire Services' and Fires Near Me app."*

However, 42.3% of organizations do not have any automated alert systems in place. Considering the fast and ever evolving business environment, even more so in crisis management situations, the lack in the use of technology to manage alerts represents a vulnerability from a business continuity/resilience perspective. In this regard, some respondents explained how they operated, typically ineffectively, without these practices in place. One participant said their systems are *"not automated and rely on human 'intervention'."* Another explained that they *"do not have automated systems for social media monitoring, weather alerts, news feeds, but we do it manually"* and a last participant stated that *"WhatsApp is our fastest communication tool."*

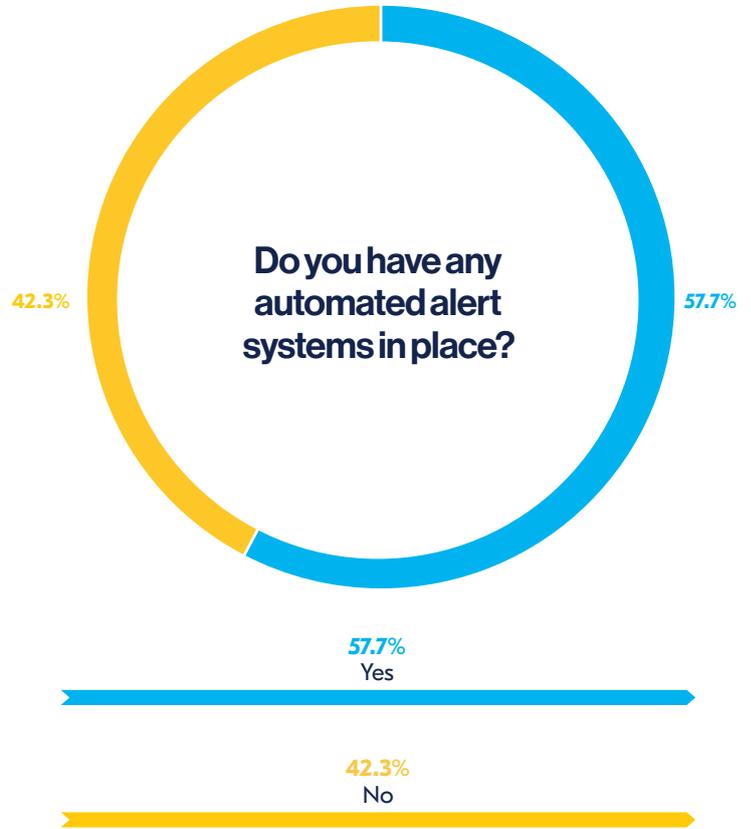


Figure 30. Do you have any automated alert systems in place



Section four: **Building resilience**



Section four: Building resilience

- **There has been an increase in frequency of organizations carrying out emergency communications training this year, with more than a third of organizations (36.3%) carrying out training twice a year or more (2022: 24.0%).**
- **Annual exercising of plans has long been the standard for organizations, but the frequency is now rising: 41.2% of organizations are exercising plans twice a year or more (2022: 36.8%).**

Resilience and business continuity professionals are well aware of the importance of training and exercising as a way of embedding business continuity practices within the organization and validating plans and procedures to ensure their organization is resilient in the event of a crisis.¹⁶

The importance of training personnel and exercising the different elements of crisis management plans is a well-established notion within the industry. The ability to communicate in an emergency or crisis is the backbone to any crisis management plan and this section seeks to determine the extent to which organizations both train their employees to understand the emergency communications plan as well as exercising of these plans.

2020 and 2021 saw an abrupt transition to remote working and many organizations struggled to carry out training as often as they did before the pandemic. Organizations reported that they were having to activate their plans so frequently as a result of the pandemic there was little time left for training. Furthermore, with many organizations moving either temporarily or permanently to remote/hybrid working, most emergency plans needed to be revisited and training processes revised in the face of new working environments. Lessons have now been learned following the pandemic and incorporated into crisis communications plans.

¹⁶ The Business Continuity Institute- BCI- (2018) Good practice guidelines 2018 edition (online) Available at: <https://www.thebci.org/product/good-practice-guidelines-2018-edition---download.html> (Accessed: February 2, 2023).

Annual training continues to be the most accepted practice within institutions, with a third of organizations (32.1%) still following this practice. However, this year there has been a notable increase in the frequency of training: 36.3% of respondents say their organization now carries out training at least every six months, with 11.3% saying training is carried out every three months or more frequently. Moreover, *ad hoc* training has seen an increase from 12.3% last year to over 21.2% this year. Carrying out training after a real-life activation has happened can help to highlight any errors during the activation and advise on what to do during the next activation.

An interviewee from an international organization explained how training on their crisis management system was not only a regular occurrence within the organization, but was an integral part of the organization's induction training.

“Each person that joins the organization has a mandatory three level online security training, including a crisis management online simulation. They also have cyber security training online, anti-fraud and anti-corruption training. Before they arrive at their duty station, they need to prove that they have done this certificated, eLearning training.”

