Find out more
www.thebci.org

Thought Leadership

Emergency and Crisis Communications Report 2022

F24

Leading the way to resilience

Contents

5 Executive summary

13 Section one:
The tools of the trade

29 Section two:
Response and timing

39 Section three:
Key challenges

43 Section four:
Requirements in support tools

50 Section five:
Training and exercising

57 Section six:
The Internet of Things (IoT)

60 Section seven:
Information and data acquisition

65 Section eight:
Communicating with stakeholders

71 Annex

Foreword

The last two years have been a period of change for many organizations. The pandemic, coupled with record breaking severe weather around the world, have seen supply chain models rewritten, the traditional office continues to evolve with hybrid or remote working and staff, who previously used meeting rooms for discussion, have moved towards virtual communication habits. Technology has been often cited as the primary enabler during the pandemic, and emergency and crisis communications have been at the heart of this.

In 2020, many organizations struggled to deal with the pandemic and their communications around it. This drove an increase in the purchasing and use of specialist emergency and crisis management systems at the same time as workers around the world also became familiar with tools such as Microsoft Teams and Zoom for communication. Indeed, the fear driven by a new pandemic saw management looking to understand every nuance of the illness and how their own organization was being impacted. Emergency communications plans were activated on a scale never before seen in this report with five minutes — rather than 60 minutes — becoming the gold standard for activation.

2021 brought a more settled picture. Adoption of emergency communications solutions has continued to increase, but purchasers are being more discerning about the products they introduce into their organizations. While the primary purpose of emergency and crisis communications has remained the same — the ability to contact a large number of people quickly — users are now requiring far more of their tools. The means to collaborate, risk management features, information corroboration and reporting are just some of the desirable features of post-pandemic communications systems.

However, with all the focus on technology, it is important to remember the importance of people during an incident. The technology within an organization might be perfect, but training and exercising — which many organizations temporarily paused during the pandemic — now needs to be reintroduced and rejuvenated to apply the changes made during the past two years. Management is also keen to trade in fast activation speeds for more accurate information gathering and corroborating in the early part of the crisis.

We hope this year's report will provide useful reading for anyone in resilience-orientated professions and can also serve to benchmark your organization's existing technologies, processes and procedures — particularly at a time when methods of communications are changing fast. The interviews conducted for this report also help to provide learnings from practitioners with real world experiences.

I would like to express my sincere thanks to F24, our continued partner in producing this valuable report for the industry. I also wish to share my gratitude to the hundreds who took part in the survey and interviews, sharing their real-world experiences with the BCI.

Christopher Horne FBCI
Chair of the BCI

F24

Foreword

Today, we stand on the verge of a new era in managing critical situations. The evolution of the business world in the past years, with the unusual long state of crisis because of the pandemic, enables us even more to evaluate lessons learned and draw conclusions for the future. The business environment has changed, as have the ways we perceive and handle crises. And if one thing has become clear, it is that these different situations require their own solution approaches.

Therefore, a separation between the day-to-day communication and communication in emergencies and crises is crucial to the response time and success of crisis handling. Although business communication tools are valuable for our daily business, using them as main tools in crisis situations can cause more trouble than good. Not to mention the reliance and dependency on one communication tool for almost all aspects of your communications activities. It is precisely the latter aspect, which causes a major new threat to organisations in times where IT or telecommunication incidents have become the number one cause of crisis activations in 2021 (42%), together with disease outbreak.

Encouragingly, the transformation of our profession has started, and a lot of organisations have implemented steps to remodel the physical crisis room into a virtual environment. As this year's report shows, the number of organisations using a virtual crisis room/online collaboration tool dedicated for crisis management (63.5%) has almost caught up with organisation using a messenger tool for the business environment (64.3%). It underlines the increased awareness of the relevance and advantages a secure and reliable collaboration tool dedicated to emergency and crisis management has to offer. Additionally, organisations using a dedicated solution for emergency and crisis communication are happier (57.8%) with their solution while the dissatisfaction of organisations using an enterprise messenger or free messaging app increased (6.7% and 4.8%) in 2021.

We all know a pandemic is not the only scenario potentially having a major impact on our businesses — and in addition the requirements for communication are not as high as in many other scenarios. Crises can and will come in all shapes and sizes as severe weather events and other threats have shown in 2021. It's time to look at the big picture. It's time to focus on a vision for the future. It's time for organisations to prioritise and invest in building a foundation of resilience to address any type of crisis. No one can predict the future, but the right technology can support organisations in developing more clarity in crisis situations and set everything in motion when the time comes.

At F24, we have the knowledge and experience of providing reliable, state-of-the-art and easy to use solutions to support your organisation and we are very proud to continue our partnership once again with the BCI. We are delighted to sponsor the valuable insights and research of the BCI especially with this well-trusted and even further developed Emergency and Crisis Communications Report. We hope you'll gain new insights from the newest data as it supports organisations worldwide in adjusting their vision for crisis and incident management. Enjoy reading the Report!

Benjamin Jansen
Vice President Sales ENS/CM at F24

Emergency and Crisis Communications Report 2022

Executive summary

Executive summary

Laptops are no longer king for managing emergency communications activations: With the rise in remote working and hybrid working, there is an increasing requirement for emergency communications plans to be launched from mobile devices. The most popular way of activating an emergency communications plan is now via a mobile phone (95.7% of respondents), with laptops/PCs falling to second place for the first time (93.4%).

Mobility and multiple devices mean on premise installed software is now only used by one in ten organizations: With organizations desiring cross platform and cross device functionality, software-as-a-service (SaaS) solutions are now the incumbent solution for organizations. Just one in ten continue to use on premise installed software, with many of those indicating they will move across to SaaS in 2022.

Widespread use of enterprise communication software (such as Teams) has prompted investment in dedicated emergency and crisis communication tools: 64.3% of crisis teams use enterprise software (such as Teams) to communicate in a crisis but this year, almost the same number (63.5%) are using specialist tools and software to communicate. This convergence of the two most commonly used tools is symptomatic of the demand organizations now place on their emergency and crisis communication tools. Collaboration features, risk management features, information corroboration features are all now highly desired features for professionals, many of which can only be accessed with more specialist tools.

Management are now more sympathetic to the organizational need for a good emergency/crisis communications solution, but there are serious holes in organizations' strategies: COVID has proved to management the necessity of having a good emergency communications strategy, with a sharp increase in the number of small organizations employing specialist tools this year. However, some are writing emergency communications plans without considering an overreliance on one platform (such as Microsoft), not considering that all calls are routed through voice-over-IP (VoIP) which could be lost in a communications blackout and not ensuring employee contact information is kept up to date.

Human failure remains the most common cause for overall failure of an emergency communications plan activation: Over a third of organizations (37.4%) report a lack of understanding from staff is a reason for not achieving accepted response levels, with 35.1% citing a lack of accurate staff contact information. Training levels dipped slightly during COVID, primarily because there were so many real-life activations, whilst resilience managers continued their battle to work with HR and staff to ensure contact details were up to date. In countries where it is allowed, some organizations are now discontinuing staff contracts if they fail to provide contact information such is the importance placed on correct details being in place.

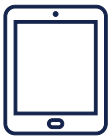
Mobile telephones become the preferred device to use in an emergency situation for the first time

95.7% of organizations use a mobile phone to manage emergency situations compared to 93.4% who use laptops. This is the first time mobile devices have headed the table, and show how solutions such as SaaS are enabling professionals to activate plans from a devices other than the traditional PC. Meanwhile, the demise of the desk phone is continuing.

Devices used to manage a crisis

95.7%
Mobile phones

93.4%
Computers/laptops



34.6%
Tablets

31.1%
Walkie-talkies/radios

30.6%
Desk phones

24.3%
Public address systems

21.4%
Satellite phones

Software as a service continues to be the standard for emergency and crisis communications software

The use of SaaS continues to dominate in the market, with just 15% of organizations now using on-premise installed software. The growth of SaaS cooled slightly in 2021 after fast growth in 2020 in the first stages of the pandemic.

Type of emergency/crisis management software used

74.2%
Software-as-a-Service solution

15.3%
On-premise installed software

The ability to get staff to move fast is the primary criterion for nearly three-quarters of organizations, but managers are now requested more advanced features from their tools

More than half of organizations want a tool that allows teams to collaborate in an incident, whilst others are now seeking additional risk functionality.

Ways in which organizations' emergency communications tools support them (top 8 responses)

71.5%
Alerting and mobilising a high number of people very fast

54.1%
Crisis handling

53.1%
Enable communication in teams

44.9%
Emergency Planning

37.7%
Employee safety

30.4%
Risk management

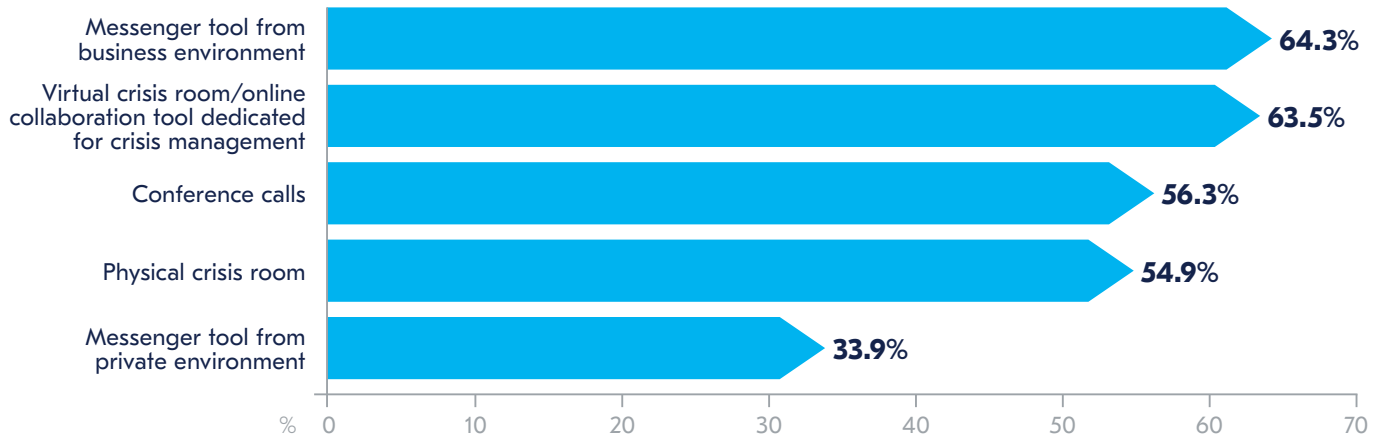
28.5%
Risk monitoring

25.6%
Documentation of all processes during an event

Dedicated online collaboration tools are about to surpass teams as the chosen method to organize collaboration within crisis teams

With a strong uptake of dedicated tools in 2020-2021, 63.5% of organizations are now using dedicated crisis management tools and/or software to collaborate within their crisis teams — less than one percent lower than those who use enterprise messenger solutions (such as Microsoft Teams). This suggests a desire for additional functionality — and security — within crisis teams.

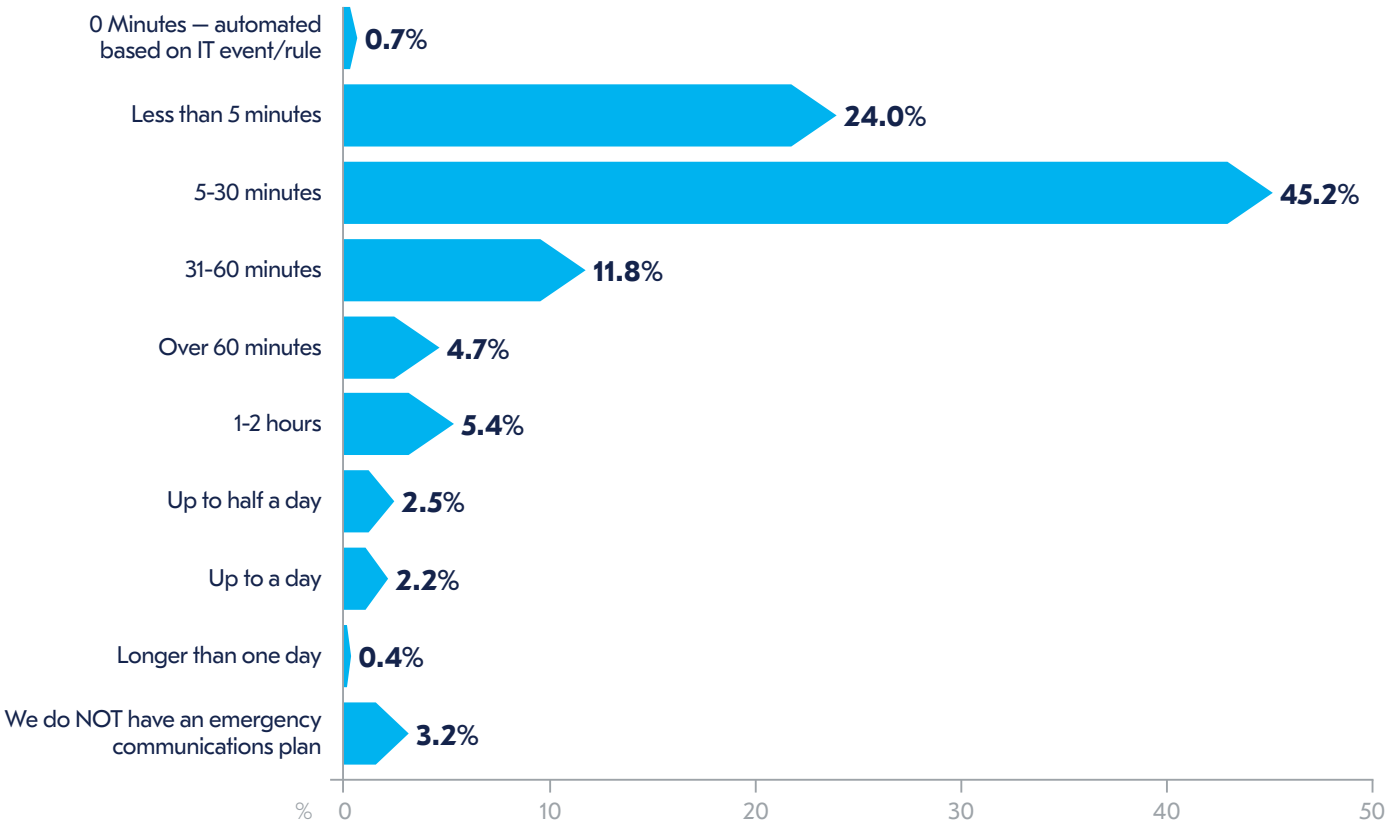
Technologies used to organization collaboration within core crisis teams



Organizations are taking longer to activate their plans this year — but this can be attributed to acquiring better and fully corroborated information

Whilst the broadly the same number of respondents can activate their plans within an hour this year when compared to last year (80%), the number who can activate within five minutes has fallen, with 5-30 minutes being the favoured time boundary. Professionals are taking more time now to analyse and corroborate information in the early stages of an incident than they were in 2020 when management were demanding fast activations in light of the pandemic.

Time taken to activate emergency or crisis communications plan



Plans can be initiated faster if dedicated tools or software is used

Nine out of ten organizations who use dedicated tools and software can activate their emergency communications plan within an hour compared to just 70% who do not use specialist software

Time taken to activate emergency communications plan

	Organizations using emergency communications software	Organizations not using emergency communications software	% difference for those using software vs those who do not
Percentage able to activate plan within 5 minutes	31.7%	14.9%	+16.8%
Percentage able to activate plan within 60 minutes	89.6%	70.2%	+19.4%

It is people, rather than technology, that is normally the cause of a plan failing

Whilst technology is often the first consideration when a plan fails, failure is normally due to human error rather than systems error. Organizations still struggle with staff following correct procedures during an activation, as well as not having the correct contact details for staff.

Reasons for not achieving accepted response levels (top 8 responses)

37.4%
Lack of understanding from recipients

35.1%
Lack of accurate staff contact information

27.0%
Unavailability of mobile network

26.6%
Problems communicating the urgency of response required

24.8%
Failure of manual processes

22.5%
Poor implementation

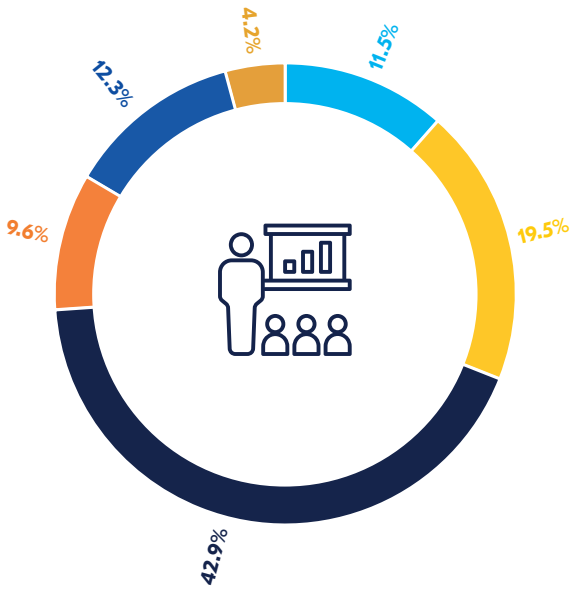
18.9%
Staff working remotely

18.5%
Lack of technical expertise in using the process

Nearly three-quarters of organizations carry out training and exercising at least every twelve months

Most organizations realise the importance of training and exercising to ensure people know how to react when an emergency communications plan is activated. Given that so many organizations still blame failure of emergency communications plans on lack of staff understanding, this suggests that training is a) needs to be carried out more frequently than annual and/or b) training programmes need to be more effective.

Frequency of training of emergency and/or crisis communication plans



11.5%
Every three months or more frequently

19.5%
Every 6 months

42.9%
Every 12 months

9.6%
Less frequently than every 12 months

12.3%
We carry out training ad hoc

4.2%
Never

Covid now causes the same number of activations as IT or telecoms incidents

Last year's report showed that 'disease outbreak' was by far the most popular reason for activating emergency communications plans. This year, the option is tied with 'IT or telecoms incident' which was always the top reason for activation prior to the pandemic.

The top eight reasons for emergency communications plans being activated in 2021

42.0%
Disease outbreak

42.0%
IT or telecoms incident

40.8%
Adverse weather

32.2%
Cyber security incident or data breach

23.3%
IT incident

17.6%
Flood

16.7%
Fire

15.1%
Non-weather related natural disaster

Introduction:

Emergency Communications Report 2022

The BCI's Emergency & Crisis Communications Report has noted a number of trends over the past few years: incidents and crises are increasingly being managed from mobile devices, activation times have lowered with the 'golden hour' now being better classified as 'the golden five minutes', managers are demanding greater functionality from their tools to allow two-way communication, information dissemination and audit facilities. The demands that practitioners now place on their emergency communications solutions means software-as-a-service (SaaS) is fast becoming the incumbent platform for emergency communications, with installed systems waning in popularity.

This year however, we have noted a slight cooling in the growth of SaaS and the employment of new tools and systems. This should be viewed as a healthy plateau, however: 2020 showed a sharp increase in the demand for new tools and technologies as organizations grappled to introduce better communications as a result of multiple activations as a result of the pandemic. We also noted a sharp rise in the employment of SaaS technologies and a drop-off in the use of free messaging systems (such as WhatsApp). This year, the rises have not been as sharp, but the survey and interviews carried out for this report show that many organizations are now fully exploiting their enterprise communications systems (such as Microsoft Teams and Zoom) to communicate, but are now seeking further functionality. Whilst some of this is being done through in-house development of tools, we are now seeing organizations who have never considered employing a dedicated communications solution begin to trial specialist emergency and crisis communications tools for the first time. The sharpest rise has been in small- to mid-sized organizations — previously those who were most likely to consider that investment was

The same problems remain, however. The first point of failure for an emergency communications plan is normally due to people, rather than technology, failure. Although we are noting slow improvements, business continuity and resilience managers are still having difficulty in ensuring staff contact details are up-to-date, and silos frequently remain between HR and other crucial parts of the resilience jigsaw. Encouragingly, awareness of these issues is increasingly, and many organizations are returning to their office environments with staff and management alike keen to engage in additional training. Whilst the pandemic had meant emergency communications plans were being activated more frequently, this meant there was little support given to training on new tools and software due to lack of time. As we enter 2022, we are cautiously looking at a future where the immediate pandemic threat has waned and is becoming more manageable. Because of this, we are expecting to see organizations grasp capabilities of new technologies and ensure best-in-class practices are employed within their organizations.