Crisis Management, advisor International Organization, Switzerland

However, whilst the figures paint a positive picture, some respondents spoke about how their training activities need revision. An interviewee from Kenya detailed how most training was done in his organization to comply with audit process and lacked the comprehensiveness required for successful training to take place. Indeed, whilst some organizations may be fulfilling their criteria in terms of number of training sessions, the quality and content of those sessions is crucial to their success.

“I think that in terms of the training, we need to enhance that further and really be able to have more of what we call targeted training and make it more frequent, just to be able to build awareness. Most of the engagement has been done just to comply with an audit process from a training perspective, but we want to embed this as a process where on a quarterly basis we are able to ensure that people are aware in terms of training. That's why with that lack of training you find, even in terms of implementing the plan themselves, they fall short.”

Group Head of Business Continuity Management, Financial & Insurance Services, Kenya

The final positive sign is that the number of organizations that admit to not carrying out any training activity has fallen to 3.3% this year; down from 4.2% in 2022.

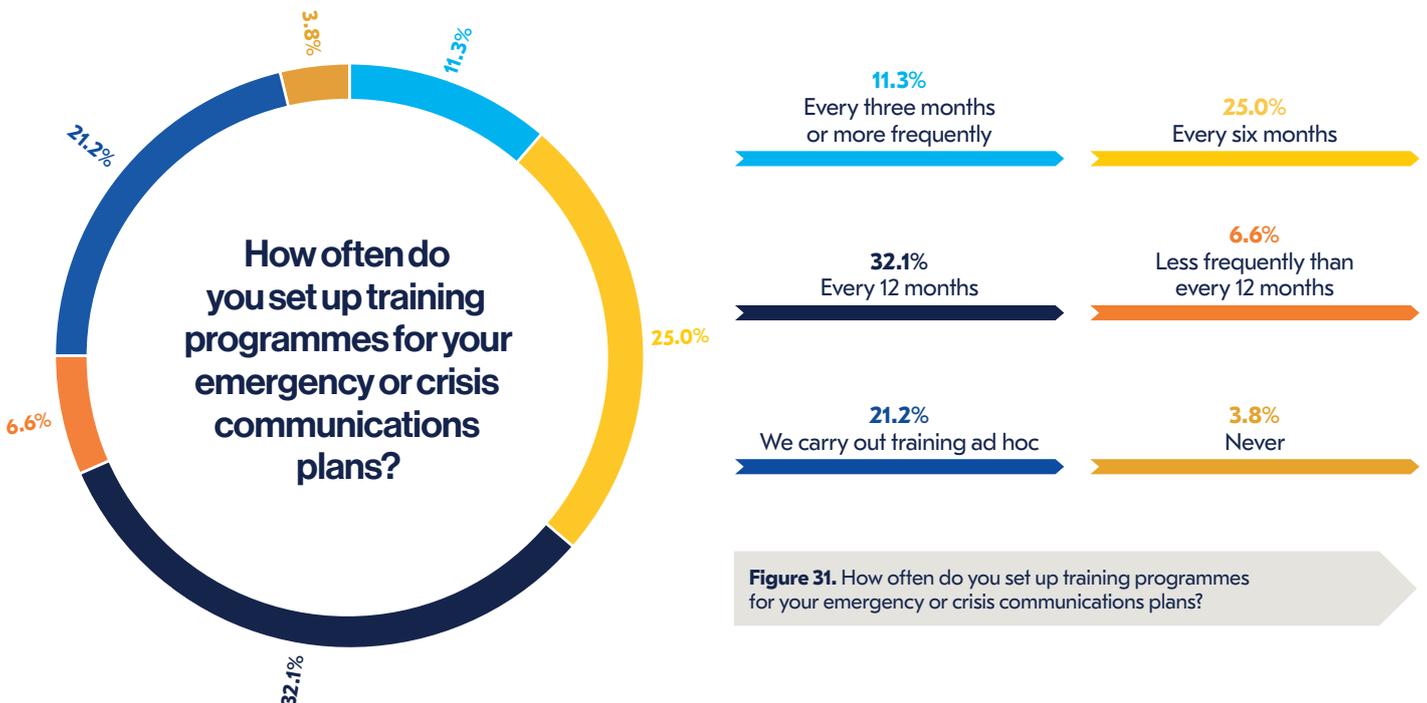


Figure 31. How often do you set up training programmes for your emergency or crisis communications plans?

Practice makes perfect!

Validation is the Professional Practice within the business continuity management lifecycle that confirms the business continuity programme meets the objectives set in the organization's policy, and that the plans and procedures in place are effective¹⁷. There should be a process in place to continually improve the overall level of resilience and exercising is an inherent part of this process: through exercises organizations can train for, test, assess and improve the resiliency of an institution. As one participant put it, *"Prevention is better than cure. Exercising is key to developing the muscle memory in an organization. It is the hidden missing link in many organizations' preparedness and resilience."*

When analysing the frequency of exercising within organizations, annual exercising remains the most popular time period, with 40.7% reporting exercising is carried out every twelve months.

However, there is a noticeable positive shift this year when examining the number of exercises organizations perform annually: 41.2% of respondents claim their organization carries out exercising at least twice a year, with 20.1% doing so every quarter or more.

An interviewee from Australia explained how the importance of using their emergency communications tool when training and exercising took place, whilst another said that short simulations were a crucial part of their exercising process for their busy senior management team who were unable to devote a significant amount of time to the exercising process. Another expressed the importance of getting the messaging right when introducing training and exercising to senior management who, in his organization, had concerns about performing badly in the exercising process.

"When we have a 'practice fire drill, evacuation or exercise', we also use our emergency response notification system for that purpose. Testing the system for routine events help our people become familiar with it, and comfortable knowing how it work. We also use it to also train a range of our people in crisis management."

Global Senior Manager Business Continuity,
Professional Services, Australia

"We have also done a couple of simulations, especially for the senior management team because our senior management team is very busy and has no time to be updated in new technologies. We managed to have senior management team involved in two simulations, which is a big step ahead for us."

Crisis Management Advisor,
International Organization, Switzerland

"I find hard to engage top management with exercising. They tend to shy away a lot because they believe that if they make mistakes in exercises it shows them up. And they're not about looking bad apparently. But we know the exercise that they're there to learn. I tell them: Let's make the mistakes in a scenario where we are comfortable right now so we can learn from it." So when the real thing occurs, you can then be very calm, confident, concise as to what you're going to do and how you're going to do it."

Health and Safety Manager, Infrastructure,
Trinidad and Tobago

¹⁷ The Business Continuity Institute- BCI- (2018) Good practice guidelines 2018 edition (online) Available at: <https://www.thebci.org/product/good-practice-guidelines-2018-edition---download.html> (Accessed: February 2, 2023).

One interviewee described how a desktop training exercise in their organization had unearthed a real issue with their systems and processes. This shows how valuable training can be in not only ensuring staff know what to do in a crisis, but can also help to unearth errors which could hamper the success of a future activation.

“In my time at the hospital, we actually had one of those should never happen things, but it did happen. And we did a full desktop planning scenario for the hospital to understand impact over various kind of ecosystems in the hospital. So when you have a sign saying, “Do not trim cables in the data centre,” that is an instruction, not an optional thing. Someone did trim a cable in the data centre and a little tiny piece of insulating foil the size of a postage stamp got drawn into a cooling fan of one of the uninterruptible power supplies, shorted it out, so the full load went onto number two, which could carry it for two hours. Then that overheated and paid off to battery pack number one, which exhausted after an hour, paid off to battery pack number two, which had failed three months ago, and everything went.”

Line of Business, Health & Social Care,
New Zealand

The trends noted in this year’s report are promising. Organizations are now carrying out training and exercising programmes with more frequency and vigour, and considering new ways of introducing training into their organizations to fit the requirements of the people in the organization (e.g. introducing short simulation-based training for senior management).