Section one: The tools of the trade

Section one: The tools of the trade

- **The mobile phone and laptop are the key means of communicating in times of crisis. Other methods, both newer and older, are also used when they suit the specific needs of an organisation.**
- **Software-as-a-service is growing in importance in crisis management just as it is in the wider business environment.**
- **In terms of messaging in crisis scenarios, the security and control of enterprise packages trumps the universality and convenience of free public apps for most organizations.**

Each year, we look to determine which devices are the most popular used in a crisis. We noted last year that COVID-19, and the resultant mass-movement of staff to remote environments, meant we saw an increase in the number of two-way communication tools used and a decrease in the number of onsite and/or one-way communication tools (such as pagers). As workers start to return to their offices, one-way communications are starting to reassert themselves in corporate communication strategies. However, with practitioners increasingly asking for auditable communications traces, crisis teams becoming more collaborative and teams organized in remote or hybrid environments, the use of one-way communications and/or onsite communications is likely to both wane and evolve to better suit newer ways of working.

When respondents were asked which devices they used in a crisis, the most used device was the mobile phone (95.7%). Whilst this may not be surprising, it should be noted that last year, laptops headed the table. This year however, the number who used laptops fell to 93.4% in 2021 from 97.8% in 2020. This shows that mobile devices are starting to play a greater role, driven by the increase of multiplatform software-as-a-service solutions and the ever increasing functionality of mobile telephones, they are fast becoming the natural tool to facilitate an emergency response.

After these two items — which are understandably popular, being broadly ubiquitous in society and particularly the business environment — there is a significant drop-off. This reflects the fact that, beyond the universal accessibility of these two devices, others will be situationally appropriate for use in some organizations but not others. Tablets, for example, are used by 34.6% of organizations (2020: 33.9%), typically with highly mobile personnel, who need to undertake basic computing tasks that would be inconvenient on a phone.

An interviewee commented that their organization had had to invest in a fleet of new tablets, computers and iPhones during the COVID pandemic to allow staff to work from home. The purchase of this new equipment had rejuvenated their emergency communications abilities as the new computers were all set-up with the same software, and staff could communicate effectively — even in remote environments.

"The way [the new investment in Mobile IT devices] factors into emergency communications is that now that we have these computers and they're linked in and we can contact each other, we can spread messages a lot quicker. We can also get messages out to people who are working remotely. Some departments have had around 85% of their staff working remotely, and we are able to get key safety messages and key emergency comms out to people through the computers. We've also had a huge rollout of iPhones, which have Teams and everything else factored in through the Outlook packages that come with them. So we are able to contact people through that and get messages out to people. Therefore, if offices do end up being closed for any number of reasons, then we can get those messages out very quickly. We have issued key remote personnel with an individual phone, and then all team leaders or people responsible for staff are also issued with phones as well, so once they get those emergency messages, they can get the messages out to their staff."

Safety Manager, Government, United Kingdom

Next come walkie-talkies/radios (31.1%). It was noted in last year's report that walkie-talkie usage fell, with just 18.5% saying they were part of the emergency communications plan. This year however, the percentage is back to pre-pandemic levels — albeit below the long-term average. As organizations start to make a return to their more familiar on-site environments, radio communications are beginning to see their usage return. As an interviewee pointed out, radio communications are still regarded as vital items to communicate in many crisis scenarios — particularly when all communications are down. Public address systems (24.3%) have also noted the same trend: their usage plummeted in 2021 with just 13.2% of organizations using them. Now many businesses are returning to full-time or hybrid working environment, usage has almost doubled year-on-year.

"There are plenty of examples I can remember that after an earthquake or even after a tsunami, the radios still continue to operate — even if all comms are down. In a lot of contingency plans there is a lot of use of the radio. Sometimes it is even dictated by the State. I have a practical example from the United States in the states of the south: Florida, Louisiana, Texas. During the hurricane season these regions can be affected by strong hurricanes. As part of the relief, the American Red Cross distribute emergency kits which include a battery radio as standard. A battery radio can also provide people with up-to-date news and you are keeping informed."

Crisis Manager, Humanitarian Organization, Switzerland

Desk phones (30.6%) have been fading from popularity in office environments for some years anyway and, with this year's figure the same as that noted in 2021, it is no surprise to see the trend remaining downward[1], particularly given the rise of remote working since the onset of the COVID-19 pandemic. Furthermore, many organizations have used the opportunity of remote working to reconfigure corporate telecommunication systems. Organizations are starting to abolish desk phones entirely, or move to web-based voice-over-IP-solutions (such as those offered by Microsoft, 3cx or Zoom) where a physical telephone is not required. Such a trend may be welcomed from a cost saving perspective, but opens organizations up to being hit by unplanned downtime: VoIP solutions normally rely on the internet, rather than traditional phone lines, to function. If an organization or individual working remotely loses their internet connection, they may be without means of contact — unless a traditional telephone line backup is in place. An interviewee commented that many IT departments have a reluctance to install "dated" telecommunications architecture to ensure a backup is available.

"We are okay until analogue phonelines are removed as these are our ICCs that are separate to the server providing addional resilience. When it that happens, we will be asking how to put a phone line in that doesn't go through the servers. IT departments are now understanding this requirement and you can hear their brains fizzing 'what do you mean you want to put an extra line in?' 'Yes, we want an extra line that has nothing to do with your server at all. Going nowhere near the network' ultimately we need to have a phone system that will still work in the event of a cyber incident."

Head of Emergency Planning, Healthcare, United Kingdom

Satellite phones (21.4%) are, of course, most useful in areas where connectivity to standard fixed-line or mobile networks is non-existent or unreliable. Their usage has remained fairly static over the past five years, but this year the number of organizations using such devices has risen by nearly seven percentage points. COVID-19 has been a reminder to many organizations of the importance of ensuring staff are always contactable — even when working in an area with no or low network coverage. One interviewee described how their organization was now using satellite WiFi hubs after being hit by network outage during a hurricane in the Caribbean.

"One of the things that we learned years ago through the massive hurricane wave that we had, we lost a country: Puerto Rico. They lost their landlines, they lost their cell towers. So we lost total communications. We kept sending messages, repeated messages, to users we hadn't heard from. When we got through to the management team, even getting people to go to their houses to check to see if they were okay became an issue. We now use satellite WiFi hubs so if this happens again, we can be ensured of continued communications."

Global Director Business Continuity & Resilience

"After the floodings in Germany last year, we had a total communication blackout. Even though we had backup systems in place, we just could not get through to our people in some of the worst affected areas. We had a few staff living in Erftstadt-Blessem — that was one of the worst hit towns — and we just could not get through because internet was down, telephone lines were down, mobile masts down. After that point, we have invested in satellite phones for some staff as we cannot have the same situation repeating itself."

Crisis Management Lead, Mining, Germany

"We are preparing to deploy a team in Tonga after the volcano explosion. Each team leader will have a satellite phone. This will not only allow us to have communication by voice, but with this new generation of satellite phones, it is also possible to use it as a modem. So we can then have guaranteed connections."

Crisis Manager, Humanitarian Organization, Switzerland

1. Gode, S. (2018) The Death of the Office Desk Phone [Online]. Available at: https://www.unifysquare.com/blog/the-death-of-the-office-desk-phone/ (accessed: 30 January 2022)

Another interviewee made the point that sometimes it was not the lack of network or phone network that caused the problem, but the over reliance on a single platform. Many organizations, particularly as a result of adopting their enterprise communication software as their primary channel of communications. The most astute business continuity managers are now considering what will happen if there was a lengthy Microsoft outage, for example. Other organizations took a different view and if there was an outage, they would encourage staff to take the time away from work. Such a strategy would obviously have business continuity issues, however — particularly for those staff who are involved in critical activities.

"Something I have mentioned to management is about our back-up processes when technology fails. Obviously, it's not necessarily my wheelhouse and I have to be careful not to step on the toes of the IT people, but I have said to them we have to think very carefully about how we get messages across to people. Say for instance, we lost the mobile phone network or if there was a serious incident and we lost a mobile phone mast and mobile phones went down, so that we couldn't get messages out to people outside or as you say, if we lost Microsoft, lost functionality of Teams and things like that, how we would contact people."

Safety Manager, Government, United Kingdom

"Our move completely to Teams and to Office 365 and their OneDrive does worry me, because we're now so digitally reliant that if it does go off, we could lose crucial functions. One of the things that came out of it as a bit of learning with the directors was that they just needed to be brave enough that if that happens then they need to say 'It doesn't matter. Just don't do any work today. You can't.'. And that was quite a big change of thinking that if you lost your main source of work, there's no point having people stressing about it while people are trying to fix it. Just give them the day. They'll be much more grateful and much more likely to catch up for you later rather than worrying about it. And that whole bit of wellbeing was very important, it went a long way."

Safety Manager, Government, United Kingdom

"I'm doing an exercise very soon using Teams, and it appears that some IT people in their infinite lack of wisdom are routing their VoIP phones through to Teams. So if they lose Teams, they lose the whole Microsoft suite, they lose their desktop phones and their work mobile phones. By VoIPing it through Teams, you are putting all your eggs in one basket. And if Microsoft suite goes down, you lose the whole shooting match."

Resilience Consultant, Australia

2. Spok Holdings (2021) Why Pagers Still Matter: The History of Pagers (1921-2021) [Online], Available at: https://www.spok.com/blog/throwback-thursday-history-pagers/ (accessed: 30 January 2022)

As an aside, it is worth noting that pagers, long considered an outmoded technology, retain a degree of importance in emergency situations, with 5.4% of organizations still using them — slightly up on last year's figure of 3.5%. They remain particularly popular in healthcare, which was the first sector to widely adopt their use in the second half of the twentieth century. End users and administrators cite the resilience and reliability of the systems, infrastructure and connectivity as key reasons why this legacy technology has not been completely abandoned, and its functionality is yet to be improved upon for a small but vital group of users[2]. Given that technologies which were once ubiquitous are now seen as verging on obsolescence — desk phones, for instance — it is worth remembering that they may retain value for crisis situations, even if no longer of critical importance in normal activities.

What devices are you using to manage emergency situations?

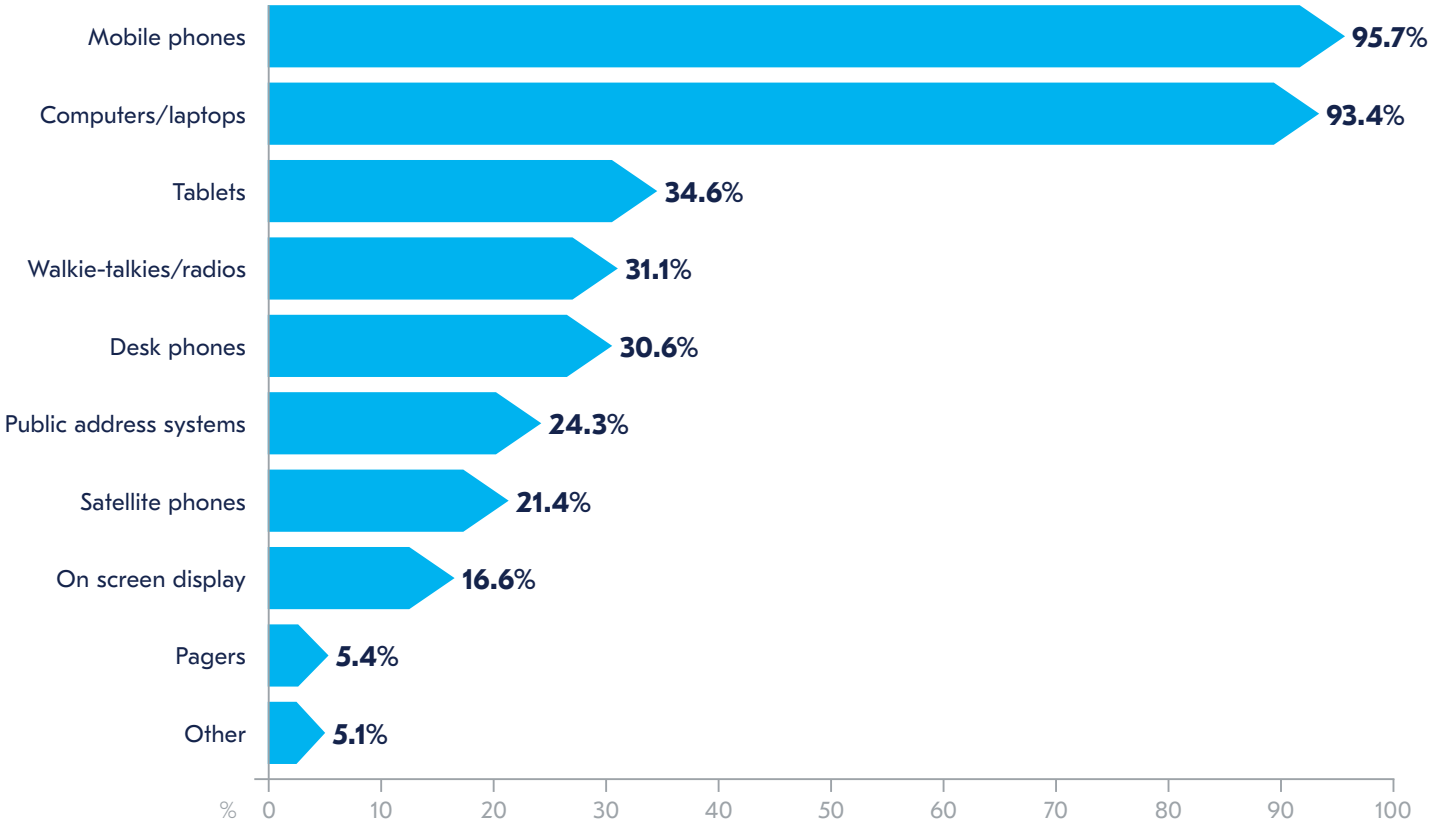


Figure 1. What devices are you using to manage emergency situations?

In total, 61.1% of respondents stated that their organization used tools or software to assist with emergency notifications and/or crisis management — a figure on a par with 2021. Over recent years, we have seen a sharp rise in the number of organizations using software-as-a-service (SaaS) solutions rather than on-premise installed solutions. Using a SaaS solution ensures emergency communications solutions can be accessed over multiple devices, providing more flexibility than on-premise installed solutions. Their rise in popularity during the pandemic was noted as organizations found themselves trying to ensure staff could continue to use emergency communication devices in remote environments, often without a computer to hand.

2. Spok Holdings (2021) Why Pagers Still Matter: The History of Pagers (1921-2021) [Online], Available at: https://www.spok.com/blog/throwback-thursday-history-pagers/ (accessed: 30 January 2022)

Indeed, between 2020 and 2021, use of SaaS software increased by eight percentage points to 74.1%. Whilst the figure has increased just slightly this year (74.2%), we expect organizations to invest in new solutions during 2022 after *The Future of Business Continuity and Resilience Report 2021*[3] revealed a strong appetite for expenditure on new software solutions in 2022.

In addition to being able to deploy a solution across multiple devices, we have noted in previous years that speed of response is directly related to the type of emergency communications solution employed — and the same is true this year. 88.3% of organizations who use SaaS can activate their emergency communications plan within 30 minutes, compared to 57.5% who use an on-premise solution. Moreover, 32.8% of those using SaaS can activate within five minutes, compared to 27.5% who use an on-premise solution. At the other end of the scale, just 3.9% of those with a SaaS solution reported their activation time being greater than one hour, compared to 30% for those with an on-premise solution.

The five-year compound annual growth rate in the of adoption of SaaS also reflects both a general shift among organizations to the use of SaaS for organization-wide tasks (human resources and other 'back office' functions are a particular illustration of this trend[4]) and the clear additional benefits for business continuity that SaaS solutions bring, particularly in case of site unavailability or problems with locally installed servers. With the effectiveness of SaaS provision in this area now amply demonstrated, this is a further reason why we expect many organizations to switch to SaaS solutions in the coming years.

Figure 2. Does your organization use emergency notification/crisis management tools or software?

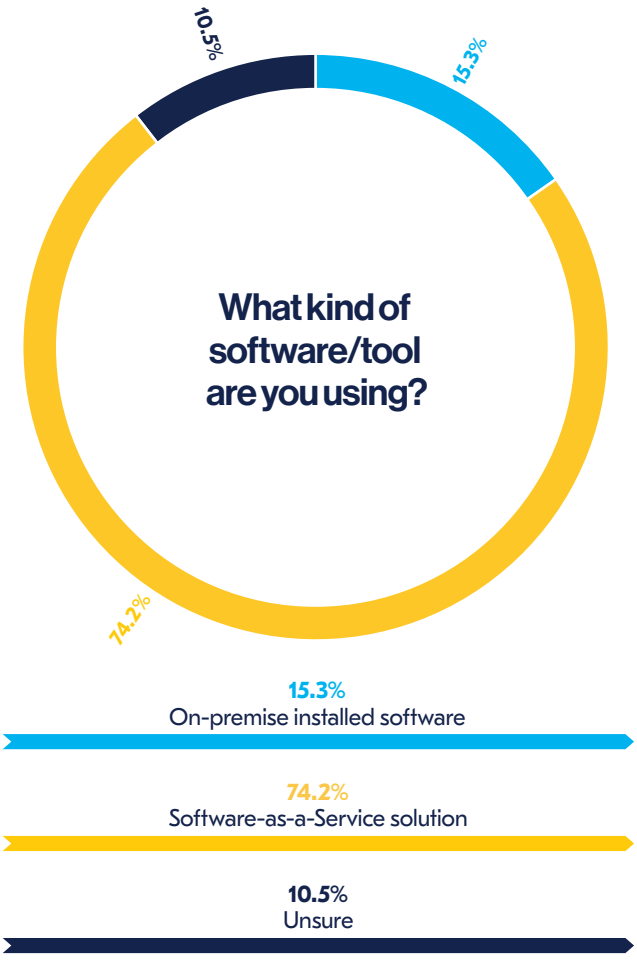


Figure 3. What kind of software/tool are you using?

3. Elliott, R., Lea, D., (2021) Future of Business Continuity Report 2021 [Online]. Available at: https://www.thebci.org/resource/bci-the-future-of-business-continuity-and-resilience--the-emerging-landscape-report-2021-.html (accessed: 30 January 2022)
4. Shiff, L., Kidd, C. (2022) The State of SaaS in 2022: Growth Trends and Statistics [Online]. Available at: https://www.bmc.com/blogs/saas-growth-trends/ (accessed: 30 January 2022)

The next question sought to dive a little deeper into the use of these tools — what did respondents use them for, or in what areas did they provide support? Obviously, with these packages being multi-functional, respondents were able to offer multiple answers, and on average each respondent ticked 4.1 of the 13 options presented. The most common area in which respondents derived support from specialist tools or software was, as has been the case in previous years 'alerting and mobilising large numbers in a short time' (71.5%). This firmly establishes that maintaining communication has long been the central element of organizational crisis planning and is likely to remain so well into the future. Indeed, whilst we have discussed how many organizations are preferring to use collaborative — rather than one-way — as the primary component for emergency communication tools, the need to mass-communicate information to staff fast can be critical to plan success. This is often done more effectively through one-way communications in the first instance, with two-way collaboration functionality following slightly later.

Other areas in which more than half of respondents were supported by their specialist software were the process management elements of crisis handling, such as reporting and updating (54.1%) and facilitating communication within teams (53.1%). Emergency planning was a key feature for 44.9% of respondents, while 37.7% used their software to assist with guaranteeing the safety of employees who may be hard to reach, such as lone workers. Risk management and monitoring both registered around 30% of respondents, while just over a quarter relying on their management tool for documenting processes during an event or for training. The least popular specific responses were for elements of crisis management that may be considered 'softer' . Nevertheless, evaluation and learning, the management of external stakeholders and that of the organization's reputation all scored between 10-20%, meaning that a substantial minority of respondents require their tools to be more complex than simply allowing effective information transmission.

In which areas does your tool/software support you?

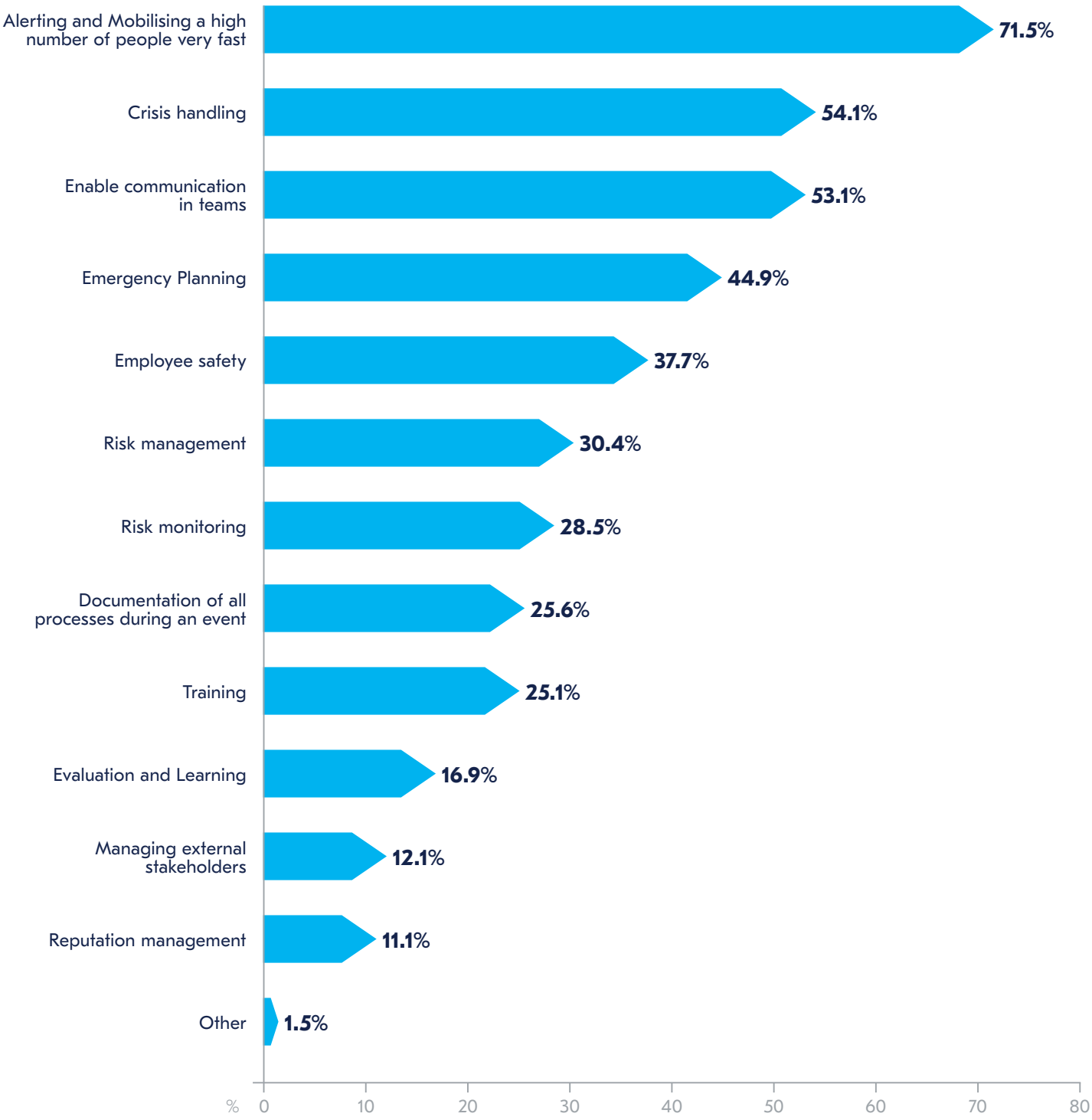


Figure 4. In which areas does your tool/software support you?

Despite nearly two-thirds of organizations using emergency communications tools and software, over a third (38.9%) have yet to introduce them within their organizations or have decided not to deploy them entirely. When respondents were questioned about why they did not yet use a platform, it was once again 'no budget' which was cited as the primary reason by 36.6% of respondents. Interestingly, despite many professionals reporting funding for people, software and systems would be easier to obtain this year, this does not appear to ring true here — particularly when only 30.0% reported that lack of funding was the primary issue in the 2021 version of this report. Wariness of complex implementation processes was the key factor for 14.8%, while 13.3% simply saw no benefit.

Encouragingly, just 11.1% of respondents said that their organization was too small for such a tool (2021: 20.0%) suggesting that smaller companies are starting to realise the benefits of having a dedicated tool in place. Other respondents suggested their organization was too small, lacked expertise to manage such a tool, or considered contact with staff to be a less urgent requirement. Interestingly, the move to remote working has not led to organizations abolishing having a tool in place: just 4.4% of respondents said that the move to remote working had meant there was now no need for them to have such a tool in place. More than an eighth of respondents ticked the 'other' box for this question, and many of them explained that software for crisis communications was in the pipeline or scheduled to be introduced when budget is available. It appears that practitioners see clear benefits from the tool-based approach to crisis communications, even if it is an unaffordable proposition at the current time.

An interviewee commented that a lack of budget frequently meant that organizations did not invest, but the desire to invest was very much there. The same interviewee also highlighted how an emergency notification system (ENS) was something which was necessary in most organizations, rather than merely desirable — and the budget should be prioritised to support its implementation.

"An example might be you need three people to go to source material at an archive warehouse. But you may only be able to contact Rachael and Chris. Mike might be the approver. How are you going to get a hold of him? You've only got a couple of approvers in your office. This really highlights the need for ENSs to have that capacity to keep dialling or using other means to find the necessary people and to keep a log of things like 'okay, we've got a hold of Rachel and Chris, but we can't get a hold of Mike, so we need to try John.' That sort of thing. This client does not have an ENS. They rely on a lot of phoning people, emailing people and all sorts of hopefulness. Now that's not to suggest for a nanosecond that they wouldn't love to have an ENS, but they haven't got a budget for it."

Resilience Consultant, Australia

"An ENS is a necessary tool. I mean, you invest in exercises. If you do have a halfway decent business continuity management system in your business, you invest in exercises. You need to invest in an ENS too, because it's a necessary tool for good service delivery your investment in business continuity."

Resilience Consultant, Australia

Another interviewee described how they had wanted a tool to use across all the geographies in which they operate but found this was proving to be impossible due to local restrictions with communications. This meant certain teams had to use their own, local solutions.

"We had the vision of having one tool for everyone and everything, but that was soon turned out to be unrealistic due to various and sometimes different needs. For example, you can have the use of a tool, but in some countries they will throttle and restrict the communications that are sent from outside countries, so it's not effective during an emergency. We've therefore gone to tools by where it's needed. We have the basic one, which is our own bespoke one, which is the default. And if there's a good reason to have a dedicated tool per region, then they have their own."

Global Security Director

36.3%
No budget defined

14.8%
Complex implementation processes

13.3%
We don't see the benefit of such a tool

11.1%
Our company is too small for such a tool

7.4%
No capacity / personnel to set up and care for such a solution

4.4%
We are now based remotely and there is no need to contact staff onsite

12.6%
Other

Figure 5. What is the main reason for you not having or not planning to have a tool/software for emergency communications/crisis management?

The BCI's *Crisis Management*[5] report in September last year demonstrated the growing importance of good communication and collaboration across the core crisis team, particularly as many organizations were remodelling traditional physical "crisis rooms" to virtual environments. When respondents were asked about the platforms they used within their own crisis teams, the use of enterprise communication software and collaboration features in dedicated emergency/crisis communication tools are fast becoming the incumbent methods of communication. Narrative additions to responses to this question suggested that organizations are increasingly using several solutions for communication within their crisis team, highlighting the long-held BC principles of redundancy and contingency.

The most popular platform was the messenger functionality included within standard business software, with almost two-thirds of respondents (64.3%) making use of Microsoft Teams or a similar package (2021: 63.5%). Interestingly, the number of organizations exploiting the collaboration and virtual crisis room features of their emergency communications tool has almost caught up with those using enterprise software (such as Teams) to collaborate within their crisis management: 63.5% cited this as a method they used, compared to 57.5% in the previous year's report. The next two choices were perhaps the solutions that would have been most popular had this question been asked 10-15 years ago. Nevertheless, conference calls (56.3%) and physical crisis rooms (54.9%) retain a significant degree of popularity — and many interviewees spoke that there would always be a need for a physical crisis room and/or a command centre within their organizations. An interviewee commented that the longevity of the pandemic had caused them to review how they communicate in a crisis and, as a result, they had built their own highly effective system around Teams and Zoom.

5. Elliott, R., Lea, D., (2021) Crisis Management Report 2021 [Online]. Available at: https://www.thebci.org/resource/bci-crisis-management-report-2021.html (accessed: 15 February 2022)

"In the past, our major incidents have been fairly short lived. They'd last maybe a week or two, but they wouldn't last two years and ongoing. So the crisis management team and the tools they used were always built around addressing the immediate risk and immediate problems, but we were aware we needed something for prolonged incidents; something that more spoke to our needs because we are quite a unique setup company. So we moved towards a bespoke tool and are very proud of ourselves for doing so! Just after that, we experienced civil unrests in various countries, then we had the pandemic and we found that we used Teams and Zoom more frequently due to their ease of use, user familiarity and availability. These communication methods were relatively unheard of beforehand, and now we use them on a regular basis. So the method for communication changed and then during COVID, the method further has evolved. It's more the BAU thing now. However, we still need an independent emergency communication tool which is off our IT network to provide resilience"

Global Security Director

"We are currently in the process of moving from Zoom to MS Teams, but at present Zoom is fit for purpose and provides the functionality that we need without having to add complexities to the situation. Over the next couple of years we acknowledge that there will be a need to ensure the technology can enable us to feel like we are in the room together and function as a virtual crisis room with supporting tools to make life easier when managing a crisis."

Head of Resilience, Financial Services, Australia

While the use of messaging services from outside the corporate environment such as WhatsApp has been widely decreased both within organizations and among the wider business security and continuity communities. However, its convenience and universality probably contributes to it still being used by more than a third (33.9%) of respondents' organizations. When this was discussed further with respondents, many used WhatsApp purely as a source of non-confidential office "chat" — although most admitted it had lapsed into being used for critical communications purposes.

The confidentiality of messaging content determines the type of platform to be used within some organizations. An interviewee discussed how non-confidential emergency communications were carried out on their enterprise communication platform whilst confidential communications were done through a bespoke, highly secure, tool. The same organization had also banned WhatsApp for communications, with staff facing disciplinary action if they were found to be using it.

We've actually stated to staff that using some applications to talk about sensitive internal things is a disciplinary issue. We'd explain why, why it's important, why you are consenting to give your data to someone else when you use them. I think two-way mass communication is going to be a real challenge because these people are so conditioned for social media and free communication applications, that's their expectation. Therefore, I believe that we need to be strict on which communication methods to use for certain types of information, however we also need to provide adequate tools that meet user needs"

Global Security Director

For some organizations, the problem is not necessarily the staff using WhatsApp, but senior management not appreciating the importance of using a robust, secure communications system in a crisis. In this instance, an education and training programme for management would be recommended in the first instance.

"In a previous job in the Government, we struggled to get buy-in from senior management around the need for emergency communications tools and facilities. We would inform them that there's a system available that would enable us to get a call cascade out to everybody that needs to be contacted if the office was closed or if there was an incident. They'd then come back with 'well, we've got a staff information line for that', 'you could just send WhatsApps,' or 'people know who are on their team, they know where they should be, they can phone them."

Safety Manager, Government, United Kingdom

How do you organize collaboration in your core crisis team?

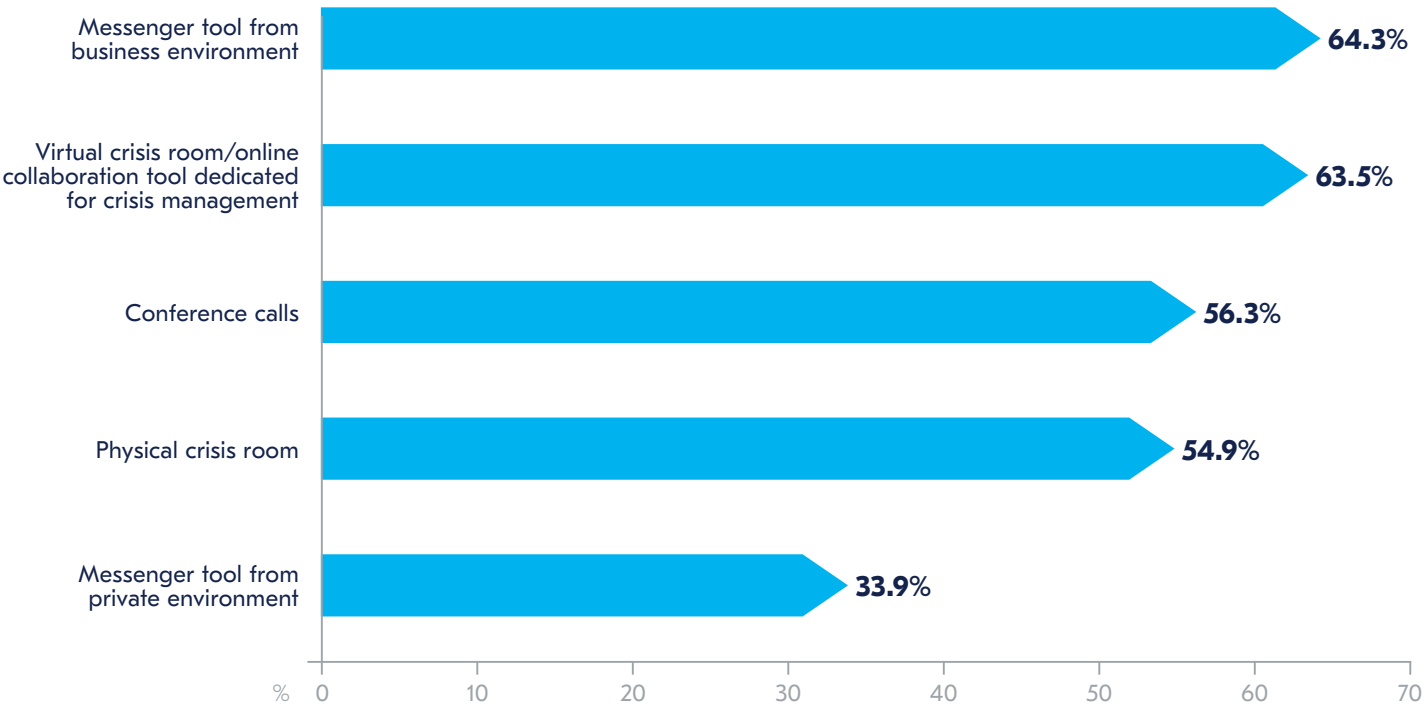


Figure 6. How do you organize collaboration in your core crisis team?

Drilling further into the specifics of messaging apps, respondents were questioned about their preferred option in emergency scenarios. With solutions such as Teams being propelled to the forefront of corporate life over the duration of the pandemic, enterprise messengers such as Teams or Slack have gained in popularity significantly. Moreover, this year we have noted a near four percentage point increase with 47.3% of respondents stating that they use enterprise messengers as their primary tool (2021: 43.5%). Dedicated secure messaging apps (integrated into emergency communications solutions) fell slightly from favour this year, with 21.9% choosing this solution within their organization (2021: 23.8%). It is likely, however, that this slight divulgence in figures for dedicated apps and secure messaging solutions will close in the mid- to long-term. Some interviewees discussed how they were looking for an alternative solution to Teams as a) Teams messaging was being overused and genuine emergency communication messages were being missed; b) some business continuity managers were concerned that their organizations were becoming too reliant on the Microsoft platform and c) there were concerns of the availability of Teams if the organization was targeted by cyber criminals.

"One of the reasons we're getting this tool is because we're worried about cyber attacks and those criminals getting into our Microsoft apps, especially Teams. It's really important therefore that we get this new software up and running as soon as we can; it's a real security hole. We need our new laptops!"

Director of Risk & Resilience,
Pharmaceuticals, United States

Despite the demand for secure messaging, one in five (20.1%) organizations still rely on free apps such as WhatsApp, WeChat or Signal (2021: 19.1%). Although WhatsApp is often viewed as the poor solution for messaging due to security information, lack of audit trails and users not seeing messages due to alerts being switched off, it can still have its place in the corporate environment, particularly to support local or team-based transmission of non-critical information. Indeed, with the growing emphasis on mental health, casual conversation over tools such as WhatsApp can help with traditional "water cooler" chats or provide a platform for conversations around non-critical issues. Messaging is still not the right solution for all organizations, however, with 6.1% choosing not to use it in any form — albeit down on last year's figure of 9.5%.

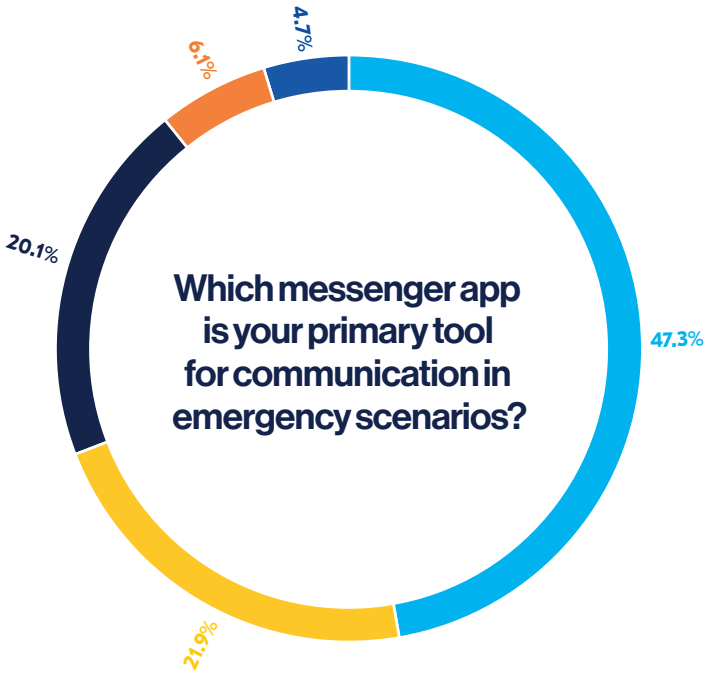


Figure 7. Which messenger app is your primary tool for communication in emergency scenarios?

As illustrated in earlier questions in this section, the right solution varies from organization to organization. This idea was reinforced when respondents were asked if they were happy with the solution that was in place in their business or institution. 86.6% that said that they were happy, roughly evenly divided between those who qualified their yes vote with 'somewhat' (44.0%) and those who were unequivocally happy (42.6%). The unhappy 13.4% are quite a large constituency however, even if a minority, and providers will be keen to communicate how their product could solve these organizations' problems.

The level of happiness is dependent on the type of solution used. 57.8% of those who use a dedicated messaging app within an emergency communications tool were happy, and just 3.3% were not. For those using an enterprise messenger (such as Microsoft teams), just 38.9% were happy — nearly 20 percentage points less than those who have a dedicated solution. For free messaging apps, whilst over a third *were* happy (36.4%), 23.6% were not happy. The figures are broadly similar to those published in 2021, although dissatisfaction levels grew by 6.7 percentage points and 4.8 percentage points for enterprise messenger and free messaging apps respectively.