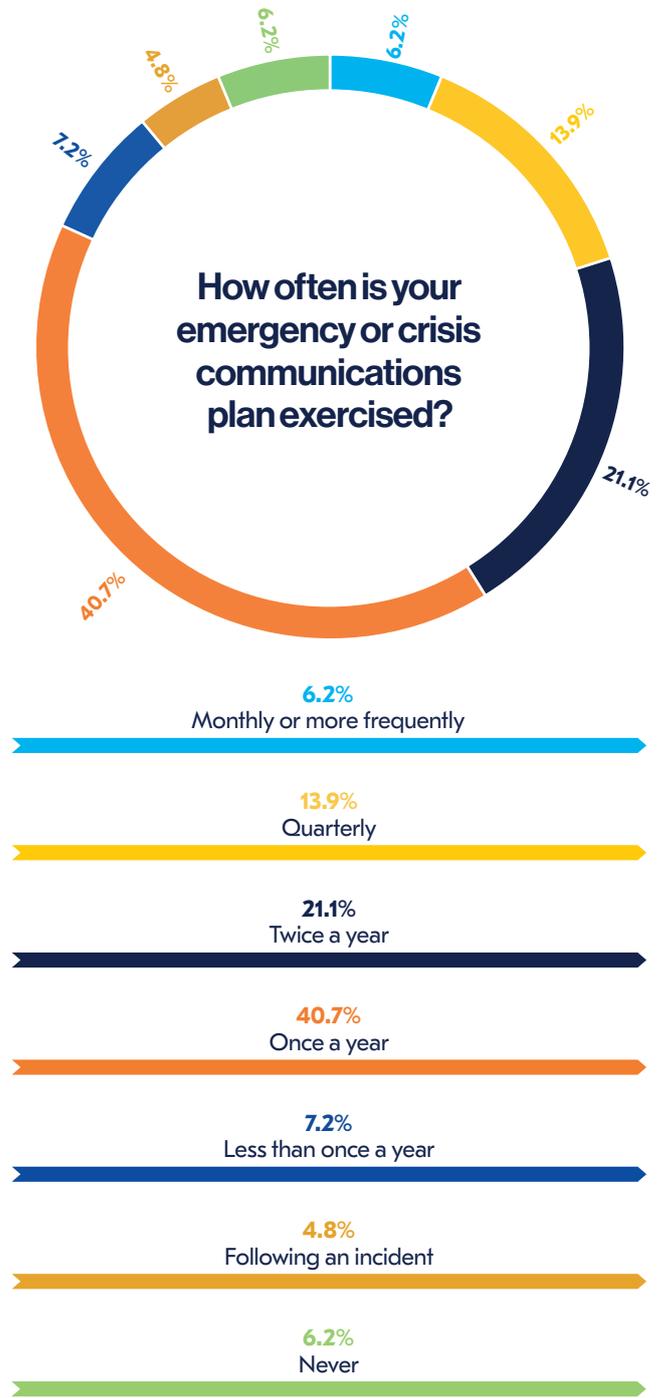


Figure 32. How often is your emergency or crisis communications plan exercised?

Section five: Looking ahead





Section five: Looking ahead

- **The implementation of Internet of Things devices within emergency communications plans is becoming more popular: 39.1% of organizations now use IoT devices or are planning to (2022: 38.4%).**
- **More than half of organizations (51.8%) still do not plan to use IoT devices with many still concerned about privacy and/or security of these devices (2022: 57.0%).**

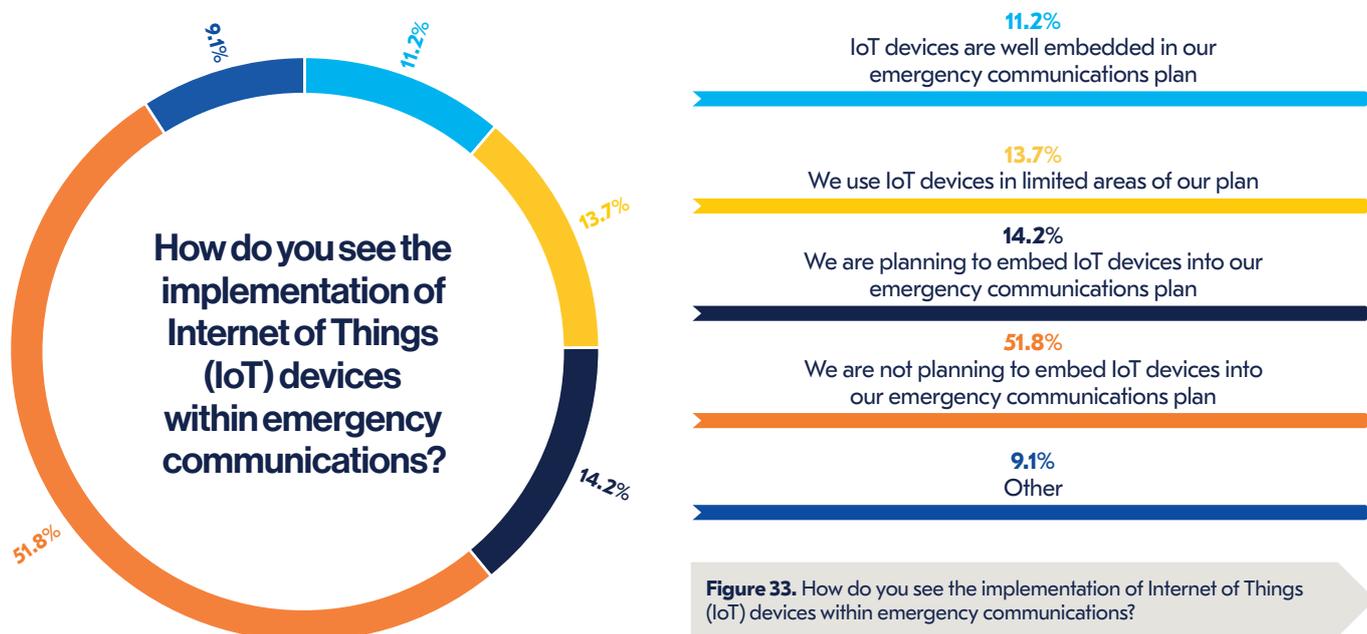
IoT is now incumbent in everyday life – but not in emergency communications

The concept of connecting any device to the Internet and to other connected devices configuring a giant network of connected things and people has the power to innovate emergency communications plans and processes. Devices are interconnected to other devices which can detect, analyse and share information to help automate and speed up parts of the communications process.

These platforms can identify exactly what information is useful and what can safely be ignored. This can be used to detect patterns, make recommendations and detect possible problems before they occur.

The use of IoT in business continuity and crisis management settings is still in the early stages. The survey data shows that whilst IoT use in emergency and crisis communications is slowly gaining supporters, most organizations are not ready to adopt this kind of technology just yet: 51.8% of respondents said they were not planning to incorporate IoT into their crisis management plans. However, 39.1% *do* now use IoT devices or are planning to, which is a higher proportion noted than in any previous year.

However, an encouraging trend that can be noted this year is the five-percentage point increase in the number of organizations that have IoT devices well embedded in their emergency communications plans: this year, 11.7% of organizations are making full use of IoT tools within their emergency and crisis communication plans. This figure is the highest ever recorded since the inclusion of this topic within our reports. Furthermore, 13.7% of respondents report using IoT devices in limited areas of their emergency communications plan (2022: 12.8%).



IoT devices well embedded in organization’s emergency communications plans 2020- 2023

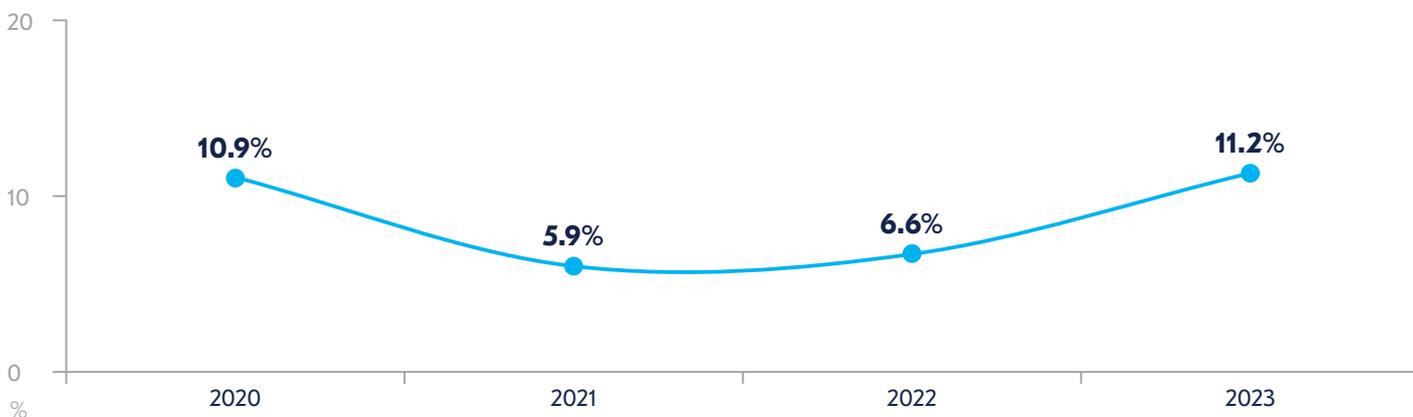


Figure 34. Percentage of organizations that report having IoT devices well embedded into their emergency communications plans

There is a notable 9.1% of respondents who ticked the ‘other’ choice. The comments here relate to a lack of knowledge around this area of technology and the potential uses within crisis communications, concern that the technology is insufficiently advanced and that its reliability may be questionable in a crisis.

Whilst it is likely that IoT will be adopted as standard in emergency and crisis communication plans in future as products are more widely tried and tested in commercial environments and offer a proven benefit over existing methods. In this sense, one respondent commented that they “have yet to see a decent IoT deployment in local government that improves on current more sophisticated monitoring systems e.g. fire alarms. BUT it will come.” Another participant explained his doubts, however: “Anything relying on the Internet would not survive power outages. This winter looks like it will see planned power outages but whilst we have generators it is unlikely Internet and mobile signals will be maintained.”

Other comments focused on the ill-acceptance of such devices in the workplace environment. One respondent stated that “there is little buy in on introducing anything related to this” and another admitted that “this approach has not been discussed internally by all stakeholders.”

Annex





Survey dates



Respondents



Countries



Sectors



Respondent interviews



Figure 35. Which of the following best describes your primary function in your role?