The limitations of free messaging apps and also with enterprise messaging apps to some extent are highlighted below:

1. The lack of confirmation to show whether a message has been delivered successfully or read leading to a lack of audit trail;
2. Confidentiality risks (e.g. staff forwarding information to outside parties or receiving information erroneously);
3. Messages being ignored as they became lost in a stream of messages;
4. Security concerns and data privacy;
5. Users becoming indifferent to messages within free tools due to the crossover with their personal life.

Such limitations remain true in 2022, and we are seeing more organizations now switch to dedicated messaging solutions because of this. Some organizations have managed to personalise enterprise software such as Teams to ensure it works as a secure messaging tool with functionality akin to a dedicated solution, although admit they needed experts within their own organization in order to achieve this. Whatever solution an organization chooses, the ability of that tool to meet the requirements of the organization is critical and, whilst developing existing in-house enterprise software works for some, others will still require the functionality of a dedicated tool and/or service — particularly if there is a lack of specialise IT experience within their organization.

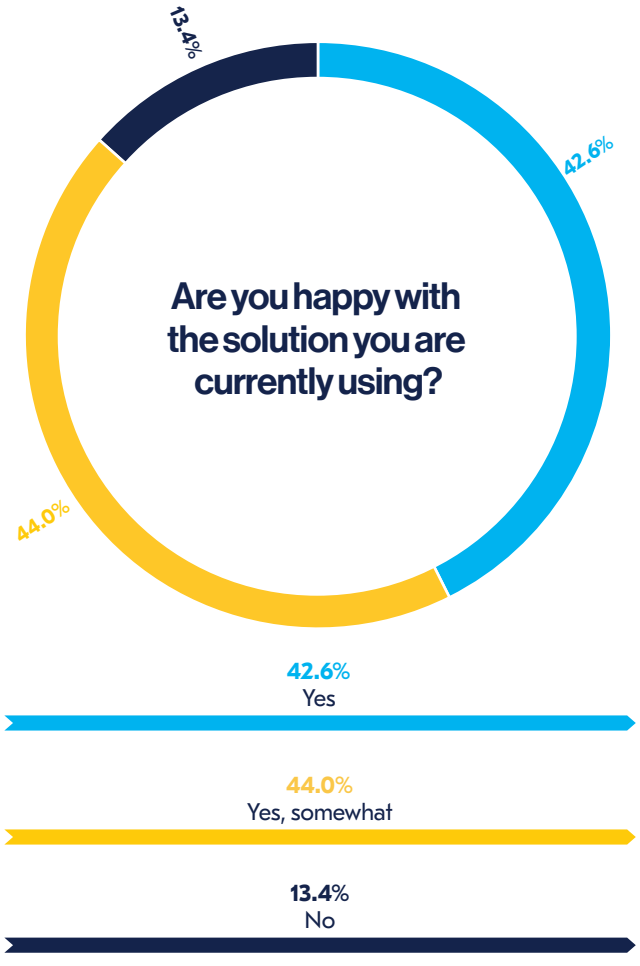


Figure 8. Are you happy with the solution you are currently using?

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

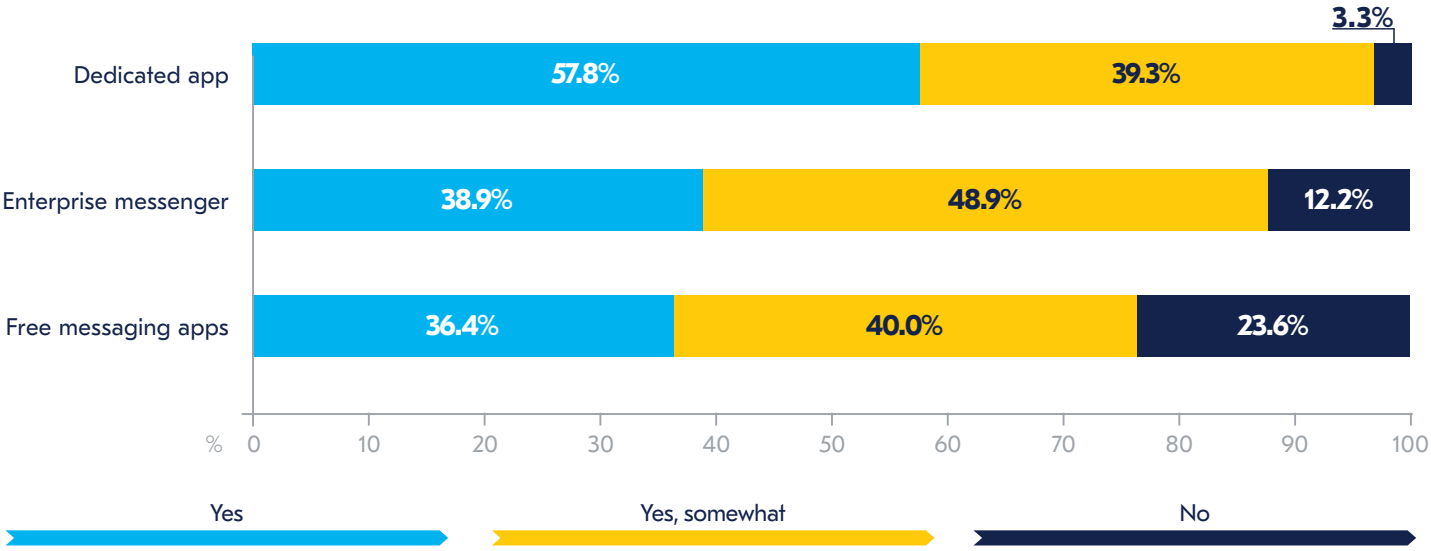


Figure 9. How important are the following aspects for your alerting and emergency communications?

Section two:
Response and timing

Section two: Response and timing

- **The idea of the 'golden hour' for responding to incidents remains valid, though the 'golden five minutes' continues to gain currency.**
- **Informing top management produces similar results in terms of timing to responding to incidents, and is effectively now a part of the latter.**
- **Expected response levels are achieved just over three-quarters of the time when initiating an emergency communications plan – lack of understanding of the required action or incorrect contact details, both on the part of recipients, were seen as the main obstacles to higher response rates.**

The next group of questions focused on responses in emergency situations. First, respondents were asked how long on average it took to activate their organization's emergency or crisis communications plan, with responses in various bands from instant (for example, via an IT event or rule) through to more than one day. The well-established idea of the 'golden hour' for reacting to emergencies remains significant — more than 80% of respondents could activate their plan in 60 minutes or less. However, for almost one-quarter of respondents, the 'golden hour' is now a 'golden five minutes' as 24.7% were able to initiate their plan either instantaneously or within that short timescale. While that was not the most popular band, it is significant that the next one, 5-30 minutes, was 45.2%. This acceleration of response times is broadly in line with the data from a similar question asked in our *Future of Business Continuity Report 2021*[6]. Each band above 60 minutes attracted less than 6% of responses, one unfortunate respondent chose 'longer than one day', while 3.2% said their organization had no emergency communications plan at all.

6. Elliott, R., Lea, D., (2021) Future of Business Continuity Report 2021 [Online]. Available at: https://www.thebci.org/resource/bci-the-future-of-business-continuity-and-resilience--the-emerging-landscape-report-2021-.html (accessed: 30 January 2022)

There is a notable decline in the number of organizations who can activate their plans within five minutes this year. Last year, some 40.8% of respondents reported they were able to activate their plans within five minutes, compared to only 24.7% this year. Although some of the difference is likely to be due to different survey demographics year-on-year, some professionals commented that 2020-2021 had seen so many activations of emergency communications plans that management were requesting information to be better analysed before plans were activated, whilst others said that pandemic related alerts required swifter attention than alerts for incidents that took place in 2021. However, now emergency communications plans were now being activated for other reasons — which did not require such a fast activation to be made — a longer activation time was preferred in order to collect and corroborate the information required.

"Five to 30, but for us, that's fast enough. We have a 15-minute response time where from [our messaging provider] to them acknowledging it. Within half an hour, if there's anything to do, that's when our strategic on-call will be looking for an update if there's something to worry about. Because we're not fighting fires or rescuing people we have a little longer to respond. If there's an IT outage or anything like that, IT need time to work out what's wrong. There's no point in trying to do it faster. It's wasted information at that point."

Head of Emergency Planning, Healthcare, United Kingdom

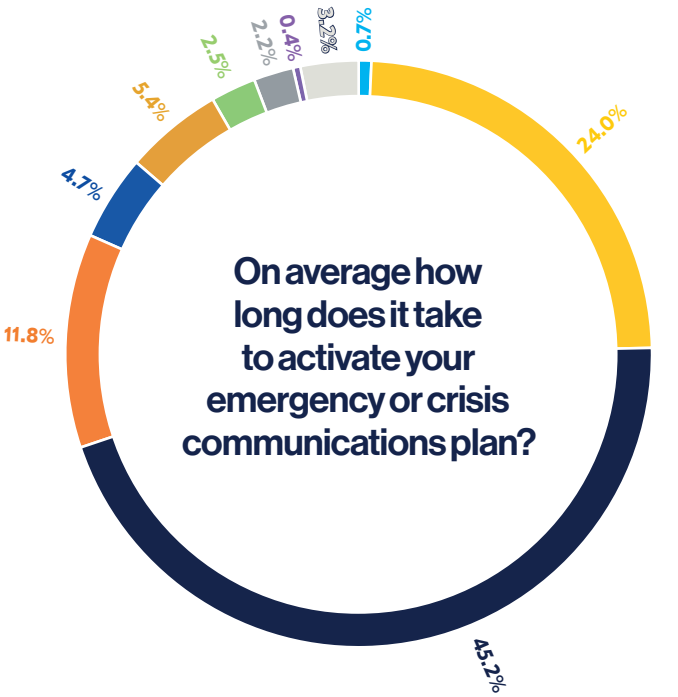
"t usually takes a couple minutes to validate and verify the information coming through prior to seeking approval and hitting send. The priority is turning the assumptions into facts very quickly and ensuring you are comfortable that they are correct. One of the things we have found is the value in spending an extra few minutes validating the information, we like to have that five to 30 minute type speed of communication that allows you to tailor messages, make sure they're accurate and then get the information out to the people that need it. It depends on the situation and uniqueness of the incident but in order to get the messaging correct having that extra time reduces confusion and unwanted panic in times of an emergency, crisis or major business disruption event."

Head of Resilience, Financial Services, Australia

"It is vital that we inform management before implementing a plan because there is a huge reputational risk. We therefore need to work with the senior management team because we are a biggest organization. There is also a big danger with social media and we need to be very careful. We tell our people that if we made a mistake in the past, only 10 people would know. Now it's more like one million. Because we are such a large humanitarian organization it could have a huge impact on the security of our colleagues. For this reason, we need to be very careful about activating our plan and ensure management are fully engaged with the process. We really need to protect our people, first and foremost."

Crisis Manager, Humanitarian Organization, Switzerland

The speed of response time is directly proportional to whether an organization uses emergency communications tools and/or software. For organizations which use emergency communications tools/software, 31.7% are able to activate their plans within five minutes with 89.6% able to do so within that traditional 'golden hour'. For those that do not use dedicated tools, 14.9% are able to activate within five minutes, with just 70.2% able to activate within one hour.



0.7%
0 Minutes — automated based on IT event/rule

24.0%
Less than 5 minutes

45.2%
5-30 minutes

11.8%
31-60 minutes

4.7%
Over 60 minutes

5.4%
1-2 hours

2.5%
Up to half a day

2.2%
Up to a day

0.4%
Longer than one day

3.2%
We do NOT have an emergency communications plan

Figure 10. On average how long does it take to activate your emergency or crisis communications plan?

How long does it take to activate your emergency communications plan?

	Organizations using emergency communications software	Organizations not using emergency communications software	% difference for those using software vs those who do not
Percentage able to activate plan within 5 minutes	31.7%	14.9%	+16.8%
Percentage able to activate plan within 60 minutes	89.6%	70.2%	+19.4%

Figure 11. How long does it take to activate your emergency communications plan?

In the contemporary business environment, enacting the crisis plan goes hand in hand with keeping the executive team informed. The next question asked how long the latter took on average — and produced a similar pattern of answers to the former. Again, the most popular response was between five and 30 minutes (51.8%), with the bands below (less than five minutes), and above (between half an hour and an hour), each chosen by just over 15% of respondents. Longer bands were once more chosen by single-figure percentages, and one respondent said it would take more than a day to inform top management in their organization. Overall, this represents a slightly slower speed than that noted in 2021, where 24.4% of organizations claimed they could provide information to top management within five minutes. Again, this is likely to be down to the increased information requirements required from management, and also the nature of the information being shared (e.g. a COVID-19 outbreak in an organization would have required an immediate response in early 2020, but urgency would be decreased in the latter part of 2021 due to COVID-19 becoming less of a deadly risk due to vaccinations and less harmful mutations).

"One of the key issues we have is because we've got so many different stakeholders, we need to determine if a message really does need to go to everyone. We usually go to the CEO or to their COO first and say, 'Look, this is the situation. These are the messages we're going to give and I'm assuming this will be out in the public domain as well, because of the nature. Do you validate this?'. We've tried to streamline this in the past, to go straight to post the message out and to have the authority. In reality however, a message can usually wait for 20 or 30 minutes in most cases, unless it's an active shooter or something like that. By using that half hour, we have the time to prepare a message with our marketing communication people. In the past, we have had communications go straight out into the public domain and it's been used against us. In addition, we often proactively prepare holding statements ready for communication, which buys us time. So this was our control of that narrative."

Global Security Director

Another interviewee commented how it was difficult to work with different geographical regions who followed different rules to following emergency communications plans. In his home nation, the United States, mass communication tools are embraced by most staff and out of hours communications readily received. Elsewhere, staff are more difficult to contact due to different ways of working and speed of communication is frequently compromised. Another commented similar issues, despite being an organization operating in a single country.

"This is a very country centric response. In the US, people, employees have accepted that mass communication is a way to communicate with employees. When you step into the European market, it's very different by country. If I'm looking to get an answer from a worker after business hours, I'm sometimes waiting until tomorrow to get a response because work communications are switched off after hours. That's why communicating with staff can be ultimately a challenge is because you want those timely responses to come in, but you may not get that timely and as fast as you want."

Global Director Business Continuity & Resilience

"Another former client has a footprint of more than 100 offices Australia-wide. They all had different health orders, because the health orders under the state Health Departments, not Federal government. So while trying to manage the information applicable to that office or those locations collectively, we discovered ENSs weren't always configured for sending these instructions to all employees at particular locations."

Resilience Consultant, Australia

The relaying of information to management tends to require more human intervention due to the need to corroborate information and provide an accurate summary of an incident to management. Nevertheless, having an emergency communications system does allow information to be transmitted quicker to management, with some interviewees commenting that the functionality of the specific tool used helped with the information verification: 84.9% of organizations which used specialist tools and/or applications were able to provide initial information to top management within an hour, compared to 79.5% of those without a tool.

"We have a feature in our solution that provides a newsfeed, interlinking with our subscription to another intelligence database, that really helps corroborate against information we are hearing from the ground. And, of course, social media. We only enabled this in August last year, and we find we're getting information passed on much quicker as we're now confident of accuracy."

Director of Risk & Resilience, Pharmaceuticals, United States

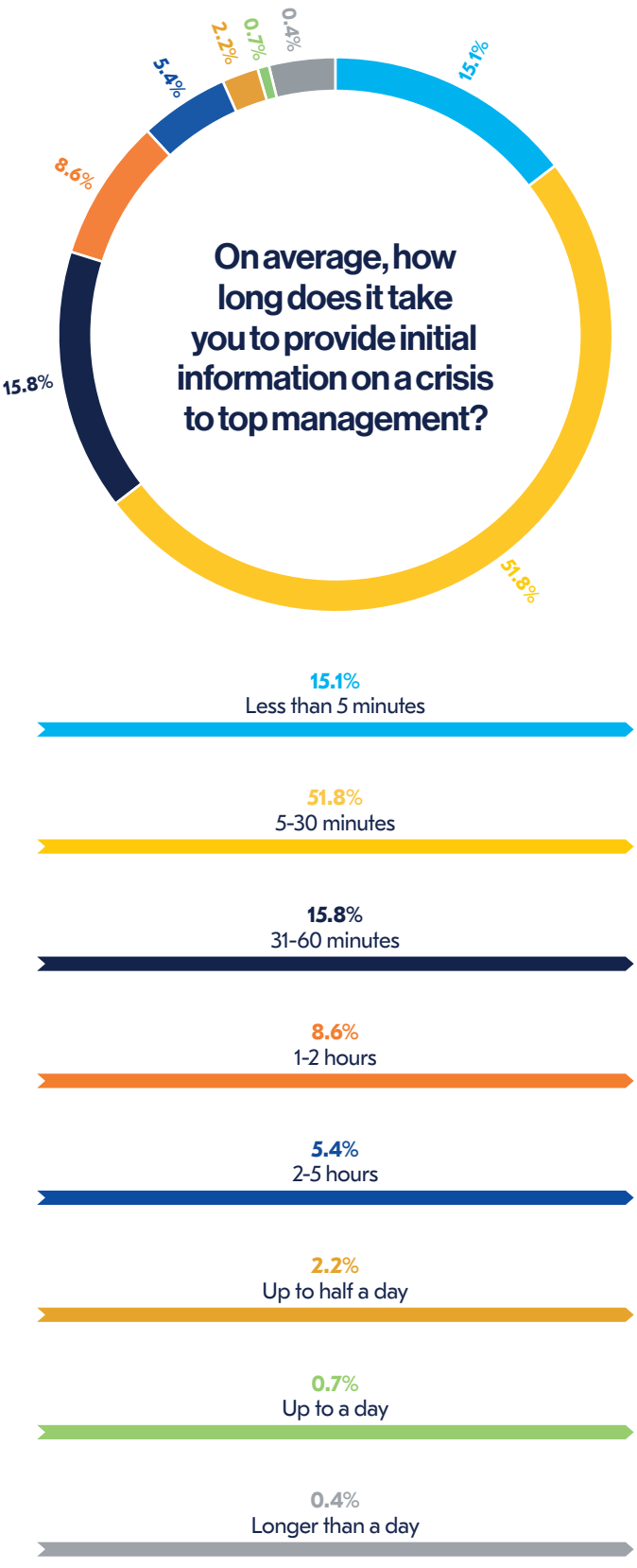


Figure 12. On average, how long does it take you to provide initial information on a crisis to top management?

Of course, the most significant tests for any plan are those where it is invoked in real situations. When asked what percentage of deployments of their plan achieved the expected response levels within their organization, the average response from respondents was 77.5%. This compares to 78.5% in 2021, but is above the 73.1% noted in 2020. Last year, some interviewees commented that remote working meant there were less activations needed onsite because all or most staff were working remotely which enabled them to better meet response times. The fact that this year's figure is just one percentage point less than 2021 demonstrates that most organizations have managed to maintain their good levels of response, despite a return to the workplace which, in many cases, also meant a brand new working environment which had the potential to affect the response. Again, the differences between those that do use a dedicated tool and those that do not was apparent: 79.0% of those who use a tool were able to meet their expected response levels, compared to 75% of those that did not.

"We've had dozens of activations this year because of COVID. As we'd drilled the importance of responding to messaging and knowing what to do in an emergency through the years leading up to COVID, they've followed well and have generally known what to do. I think if we'd have done training on the top of that though, we'd have got a little more pushback from senior management; perhaps staff reticence. Now most staff are back working in offices, we'll start our training again. Every six months minimum and we'll make sure we revise it to include learnings from COVID. We've got a lot!"

Director of Risk & Resilience,
Pharmaceuticals, United States

How often have you achieved your expected response levels?