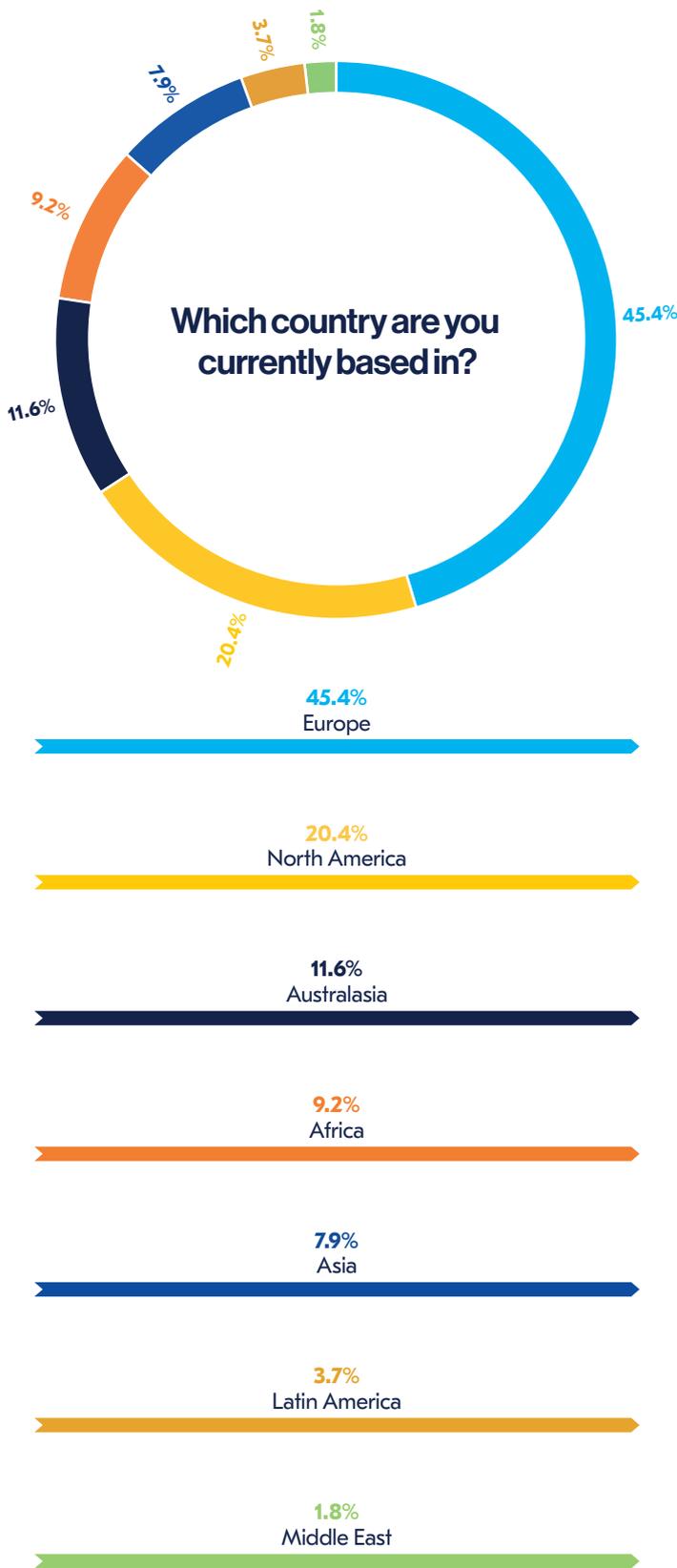


Figure 36. Which country are you currently based in?

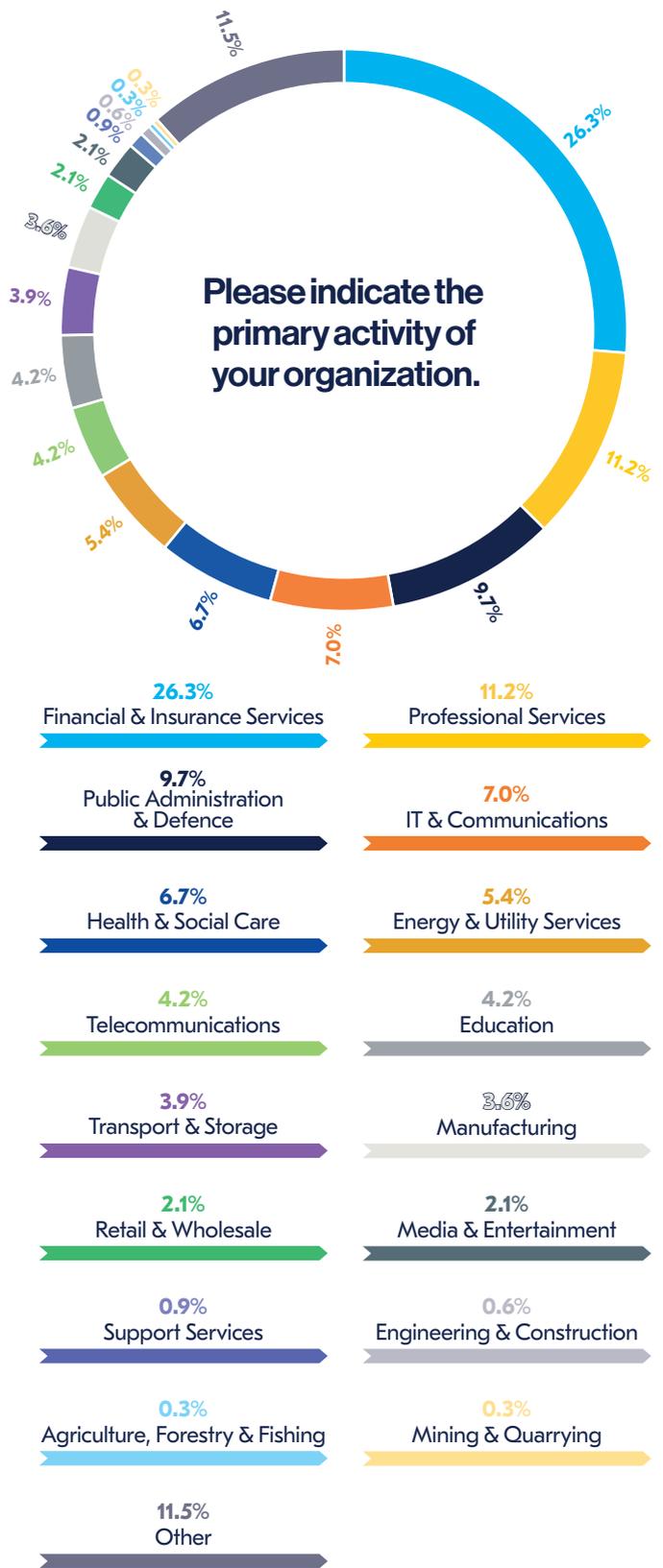


Figure 37. Please indicate the primary activity of your organization.