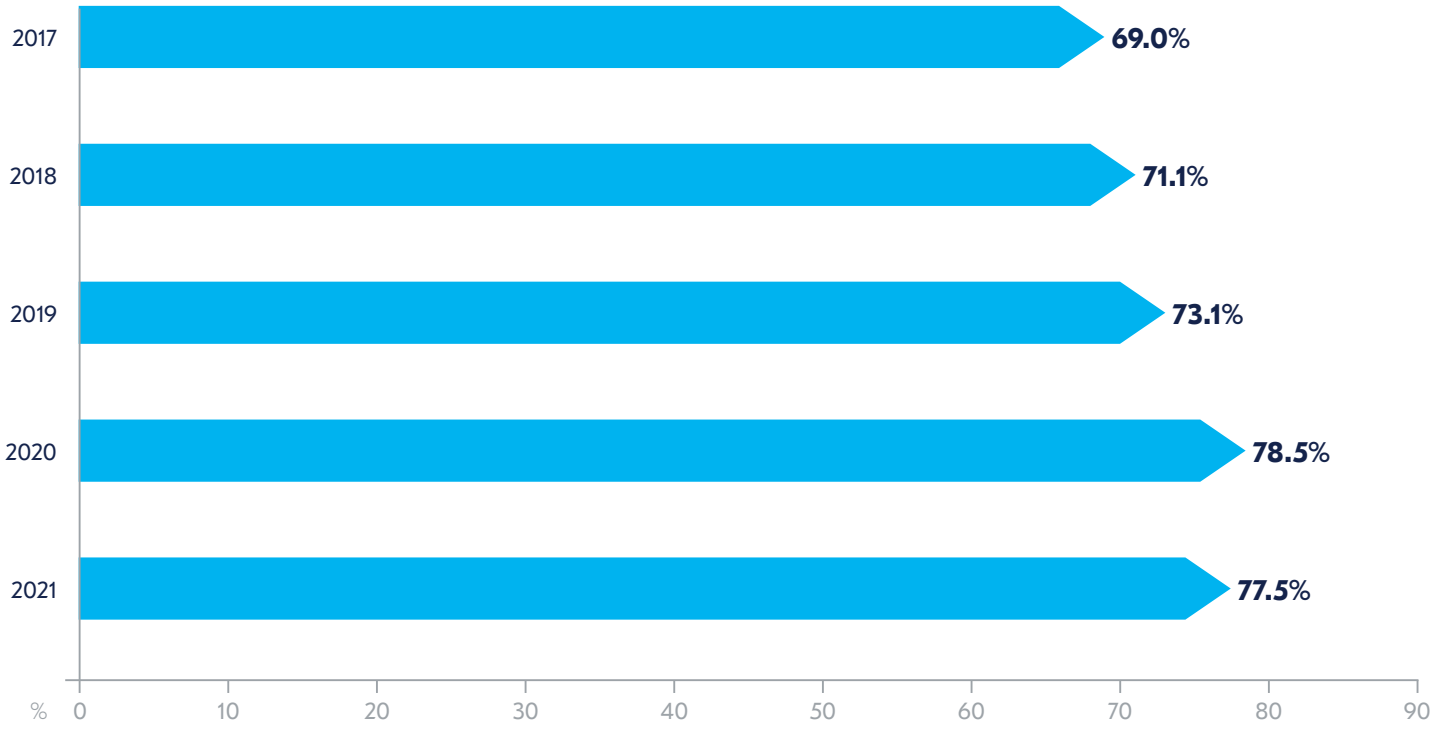


Figure 13. How often have you achieved your expected response levels?

Knowing why response levels did not meet expectations is an important lesson to be learned for future events. Each year, this report highlights how most failures are down to people and process, rather than technology itself. This year is no exception: the survey asked what respondents believed caused the failure to meet their response time, and asked them to tick as many answers as were applicable — on average, each offered about 2.7 responses.

The most common answer was lack of understanding on the part of recipients, which was cited by 37.4% of respondents. Such an answer suggests that staff have not received the training required and/or are not engaging with the communications process. An interviewee spoke that their organization had not got a tried and tested communications plan in place at the time of the Paris terrorist attacks. The organization ran a chain of shops in central Paris and many were unsure whether or not to open the following day — some did, and some did not. The interviewee described how processes had now changed and learnings made to ensure this would not happen again.

Recent BCI reports showed that training and exercising had decreased during the pandemic, often because organizations found they were having to activate their plans so much because of COVID-19 related issues, there was no time for training to take place on top of that. Whilst this would not be the advisable option to take, it does appear to have worked to a certain extent: response times not being met due to lack of understanding fell this year by five percentage points. The fourth most popular answer — communicating the necessity of an urgent response — was selected by 26.6% of respondents. Again, whilst training could help here, it also shows how using third-party free apps (such as WhatsApp) for urgent communications can lead to messages being missed, or the degree of urgency taken into account.

The second most popular reason for not meeting planned response times is due to a lack of accurate contact information, with 35.1%. Again, whilst this has fallen from last year's figure of 38.6%, there are still organizations which have difficulties keeping staff contact details up to date — particularly if they are using manual systems such as Excel.

Encouragingly, however, interviewees spoke of how COVID-19 had proved to be a useful driver for staff to regularly update contact information. The picture is not entirely rosy, however. Others spoke about how their HR team worked in silos and would not work with the business continuity team to ensure details were kept up to date. Siloed working practices have long been a point of failure in many business continuity plans and, although many professionals are slowly seeing these siloes being broken down, it is clear that many still remain — to the detriment of an organization's resilience.

Another issue is staff willingness to pass over their own contact details for out of hours. Some choose to exercise their right to keep their own contact details confidential, even though it means they may not be available in a crisis. One interviewee who struggled particularly with this issue exclaimed that many of those staff *would* happily be contactable by WhatsApp — even if they chose not to share their contact details. The frustration was palpable.

> **"I would like to be shot of WhatsApp. It's great for organizing a trip to the pub — that's what it's for. But I would like to go for a more auditable system, I have to say. But again, the last two years has torpedoed any thinking about anything other than COVID19, because there's been no bandwidth to do it. Some of the trusts use bespoke hospital communications apps. But it's an extra app that people have to use and be familiar with and download on to personal devices. So it's quite challenging, to be honest, to pick a different one. But you're right. WhatsApp is not a way to go."**
>
> Head of Emergency Planning, Healthcare, United Kingdom

Other organizations took a more rigorous approach to getting staff information; demanding staff provide their contact details in case of emergency. If a critical worker failed to supply this information, they faced the possibility of losing their job.

> **"In other places I've worked, they've actually required the critical staff to individually sign off a privacy statement that they approve and are willing to release their personal information like mobile phone or cell numbers for exercises and incidents. We've actually had to quite actively go out to all of our critical staff and get them to complete and sign the declaration. Occasionally they won't sign. To which my reply is 'That's fine' and I say to their team leader "this person doesn't wish to sign, that's fine. Replace her on your team."**
>
> Resilience Consultant, Australia

The first technical point of failure - network unavailability — came next with 27.0% of respondents. Manual processes failed in 24.8% of cases, while poor implementation was blamed by 22.5% of respondents. Other responses attracting ticks from more than 10% of respondents were the problems caused by remote work, lack of technical expertise in using the process, the failure of IT, and the failure of devices. Some professionals might consider network unavailability to be something which can be blamed on network outages or IT department failures. However, in reality, outages can be caused by other reasons — and some which may not have been considered in BC plans:

> **"One of the reasons why we got limited or no bandwidth is, everybody's watching Netflix. During the day, it's because kids are on Zoom being home-schooled. So communicating with remote workers, if you're relying on networks that might be also be used for home-schooling or Netflix, you're running out of bandwidth whereas if you have a standalone ENS, that's less of an issue."**
>
> Resilience Consultant, Australia

Additional narrative responses shed further light on why and how failures occurred. A number of these cited an absence of training or noted a failure to test plans often enough for personnel to be aware of the expected response. Fear of phishing or other bogus messages was also specified as a reason why staff failed to respond. This is likely to become a more significant problem as phishing attempts become more sophisticated, phishing simulation exercises conducted within organizations follow suit and become more common[7], and workforces become accustomed to being the first line of defence against phishing[8]. Instilling confidence in staff that an emergency message is not a phishing attempt looks likely to be an important challenge for security, IT and BC teams.

7. Rapid 7 (2018). Why You Should Let Your Security Team Go Phishing [Online]. Available at: https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-whitepaper-why-you-should-let-your-security-team-go-phishing.pdf (accessed: 30 January 2022)
8. ain, D., Kostiainen, K., Capkun, S. (2021). Phishing in Organizations: Findings from a Large-Scale and Long-Term Study [Online]. Available at: https://arxiv.org/pdf/2112.07498.pdf (accessed: 30 January 2022)

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

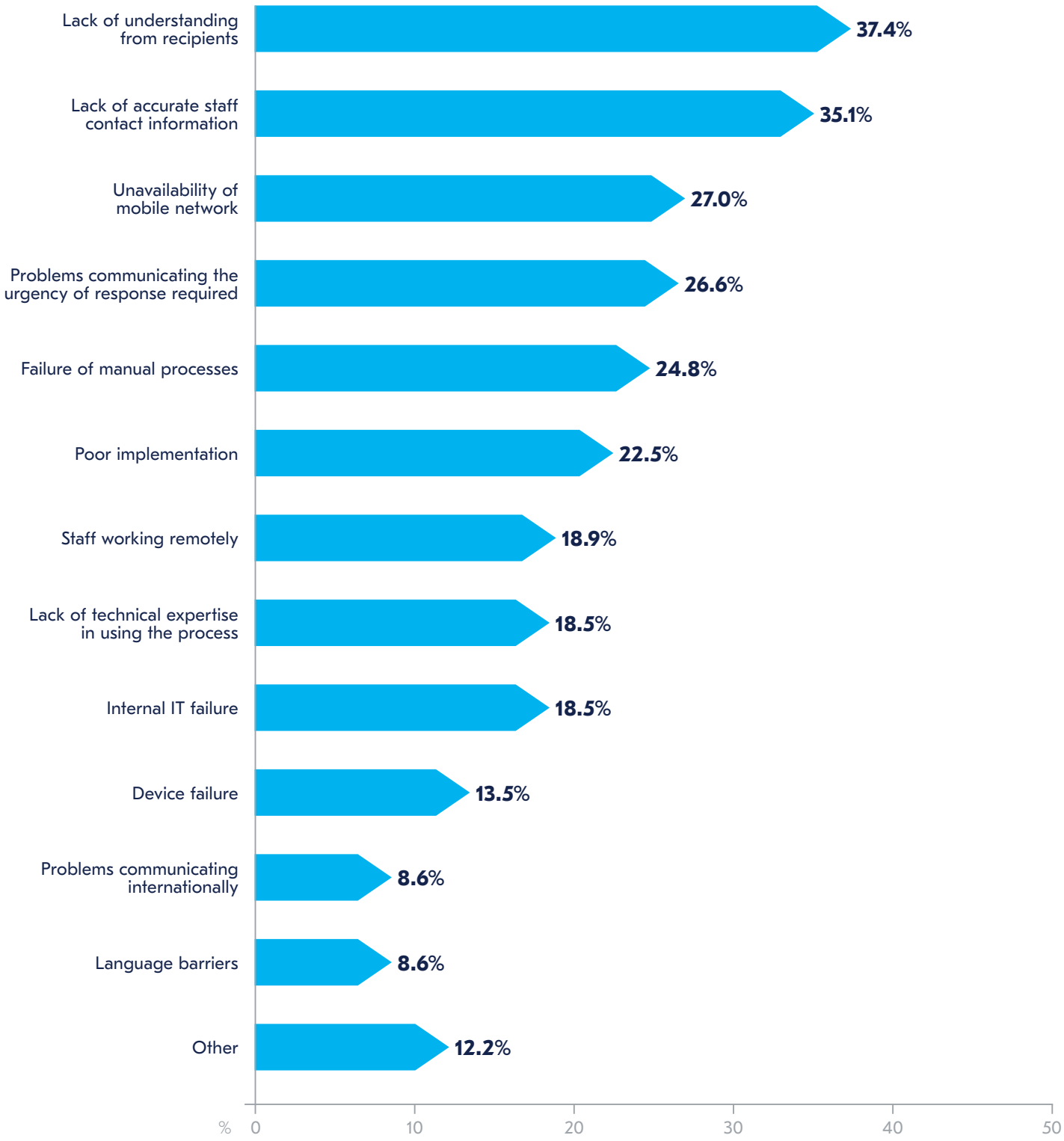


Figure 14. If you failed to achieve your accepted response levels, what caused the failure?

Section three:
Key challenges

Section three: Key challenges

- **Information, information, information – the biggest challenge to communicating outwards in a crisis is the quality and quantity of information coming inward.**

- **Effective communication with staff – and ensuring that they follow planned procedures – are also vital.**

Crises and emergencies are, by definition, challenging situations. But what aspects of the management of crises and the communication undertaken to manage them do practitioners find most challenging? The survey offered respondents a list of ten named challenges and an 'other' option, with space for a narrative response, and asked them to choose the three that they found most difficult. While responses were, unsurprisingly, spread widely among the 11 choices, there was a clear, if not overwhelming, winner: 'gathering, validating and sharing accurate information' received most first-place votes (27.9%), most second-place votes (23.6%), and most votes overall (22.0%). This choice is at the top every year and is arguably becoming a bigger challenge year-on-year as information sources become more plentiful and data becomes richer. Senior management are becoming increasingly demanding about the information they wish to receive about an incident, and the wealth of information sources available now makes the information gathering, corroboration of information and reporting of information a more complex process. The difficulty of sharing accurate information can also be down to problems communicating with the *right* people which, as discussed in the previous section, requires correct contact information to be used.

To back this up further, 'communicating with staff' finished just behind in terms of first-place votes (25.7%) and had more first-place votes than second and third choices combined. An interviewee explained how having large numbers of staff working in manufacturing facilities often caused delays in messages getting through as mobile phones were not prohibited on factory floors. Such situations are ones where onsite display messages would serve a very real purpose.

In terms of total votes, the second most significant challenge (18.0%) was to keep an overview of the current situation or status — this was more common as a second or third choice than as a first, as would befit an 'observational' task rather than an action. A similar pattern was followed by the fourth most popular choice, getting staff to follow planned procedures, with 11.7% of the total votes, but most commonly a second choice.

An interviewee spoke about how in his sector — and in many other large organizations — it was difficult to get staff to follow planned procedures and communicating with staff was an issue. In his experience, even with staff receiving the correct training and exercising, getting them to react and follow procedures during a real activation was difficult.

"It very hard within Civil Service to get people to follow any form of planned procedure, whether it's a fire drill or a lockdown drill. Even if you're doing a shooter scenario or a random knife attacker, whatever it might be even an intruder in the building scenario, they just don't follow instructions and they don't follow alarms. It isn't just for me, it's been a huge problem for Incident Management professionals and safety professionals across the Civil Service, and this is that people just don't take it seriously. People get fixated on their role and fixated on their job, they just assume an actual activation is a drill, and just don't follow plans. I've seen it time and time again. Even when you drill and you get messages out to people and you do tabletop exercises, it is still very, very hard to get that out there."

Safety Manager, Government, United Kingdom

The specified challenge found least significant by respondents during emergency notification and crisis management was communicating with staff members' next of kin, selected by just 1.9% of respondents and receiving just 0.7% of first-place votes. It is likely — and very much hoped — that this reflects an absence of incidents in which such communication is necessary, given that doctors, police officers and others in similar vocations anecdotally suggest that it is one of the more difficult aspects of their job.

Other less popular responses included communicating with remote workers, considered a top-three problem by just 3.2%, and locating staff (4.5%) - suggesting that the patchwork of communications solutions described earlier in this report are effective and reliable enough to meet practitioners' needs. This last point was reflected in the narrative additions made to responses to this question, with several stating that the tools at their disposal ensured that the situations presented, or at least some of those previously considered problematic, were now generally not so.

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

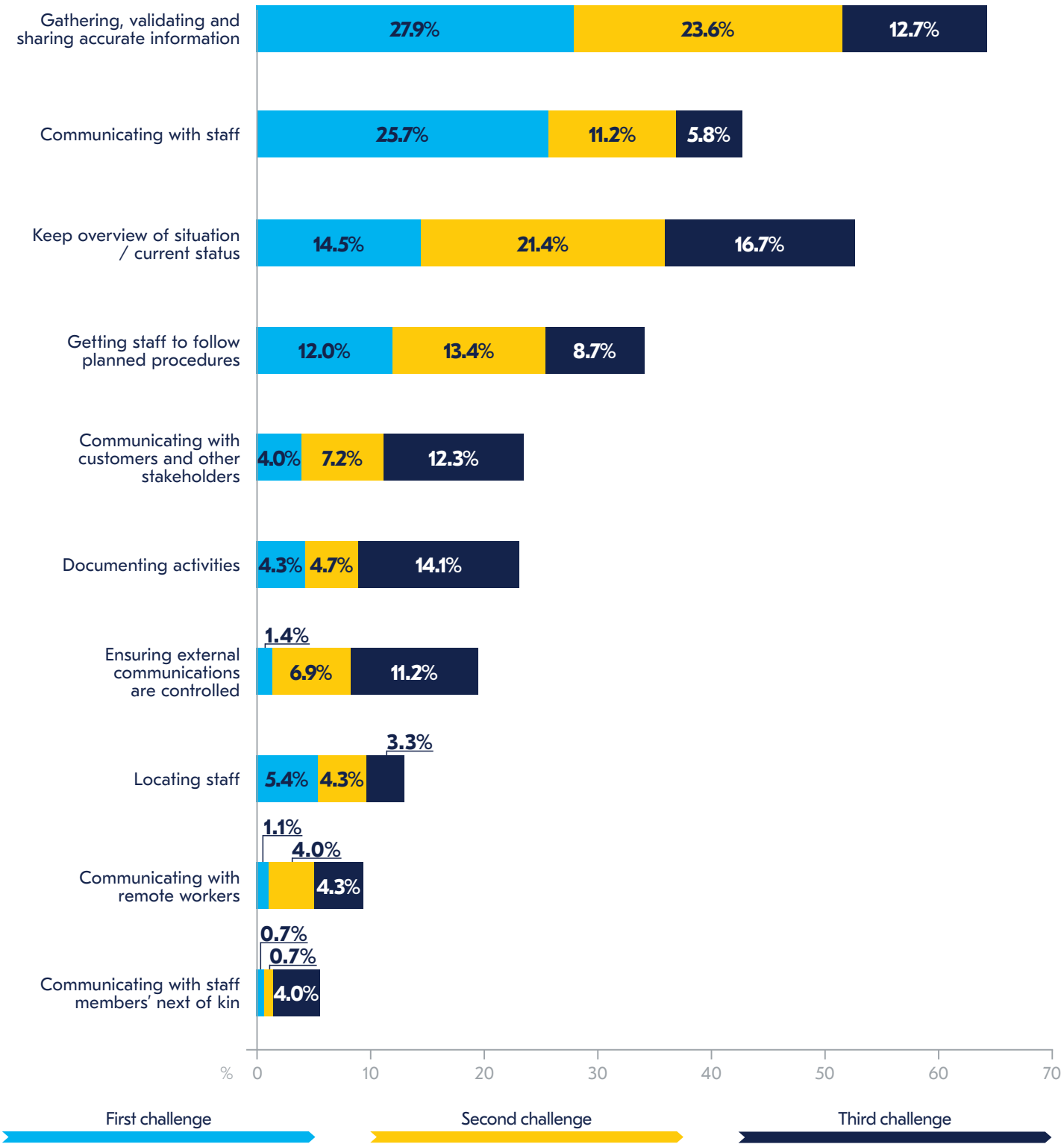


Figure 15. What are your key challenges during emergency notification/crisis management?

Section four:
Tool requirements

Section four: Tool requirements

- **Software and other packages designed to facilitate emergency communications must allow for a constant exchange of information to enable decision making and allow teams to collaborate in real time.**
- **The pandemic – and, to an extent, other events of the last two years - has changed a small majority of respondents' views on the requirements of their support tools, with the collaboration aspect now more important, in a world of increased remote working.**
- **Better integration with organizations' alerting scenarios is an area where respondents believe improvements can be made to support software**

After discovering what respondents said their emergency communications tool did for them, the next batch of questions sought to discover what features they required in the design of an emergency communications tool, and how that design may be improved. The first question in this section offered 11 features and asked the audience to rate on a five-point scale, from 'critical importance' to 'of no importance'; how significant each of them is in their organization's alerting and emergency communications.

This question again reinforced the idea seen throughout this survey — in any incident, information is key. The most popular answer at any rank was 'constant exchange of information to enable decision making', chosen at 'critical importance' by 46.0% of respondents — it received more ratings of critical importance than the total number of ratings of 'no importance' given. In all, 93.8% considered this to be of 'critical importance', 'very important', or 'important', and only 6.2% thought it 'not very important' or 'of no importance'. As demonstrated by the rising popularity of choosing a tool which allows collaboration during a crisis and the growing unpopularity of one-way communication, collaboration during an emergency remains crucial to ensuring a co-ordinated, multidepartmental response as well as ensuring the right people can be kept informed during a crisis which can include external stakeholders such as emergency services, the media or local government.

The second most important aspect of a tool also demonstrates the importance of collaboration: 'enabling expert teams to collaborate easily and in real time' saw 3.9% of respondents rate it as 'critical' with 94.9% of respondents considered 'important' or more so. One-way mass communication clearly still has a defined place in a crisis, finishing as third most desired aspect of an emergency communications tool.

The mid-range results to this question also proved interesting. The feature with the lowest percentage believing it to be of 'critical importance' was integration with other technology used by the organization, with 12.6%.

This answer, although rating similar to the previous year, still comes as somewhat of a surprise. Interviewees said that one of the major barriers for introducing a new tool or application was down to the difficulty of integration within their existing technology infrastructure. Nevertheless, it is clearly still required by most: just 4.7% said such a feature was of 'no importance'. The feature considered 'of no importance' by the greatest number of respondents (10.4%) was superior geographic coverage, probably reflecting the fact that most businesses do their work in relatively straightforward locations in terms of connectivity and communications, or have already prioritised good geographical coverage in geographies with known connectivity issues.

"Some of our divisions have got such old software, like really old Windows versions. Some of our field staff still have fairly old laptops. We can't afford to replace them all right now, but unfortunately this means we're also having problems implementing our new communications tool. I think we're going to be getting new laptops this year for the affected staff, but until then, I'm a little nervous."

Director of Risk & Resilience,
Pharmaceuticals, United States

In terms of respondents' assessment and distribution of importance levels, they classed an average of 2.9 features as of 'critical importance', 3.3 as 'very important', 2.8 as 'important', 1.2 as 'not very important', and 0.4 as 'of no importance'. All the specified features received votes at all five levels, underlining the impression that the needs of different organizations vary substantially, even in crisis situations.

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

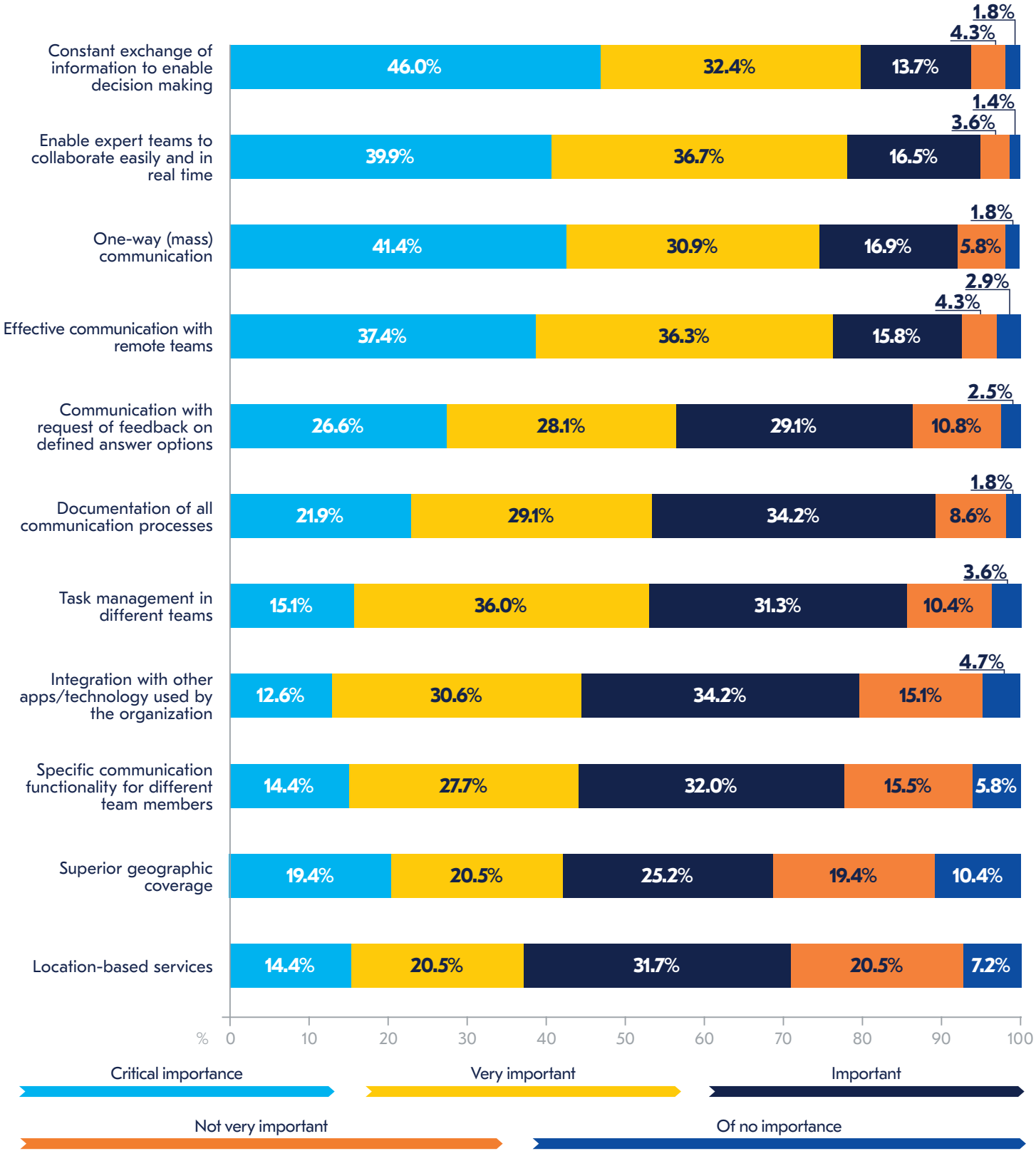


Figure 16. How important are the following aspects for your alerting and emergency communications?

Given how much the working world has changed over the past two years both in terms of virtual and physical environments, it might be expected that professionals' demands of a tool have changed since the beginning of 2020.

On the basic binary question, respondents were fairly evenly split — 52.3% had changed their view, and 47.7% had not. Examining the more detailed responses, there is a clear view that the shift to remote working that resulted from the COVID-19 pandemic has required a concomitant shift in organizational communications strategy. Some who had specialist support tools in place before the rapid changes of the first half of 2020 have found that their system copes well with the 'new normal', while others have appreciated the need for a fundamental redesign of their approach to crisis communications now that the old model of office-based work is temporarily gone and perhaps permanently threatened.

Some of the major themes to emerge from this question were as follows:

- **Microsoft Teams and Zoom have changed how workplaces function:** There were comments that the two popular enterprise platforms have greatly improved communications within offices over the past two years which has led to better collaboration overall during crises.
- **Integration and consolidation of existing tools:** Despite the previous question showing that very few respondents feel integration with other technologies used within the organization was critical, there is a clear demand for tools and technologies to work with existing platforms within the organization, or even try and consolidate better emergency communications offerings within existing business continuity software packages.
- **The requirement for instant, real time communications:** Respondees expressed how the importance of real time communication had come to the fore during the pandemic and were seeing better communications happening between the strategic/tactical teams and the operational teams during a crisis. They felt that new technologies were helping to facilitate this happening.
- **Moving away from a reliance on SMS/email:** Up until the pandemic, this report showed how many organizations were still relying on mass SMS alerts — or even email — to communicate during an incident. The pandemic has demonstrated the importance of using more reliable forms of communications which many respondents said had already been invested in.

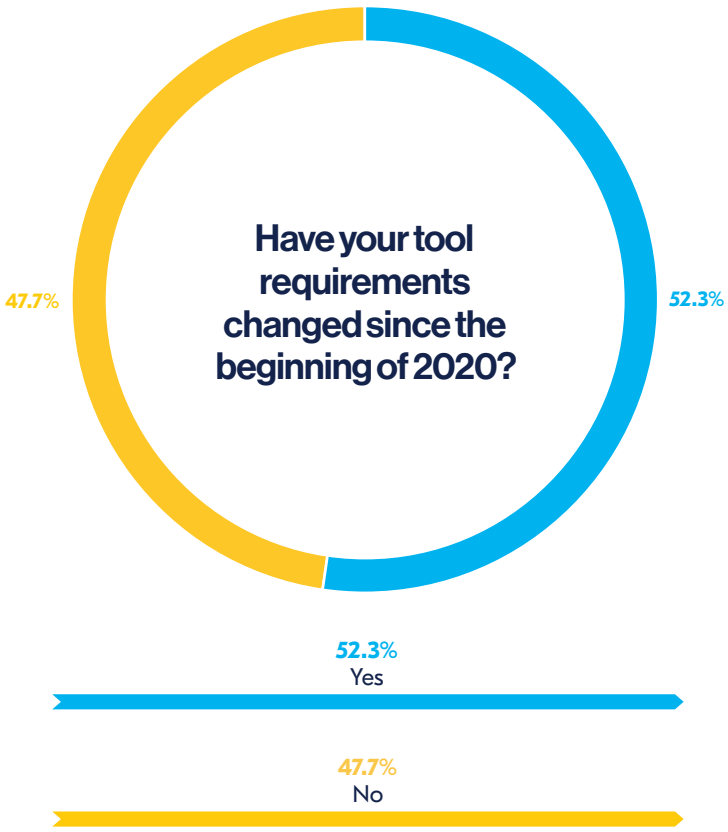
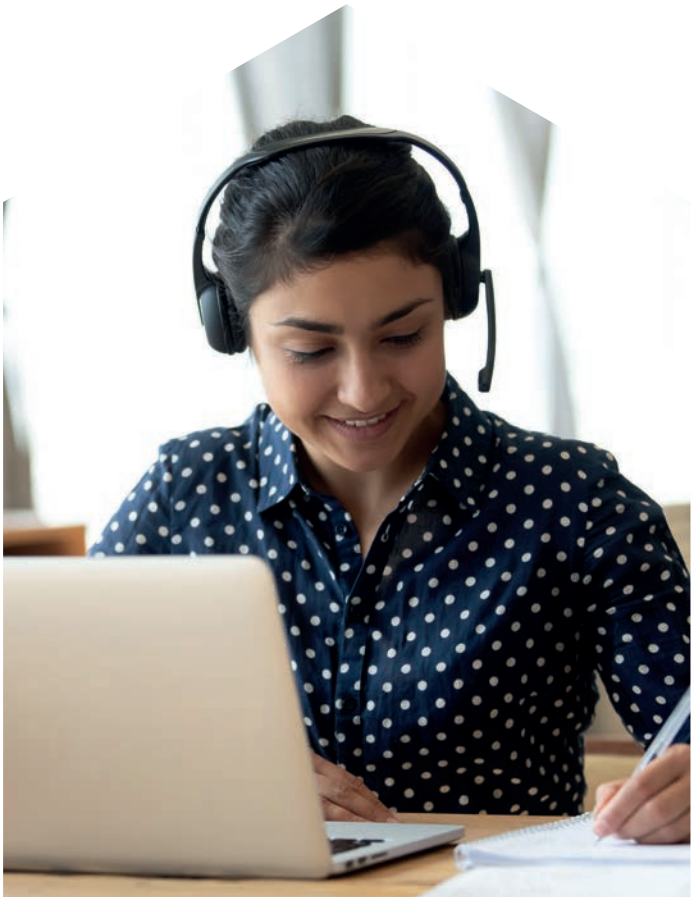


Figure 17. Have your tool requirements changed since the beginning of 2020?



The last question in this group focused on those who described themselves earlier in the survey as either not happy or only somewhat happy with their current emergency communications solution. Given seven specific options and an 'other' to choose from, each respondent offered an average of 1.9 choices. This was less than the more common average for multiple response questions in this survey, of between 2.7 and 2.9, suggesting that the reasons for dissatisfaction with a solution tend to be rather narrower and particular to each organization.

Despite this rather lower number of choices given by the average respondent, the spread of options selected remained relatively wide. The least popular responses were still ticked by more than 15% of the field, and only one option exceeded the 30% mark. This was the impression that the solution did not offer sufficient integration with the organization's alerting scenarios, selected by 52.3% of those who answered the question — a clear indicator to providers that this is an area in which improvements can be made. The answer also led the responses in last year's survey, although the gap has widened further this year between the first and second choices.

Interestingly, the number of respondents who said that their current app lacks the functionality they require dropped to 29.8% this year — exactly ten percentage points lower than last year's survey. This suggests that organizations are now happier with their emergency communications solutions than they were a year ago, either purchasing new solutions or fully realising the capabilities of their existing technologies.

Legacy systems continue to provide a barrier for 17.9% of respondents, which echoes the previous question where there is clear demand for solutions to integrate with existing solutions. A lowly rated barrier was that of language problems. Whilst this might not a problem for many organizations who operate in a single geography or multiple geographies where one language is understood by all. However, for some organizations, language does remain a problem with an emergency response.

"We have a global workforce so language is important. We have some positions such as drivers or cleaners where English is not a requirement. And, from time to time, our crisis messages go out only in English. Because of this, we now we try to have a message in different languages because if we are in crisis mode, we need to communicate it to all the staff, and all the staff need to be able to understand, right from the bottom to the top level."

Crisis Manager, Humanitarian Organization, Switzerland

Once again, this question offered space for respondents to make comments, in addition to the tick-boxes that formed the main part of the question. Several themes emerged in these comments — particularly notable was the idea that technology in the field advanced so quickly that by the time a change had been implemented, a new solution with substantive improvements was available. Some organizations have concerns over the cyber security or data protection implications of their current tools, while others found that providers of solutions did not release updates regularly, and there was a lack of consistency of tools used across the organization. Some also flagged the problem that different blue light services (e.g. fire, police, ambulance) all used different emergency communication systems which could, in extreme circumstances, lead to fatalities.

Reasons cited for being either "somewhat happy" or "not happy" with current emergency communications tool

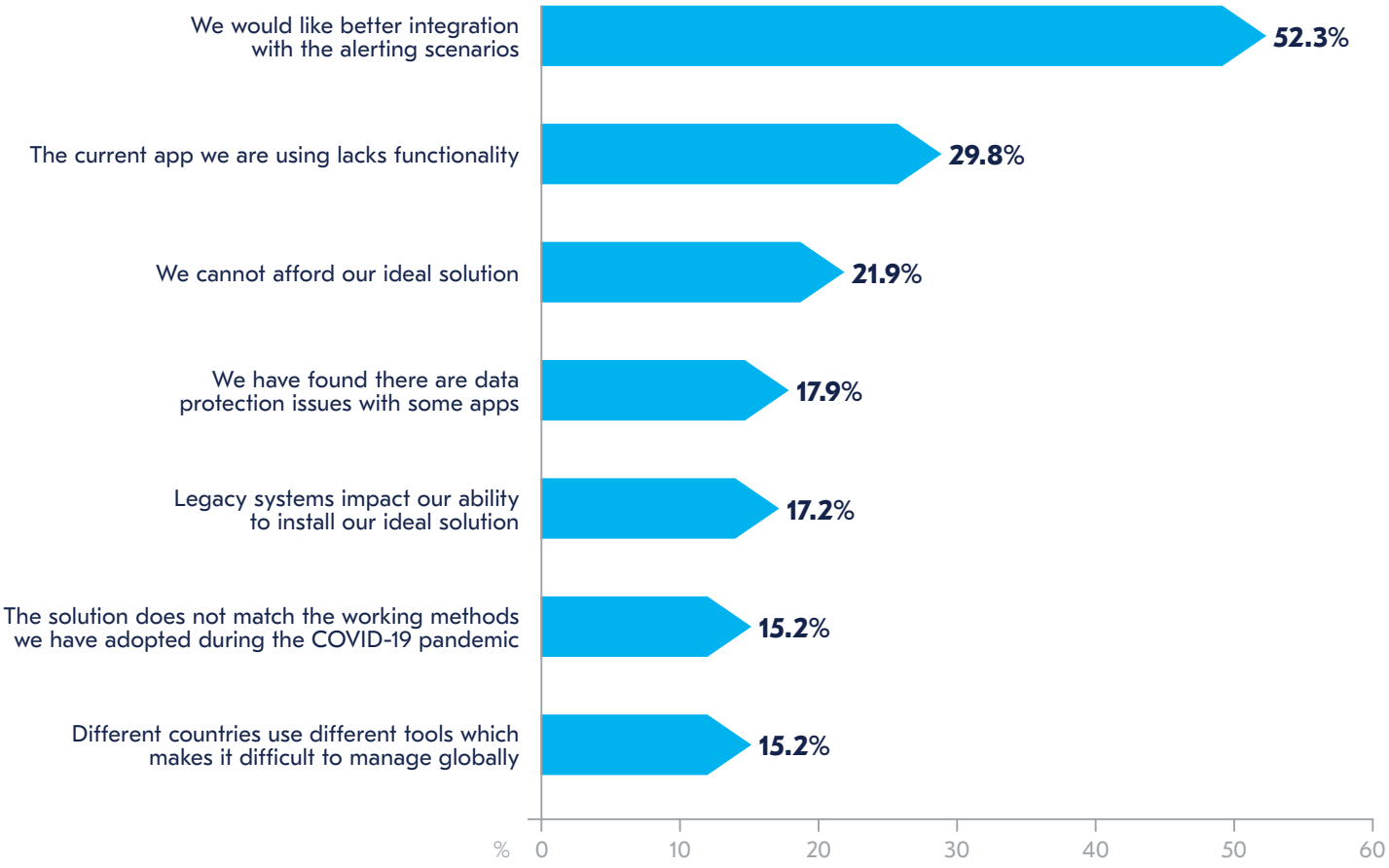


Figure 18. Reasons cited for being either "somewhat happy" or "not happy" with current emergency communications tool

Section five: Training and exercising

Section five: Training and exercising

- **An annual schedule remains the standard both for exercising crisis communications plans and for training initiatives.**
- **Few organisations invoke their emergency communications plan more than five times in a given year.**

The importance of training and testing all aspects of crisis management is a long-established principle of the discipline, and this section seeks to discover how organizations applied this to crisis communications. 2020 and 2021 were difficult years for most organizations and with many organizations having all or some staff working remotely, training sessions were not carried out with the regularity that they had been pre-pandemic.

This year, the results are similar to those in last year's survey: 73.9% of organizations carried out training at least once a year compared to 73.1% in the previous year. The biggest group (42.9%) organised training programmes for their emergency communications plans every 12 months. The next group, less then half as numerous (19.5%), did so every six months while 11.5% run training at least every three months. Respondees in this group highlighted how frequency of training was often driven by the regulator, or the adoption of new systems during COVID-19. Training is carried out on an ad hoc basis — be that because of a new system, or a concentration of new staff, or other motives — in 12.3% of organizations. Just 9.6% fail to offer training on at least a yearly basis, while 4.2% never see training programmes in crisis communications.

As was highlighted in the previous year's report, many organizations admitted to carrying out less training and exercising in 2020-2021 as a result of so many real-life activations. Most organizations reviewed each of the activations, with feedback given to staff and changes to processes made which were incorporated into future training sessions.

"One thing is, we've had lots of practice at managing emergencies/incidents. In the last four years with these various different crises/ pandemic/emergency incidents, people know the situation. However, three, four years ago they probably didn't. So we've got muscle memory in this. We also do practices and we do training for our staff, so people know that communications are not some sort of fraudulent email they're receiving. You can click on this, you can do this. And people get to know it. And we've also included it within our people program and our cultural behavioural aspects for people to know that this is important to the organization and they have a role to play."