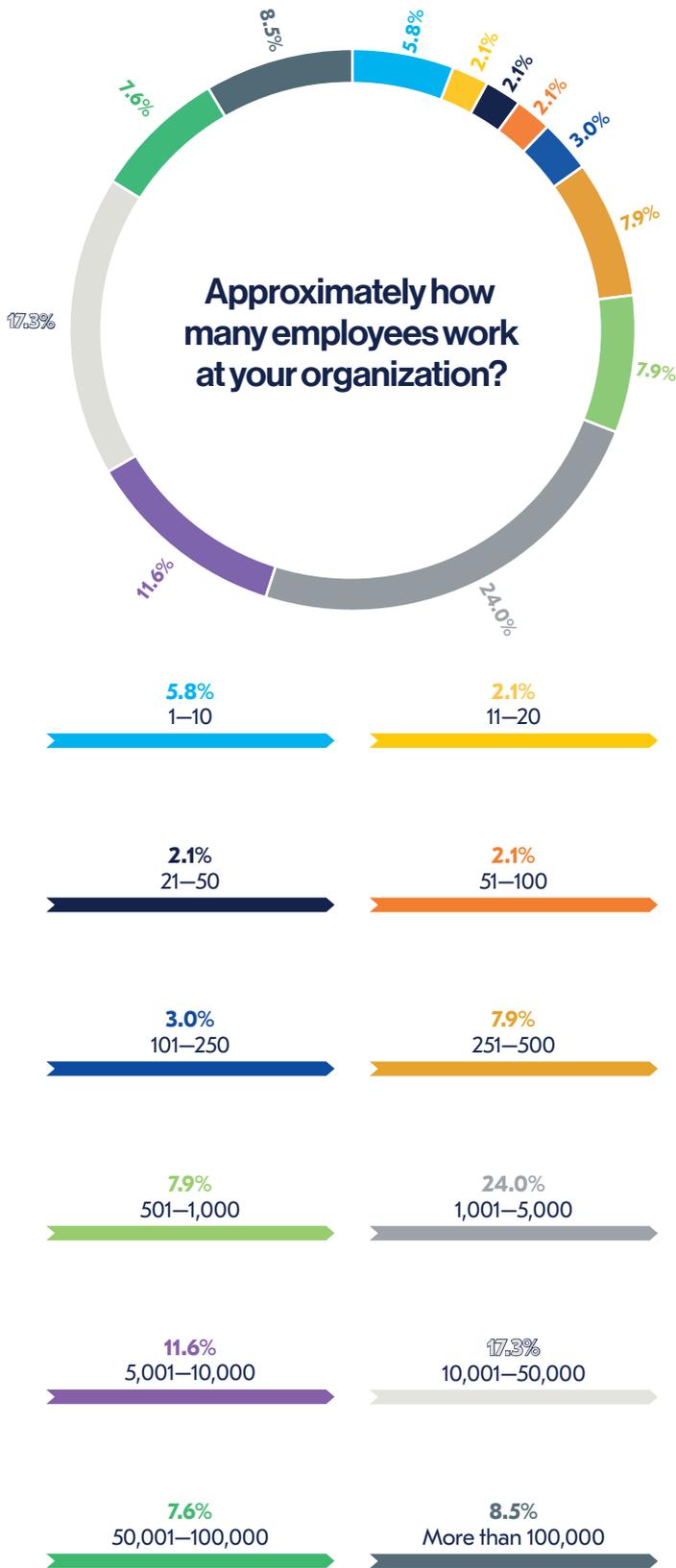


Figure 38. Approximately how many employees work at your organization?