Global Security Director

11.5%
Every three months or more frequently

19.5%
Every 6 months

42.9%
Every 12 months

9.6%
Less frequently than every 12 months

12.3%
We carry out training ad hoc

4.2%
Never

Figure 19. How often do you set up training programmes for your emergency or crisis communications plans?

The next question asked how frequently emergency or crisis communications plans were exercised. This year has shown a fall in the amount of exercising taking place, with 78.6% of organizations exercising plans at least once per year (2021: 82.3%). Annually was by far the most popular response, with a similar proportion of respondents (41.8%) to the earlier question on training. Just less than a fifth (18.0%) exercised their plan twice a year, and just over an eighth (13.0%) did so quarterly. 5.8% of organizations carried out exercising at least every month. One in twenty respondents said their plans were never exercised, while 5.8% said that exercises only took place following an incident. Failing to exercise plans can lead to failure: problems will not be identified, and people will not know how their role interplays with others during an event. Indeed, the BCI's Good Practice Guidelines 2018 highlight how exercising should be an ongoing part of an organization's Business Continuity Strategy:

> **"Exercising is not a one-time activity. It should be scheduled and programmed into a series of events and activities that allow the organization to gradually improve capability over time."**
> Good Practice Guidelines, BCI, page 88

Whilst staff training can take place within remote environments, it can be more difficult to exercise plans — particularly if they are built around a physical office environment. This should not necessarily be an excuse however, as exercising emergency communications plans for remote staff is of great importance — particularly when remote work is a new concept to many. An interviewee commented that when they had requested that an exercise should take place to senior management, they were told it was unnecessary due to the current working environment.

> **" When I flagged to the COO that we needed to get some training in with staff all in different environments they said 'no, you don't need to do that. Everyone is busy at the moment and is in a temporary situation which will change soon. Do the training when everyone's back'. This was very frustrating for me; it meant our response to the floods was not as good as it should have been."**
> Crisis Management Lead, Mining, Germany

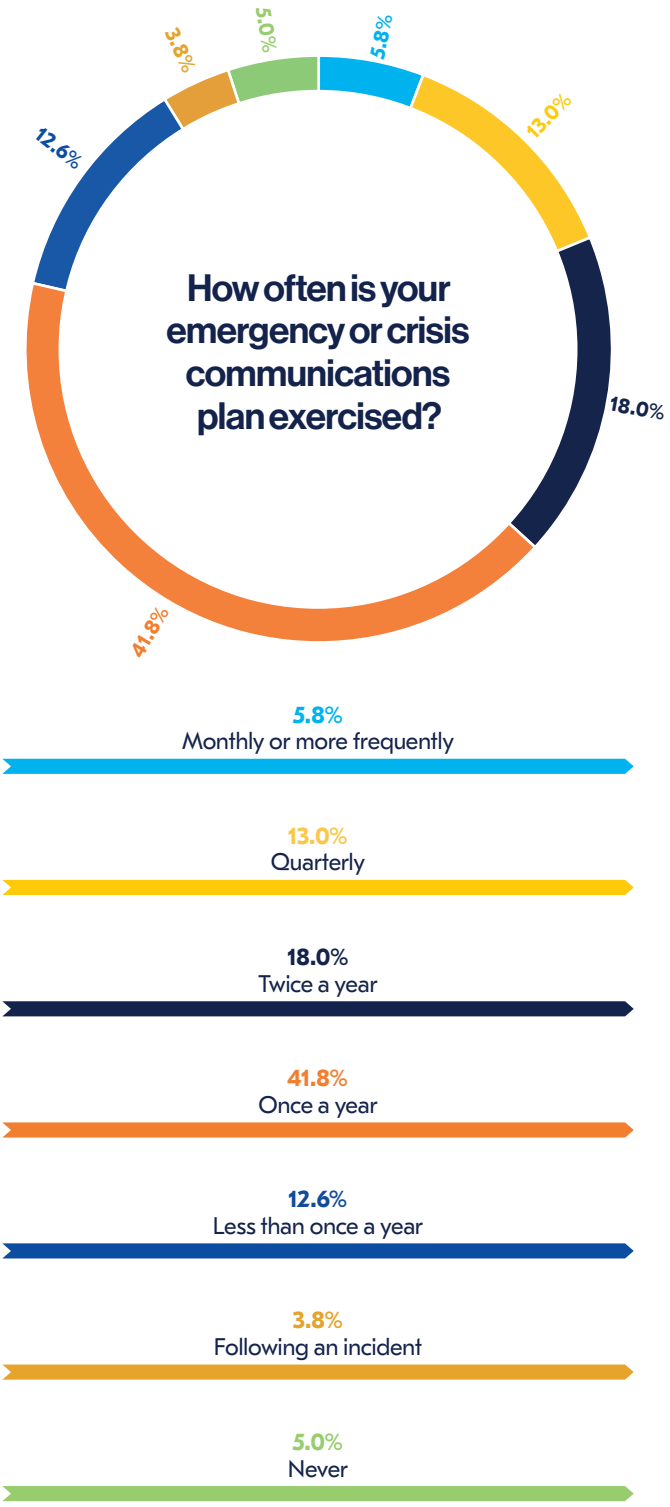
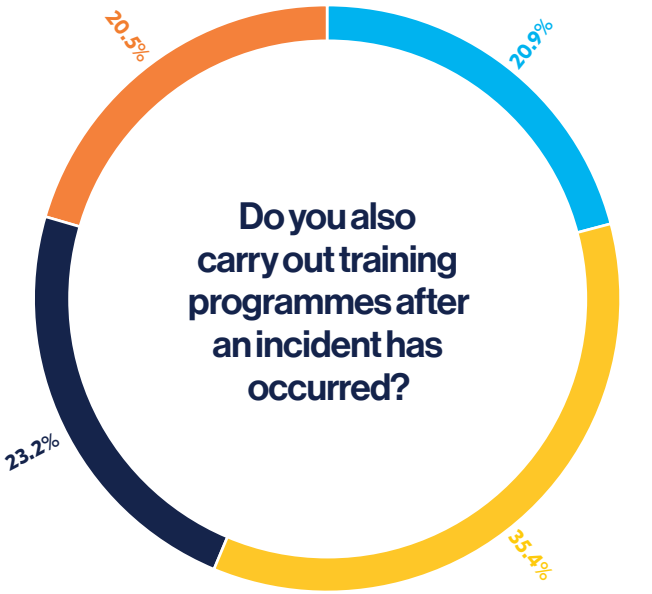


Figure 20. How often is your emergency or crisis communications plan exercised?

Another common principle in security, business continuity and crisis management and other resilience disciplines, is learning from incidents, and training personnel appropriately. Our survey discovered that 20.9% of organizations always carry out training programmes after an incident, while 35.4% say they do so sometimes, and 23.2% say that they do, but rarely. Post-incident training is not a feature in 20.5% of organizations.



20.9%
Yes, always

35.4%
Yes, sometimes

23.2%
Yes, but rarely

20.5%
No

Figure 21. Do you also carry out training programmes after an incident has occurred?

No crisis communications plan is complete without exercises to test its resilience and effectiveness. While these efforts should seek to recreate live situations as closely as practical and possible, there are always elements of live incidents, or other non-test scenarios, that highlight aspects of the plan that tests do not. The survey asked respondents how many times their emergency or crisis communications plan had been initiated in the previous year. Just over one-fifth (20.7%) of respondents said it had not been invoked at all which is likely to be positive for the organization and represents a near four percentage point increase in the previous year. However, the increase in the number of non-activations further highlights the importance of ensuring regular testing and training takes place.

The most common answer, however, was between one and five times, which accounted for nearly two-thirds (62.5%) of respondents — the same proportion as the previous year. Last year, we noticed a decrease in the number of organizations that had activated their systems multiple times, with 7.8% of organizations reporting they had activated their plans 11 times or more. This reflected many organizations moving to virtual environments and there was less of a need to invoke plans when few — if any — staff were on site. With staff now returning to offices, the number activating their plans 11 times or more has increased to 10.8%, and we would expect to see this increase further in 2022 as some organizations move back to non-remote models.

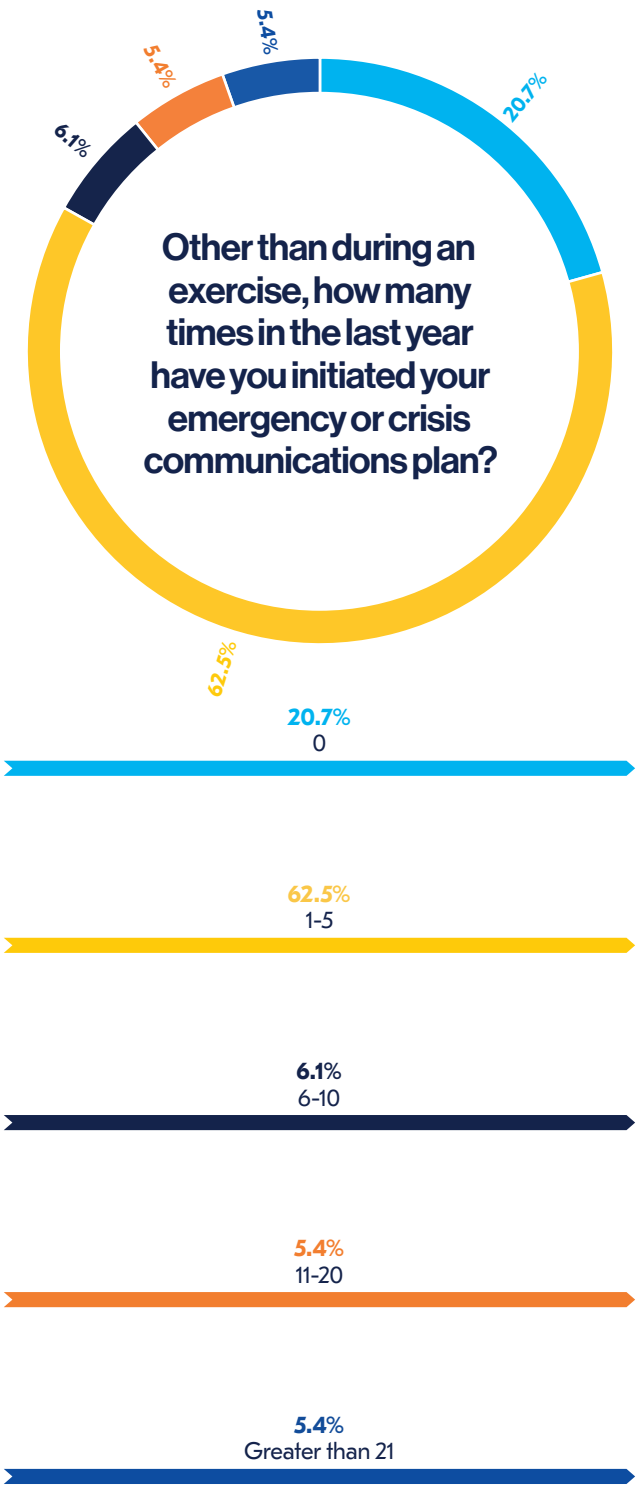


Figure 22. Other than during an exercise, how many times in the last year have you initiated your emergency or crisis communications plan?

The next question asked what types of incident had caused organizations' emergency or crisis communication plan to be triggered in the previous year. Last year's report, perhaps unsurprisingly, had *disease outbreak* as the most common reason for activation. This year however, we have noted a fall in the number of respondents citing this as a reason for activation. Although still a top answer, disease outbreak — most likely COVID-19 — was the cause of less than half of activations (42.0%) and actually tied for first place with an IT or telecoms incident, very much reflecting the reality of the working environment over decades.

Adverse weather caused plans to be triggered in 40.8% of respondents' organizations, and with extreme weather events becoming more common[9], this is likely to increase in years to come. Some respondents commented that adverse weather had caused less of an effect in 2021 than it had in previous years, purely because staff were located away from offices and additional homeworker resilience had been added over the course of the year. This will be an aspect which will need to be considered over the medium term, particularly as recent BCI research has revealed that adverse weather is still primarily dealt with as an acute, rather than chronic, risk.

We commented in last year's report about the rise of cyber security incidents, many of which had stemmed from organizations having staff working remotely who were using systems which were not fully protected, or users themselves were more at risk of social engineering. Last year, the number of initiations for cyber security incidents rose to 24.7% from 19.1% in 2020. This year, the figure has risen to 32.2% which is symptomatic of the rise in cyber-crime which is currently being reported: the World Economic Forum's *Global Cybersecurity Outlook 2022*[10] showed that ransomware attacks rose by 151% year-on-year in 2021, whilst organizations were targeted on average 270 times in 2021 — an increase of 31% on 2020.

Among the options lower down the list, critical infrastructure was a trigger for 15.1% of plan enactments, workplace violence for 11.8% respondents, supply chain disruption for 9.4%, and geopolitical change for 8.2%. Additional information supplied by respondents who ticked the 'other' option gave a picture of how COVID-19 related difficulties had caused plans to be triggered — one organization was forced to trigger their plan by the differences between the regulations applied in the various sub-national divisions of their main country of operation, while another triggered as a response to several infected personnel. One organization applied its plan as a client requirement, most likely reflecting the increasing trend in the corporate world for companies to demand that key elements in their supply chains comply with their standards in areas such as cybersecurity and crisis response[11].

9. Sreenivasan, H., Tebaldi, C. (2021) Climate Change is Making Extreme Weather Events More Common [Online]. Available at: https://www.pbs.org/newshour/show/climate-change-is-making-extreme-weather-events-more-common-study (accessed: 30 January 2022)
9. Pipikaite, A. et al (2022) Global Cybersecurity Outlook 2022. World Economic Forum [Online]. Available at: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (accessed: 15 February 2022)
9. Receiprocity (2021) What Is Supply Chain Compliance? [Online]. Available at: https://reciprocity.com/what-is-supply-chain-compliance/ (accessed: 30 January 2022)

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

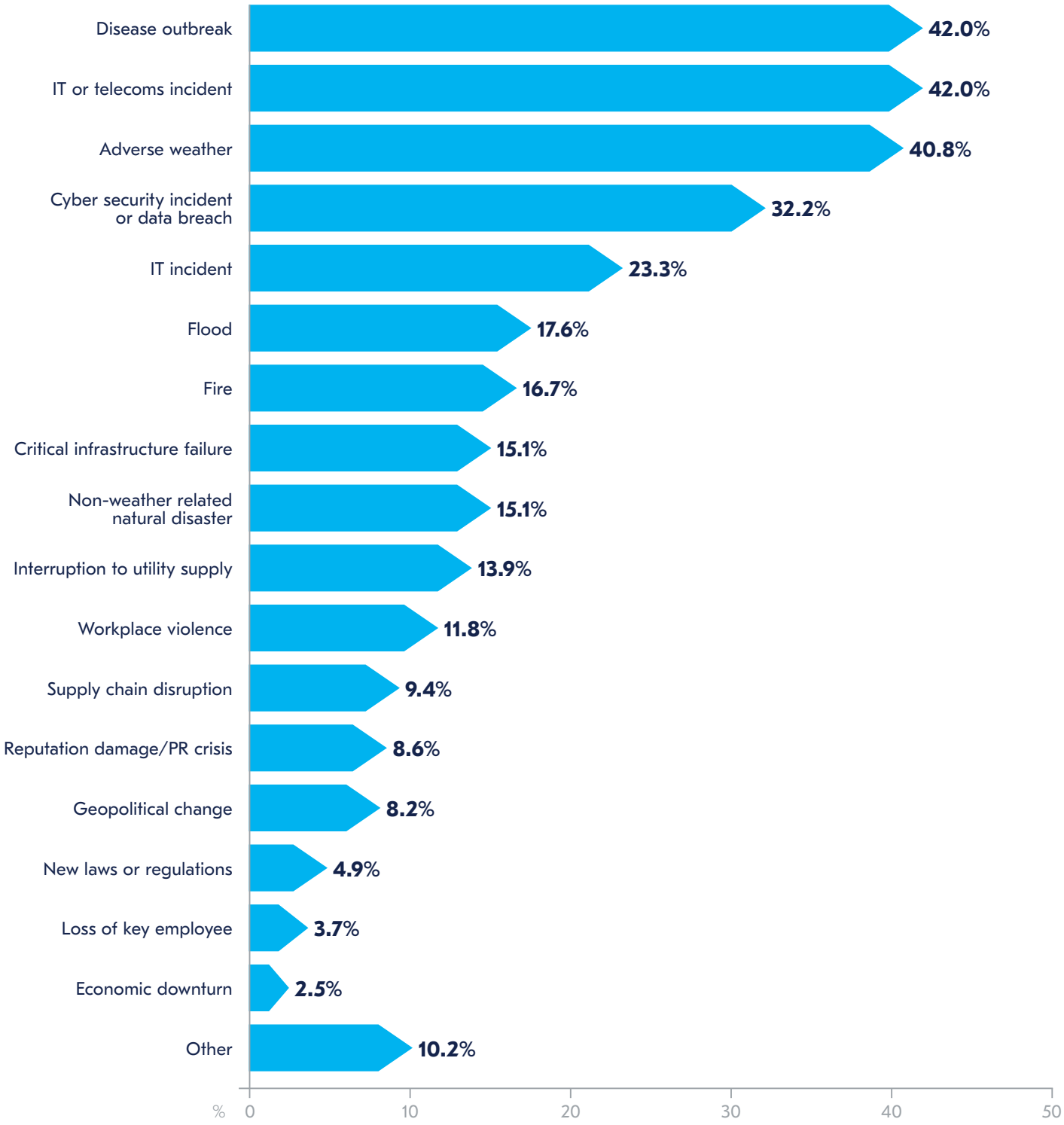


Figure 23. Which of the following triggered your emergency or crisis communications plan in the past twelve months?

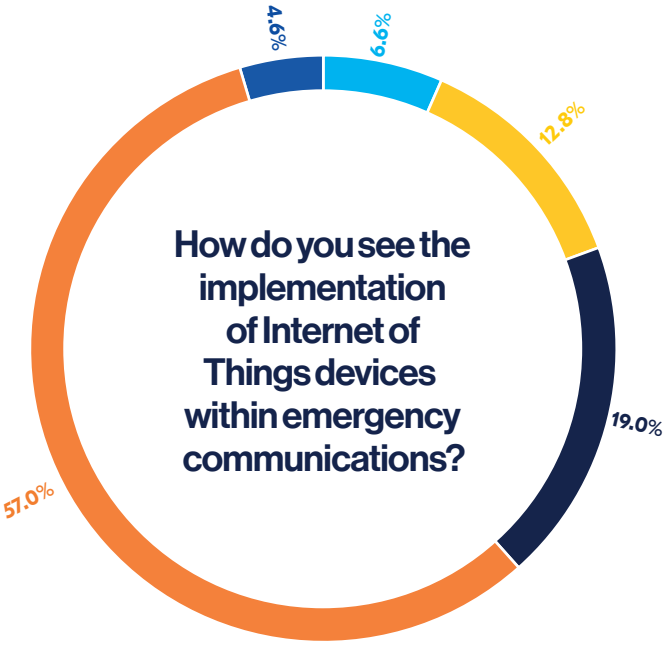
Section six:
The Internet of Things (IoT)

Section six: The Internet of Things (IoT)

- **More than half or respondents say that there are no plans for the integration of IoT devices into their communications plan.**
- **There is significant mistrust of the reliability of IoT devices in many crisis situations.**

While the Internet of Things (IoT) came to prominence several years ago, its use in business continuity and crisis management is still in its infancy. The survey asked how practitioners saw IoT devices contributing to the emergency communication effort, giving the example of fire sensors sending out alerts.

The general impression from the survey is that while the use of IoT in communications or in crisis response more widely is gaining adherents, this is an idea whose time has not yet come, with 57.0% of respondents stating that they were not planning to embed IoT devices into their emergency communications. Only 6.6% of organizations had IoT outputs well embedded in their strategy, while 12.8% made limited use of these devices. A further 19.0% were planning to introduce IoT devices in the future. The additional responses given by the 4.6% of respondents who ticked the 'other' response suggest that some are concerned that the technology is insufficiently advanced, and that its reliability may be questionable in a crisis. It is somewhat inevitable that the industry will embrace IoT when offerings are tried and tested and offer a quantifiable advantage over existing methods but, for now, levels of adoption are remaining broadly the same, year-on-year.