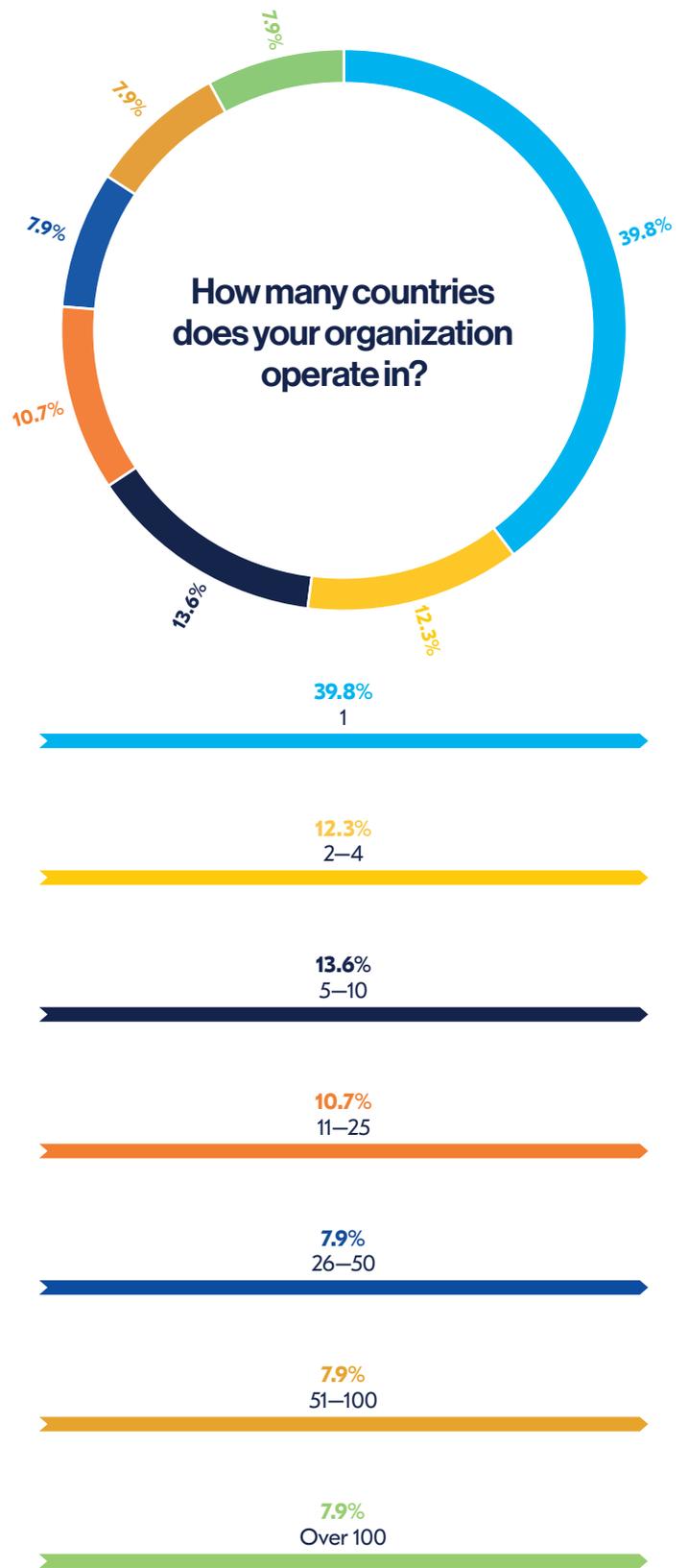


Figure 39. How many countries does your organization operate in?

About the Authors



Rachael Elliott

(Head of Thought Leadership)

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

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



Maria Florencia Lombardero Garcia

(Research Manager)

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

She can be contacted at maria.garcia@thebci.org



About the BCI

Founded in 1994 with the aim of promoting a more resilient world, the Business Continuity Institute (BCI) has established itself as the world's leading institute for business continuity and resilience. The BCI has become the membership and certifying organization of choice for Business Continuity and Resilience professionals globally with over 9,000 members in more than 100 countries, working in an estimated 3,000 organizations in the private, public and third sectors. The vast experience of the Institute's broad membership and partner network is built into its world class education, continuing professional development and networking activities. Every year, more than 1,500 people choose BCI training, with options ranging from short awareness raising tools to a full academic qualification, available online and in a classroom. The Institute stands for excellence in the resilience profession and its globally recognised Certified grades provide assurance of technical and professional competency. The BCI offers a wide range of resources for professionals seeking to raise their organization's level of resilience, and its extensive thought leadership and research programme helps drive the industry forward. With approximately 120 Partners worldwide, the BCI Partnership offers organizations the opportunity to work with the BCI in promoting best practice in business continuity and resilience.

The BCI welcomes everyone with an interest in building resilient organizations from newcomers, experienced professionals and organizations. Further information about the BCI is available at www.thebci.org.

Contact the BCI

+44 118 947 8215 | bci@thebci.org

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



About F24

F24 is the leading Software-as-a-Service (SaaS) provider for business messaging, emergency notification as well as incident and crisis management in Europe. The highly innovative F24 solutions support customers through the whole value chain from high-volume communication in the corporate environment through governance, risk and compliance (GRC) up to Emergency Notification and Smart Event Communication as well as Comprehensive Crisis Management. More than 3,000 customers worldwide rely on F24's solutions to manage their communication needs, as part of their day-to-day communication of critical or confidential content, or in the event of a crisis.

Contact F24

+49 89 2323638 81 | www.f24.com | patrick.eller@f24.com

Ridlerstraße 57, 80339 Munich, Germany

BCI 9 Greyfriars Road, Reading, Berkshire, RG11NU, UK.

bci@thebci.org / www.thebci.org