6.6%
IoT devices are well embedded in our emergency communications plan

12.8%
We use IoT devices into limited areas of our plan

19.0%
We are planning to embed IoT devices into our emergency communications plan

57.0%
We are not planning to embed IoT devices into our emergency communications plan

4.6%
Other

Figure 24. How do you see the implementation of Internet of Things devices within emergency communications?

Section seven: Information and data acquisition

Section seven: Information and data acquisition

- **A broad range of information sources is vital if an emergency communications plan is to be effective, proactive and reactive.**
- **Automated alerts such as weather alarms or messaging from travel security providers are an increasing part of the information mix, but still only used by just over half of respondents.**
- **Keeping staff contact details up to date remains a key challenge, and multiple means are required to ensure that lists are correctly updated and maintained and crisis communications are directed accurately.**

The importance of obtaining reliable, fully corroborated information in a timely manager is critical to the success of an emergency communications plan. If information is passed to management that has not been corroborated or verified, it could lead to plans being activated incorrectly which could not only lead to financial loss, but also to lack of trust from staff which is likely to lead to future activation not being taken seriously. Sourcing information from a broad range of sources is key to gather a true picture of an unfolding situation. However, the job of the resilience professional is to balance the need for quick information transmission with the validity of the information which has been collected. This is something that training and exercising can help to accomplish.

Respondents were questioned how their organizations ensured the acquisition of timely and reliable information in a crisis. The first thing to note is the breadth of responses — each respondent chose on average 6.7 of the 18 options offered, illustrating the necessity for a diverse range of information sources in the contemporary business environment. More than two-thirds of respondents (67.6%) highlighted the importance of ensuring that employees' contact details are up to date, a problem which has surfaced at multiple points in this survey. Beyond this, respondents primarily made use of key open-source information, with weather alerts (54.0%), government and other official web sites (52.4%) and official social media accounts (47.6%) all being among the most common answers.

Collaboration with emergency services is also seen as important, with 48.0% of respondents making use of such links. Other collaborations to prove useful in information-gathering were those with local authorities (45.2%), industry peers (36.4%) and other local organizations (34.8%). The importance of good community resilience has been highlighted as being a successful driver in realising a good response. The importance of resilient communities is becoming a driving force within countries around the world. In the United Kingdom, a paper was launched in September 2021 around the development of a new national resilience strategy[12], whilst the Federal Mission Resilience Strategy was launched in the United States in December 2020 which encourages a more cohesive approach to national resilience[13]. All the specific options were relatively popular, however, with even the least ticked being offered by 22.0% of respondents.

12. Local Government Association (2021) National resilience strategy call for evidence Local Government Association response [online]. Available at https://www.local.gov.uk/parliament/briefings-and-responses/national-resilience-strategy-call-evidence-local-government (Accessed: 15 February 2022)
13. Center for Homeland Defense and Security (2020). Federal Mission Resilience Strategy [online]. Available at https://www.hsdl.org/?abstract&did=848323 (Accessed: 15 February 2022)

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

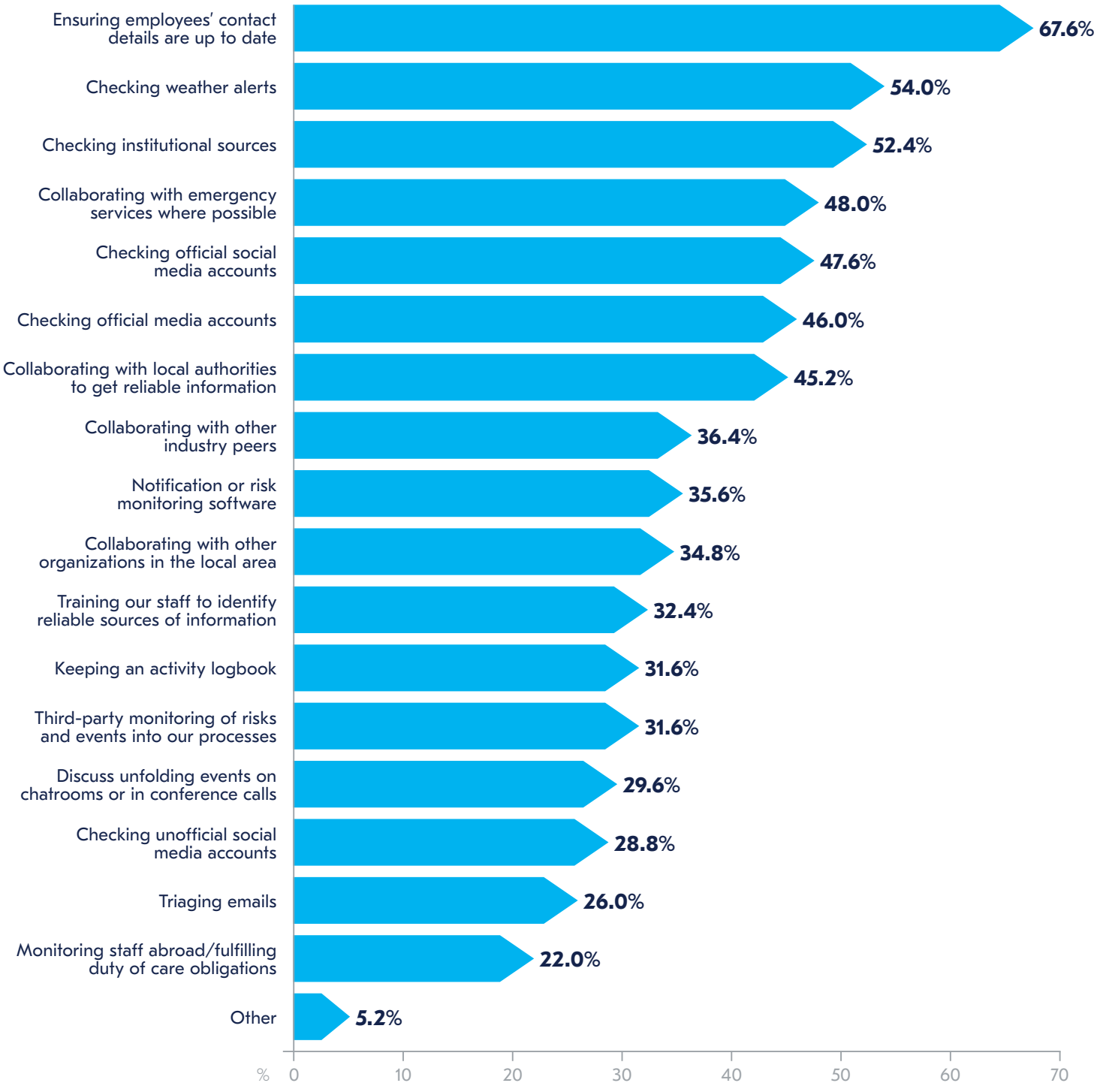


Figure 25. How do you ensure the acquisition of timely and reliable information when it comes to an incident or crisis situation?

Automation of tasks that consume staff time is a never-ending quest in the modern business environment, and it is no different for those in charge of crisis communications. The survey asked if respondents had any automated alert systems in place. Just over half the respondents (54.4%) had some form of automated alert: monitoring of weather and of social media appear to be the most common from the narrative responses, while feeds from emergency services, as well as travel security and other specialist providers are used by a smaller, but still significant number. Organizations are still understandably wary of using automation for tasks, particularly during an emergency, as most business continuity managers and senior management do not feel comfortable invoking emergency plans based purely on automated information. There are some, however, who would welcome such automation to start to take effect — as soon as the market is ready for it.

"I think from the very start is taking the human element out of how the tools are administered. I would love to see some automation a little bit more enabled on the communications tooling, but we still have some human interaction that has to happen there. But other than that, it really is about people embracing the technology or even the change in technology. As an example, when our plans were deployed using [our emergency communications tool], we were heavily using the conferencing feature but now technology has progressed and we're using teams, the conferencing feature usage has gone down dramatically. I mean, I can't think of the last time I was on a conference call. Conference bridging has now moreorless disappeared."

Global Director Business Continuity & Resilience

Respondents were also asked how they ensure that contact details of employees and other contractual staff is kept up to date. Rather disappointingly, it appears that no real progress has been made in this area over the course of 2021. 41.6% of respondents report that their own system interfaces with HR systems allowing for automatic updates. Although this is the top answer, it is down on the 49.0% recorded in the previous year, and it would be encouraging to see the previously reported siloes between business continuity and HR broken down to enable this to happen. In a marginal second place was communication with HR allowing for detail-sharing (41.2%) which is again down on last year's figure of 48.3%. Of some concern is 40.8% still ensure details of employees are kept up to date by the maintenance of manual lists, often using Excel. This represents an increase of three percentage points on 2021 and still demonstrates that spreadsheets remain the incumbent practice for contact data storage in many organizations. Storing contact information on spreadsheets can not only lead to data protection issues, but version control of such documents is also key to ensuring all parties have access to the same data. Furthermore, holding confidential information on staff on multiple computers can be a security risk, particularly if data is stored on personal devices.

Just over a fifth run regular test exercises with corrective actions to follow if no response is received (22.4%), while just less than a fifth (18.8%) issue automated requests via their emergency notification system. Of the 8.4% who used other means, dedicated contact lists as part of the organizational BC plan came up in several answers, as did regular active reviews of the information on file. One respondent noted that information-sharing with HR was not effective in their organization, and that privacy legislation combined with this to complicate the effort of maintaining up-to-date lists.

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

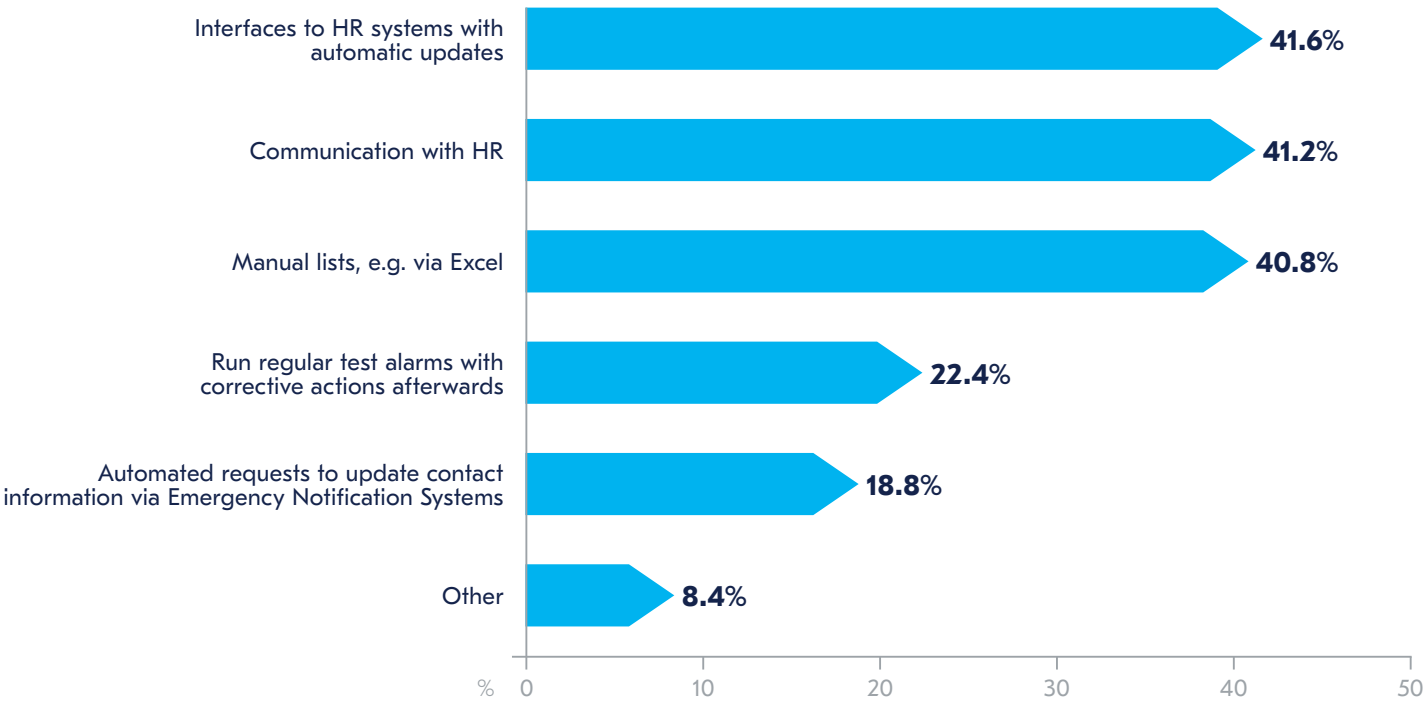


Figure 26. How do you ensure contact data of employees, experts, etc. is up to date?

Section eight: Communicating with stakeholders

Section eight: Communicating with stakeholders

- **Email remains the key communication channel, just as the mobile phone and laptop remain the key devices in business circles.**
- **Specialist emergency management software is popular for communication with internal stakeholders, but its use does not cross the boundaries of many organizations.**
- **Advanced methods such as IoT devices and dark sites remain relatively little used.**

The final section discussing communication practices for both internal and external stakeholders, essentially the type of platform used within an emergency scenario. Internally, the wrong platform can lead to a marred response by staff and externally, a poorly communicated message can, in a worst case scenario, lead to loss of customers, reputation damage, a fall in company value and legal issues.

For *internal* stakeholders, email was the most used channel during an incident, with 43.1% of respondents using it for all incidents, and the same number for 'some incidents'. Only 1.2% never used email in these situations — the same number were unsure. Interviewees commented that some IT departments were still using email to notify staff of a system outage or cyber-attack, which will obviously fail if staff cannot access their systems.

SMS messaging remained the next most popular, used in all incidents by 24.4% of organizations, and in some incidents by 35.4%, with 18.7% occasionally using this method.

The specialist emergency management software referenced earlier in this report is used for all incidents by 19.5% of respondents, for some by 23.6%, but never by 26.0%. Again, the type of platform used will vary according to the type of incident occurring. Whilst emergency management software might be effective in communicating a serious incident, using it to inform staff of a short-term system outage might dilute the effectiveness of a communication when a more major incident occurred.

Manual call trees may seem like a time-consuming and outmoded means of communicating in a crisis, but they remain popular in some circumstances — only 12.2% of organizations use them all the time, but 31.7% use them for some incidents, and 24.0% make occasional use of what was once the standard method of conveying messages to personnel in an emergency, particularly one that occurred out of office hours. Manual call trees can be used when internet communications have failed, and interviewees commented that they regularly used this method for such incidents.

> **"Yes, we have manual call trees. Actually we've gone back to using them a bit more recently when we've had internet blackouts in the floods. They're really reliable and do get the information out there. We're actually going to put it back into our plan now."**
>
> Crisis Management Lead, Mining, Germany

As significant as what methods are used can be what methods are not used. The survey found relatively little involvement of means such as third-party call centres (48.8% never used) dark sites (48.4% never used), or IoT devices (45.5% never used). These methods also carried substantial contingents who were unsure or did not answer, so their non-use percentage is probably even higher.

An interviewee spoke how they used multiple methods of communication to ensure messages were effectively communicated. Although structured, the 'scattergun' approach was highly successful within their organization.

What methods of communication do you use to communicate with internal stakeholders (e.g. employees, contractors) during or shortly after a live incident?

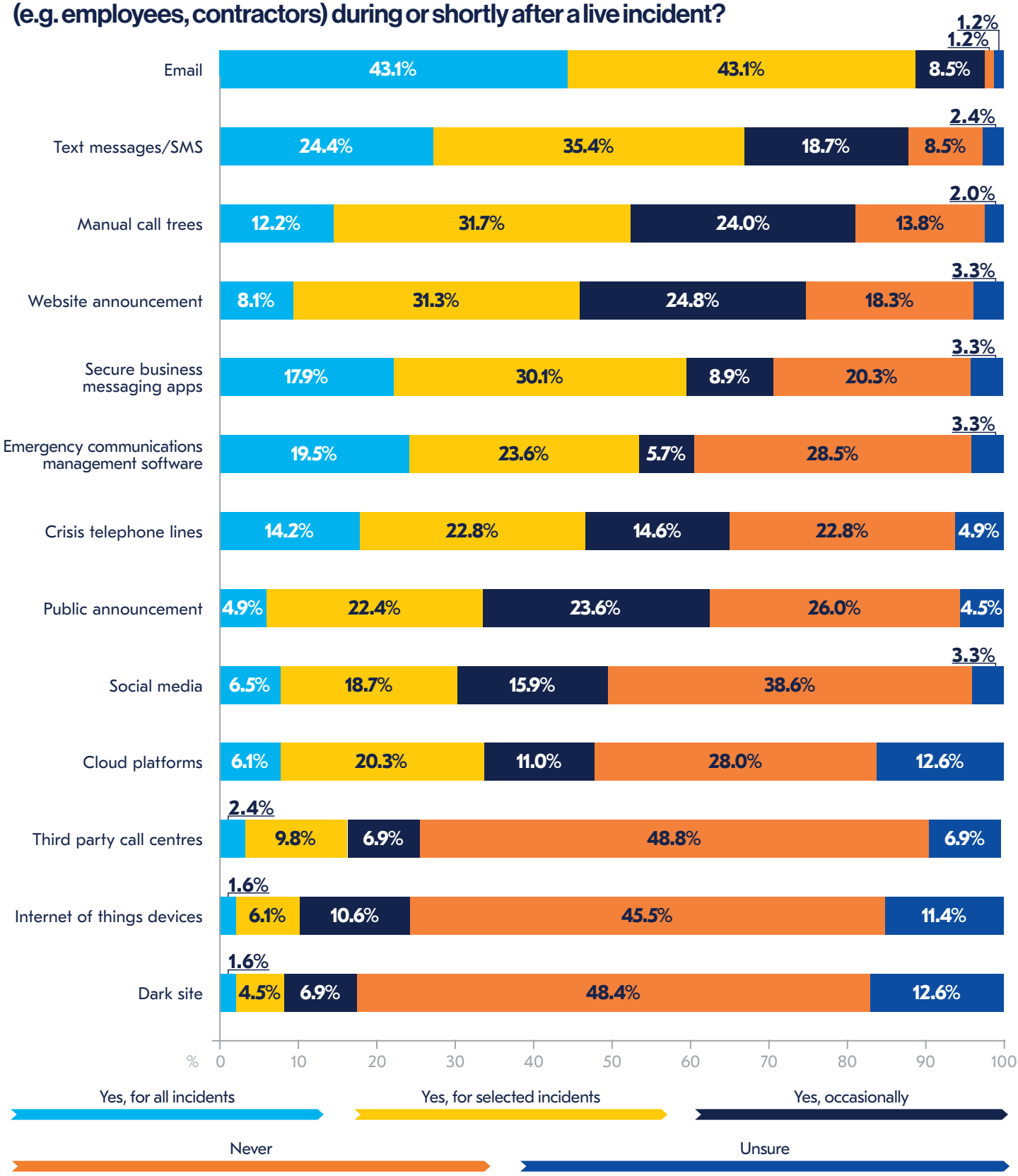


Figure 27. What methods of communication do you use to communicate with internal stakeholders (e.g. employees, contractors) during or shortly after a live incident?

Shifting to external stakeholders, such as customers or suppliers, the pattern changes, but less obviously than one might expect. Email remains the key communication method, used in all incidents by 19.2%, and in selected incidents by 45.3% (the largest figure of any positive use in this question). As might be expected, external-facing measures such as website announcements and other forms of public announcement were more commonly used for external communications than for internal. It might be surprising to some, but social media is rated as the third most popular means of communicating with external stakeholders. Still commonly viewed by many as the poor relation in terms of stakeholder communication owing to the possibility of misinformation being transmitted quickly, the speed of communication can also be advantageous to organizations if a message needs to be transmitted fast. Use must still be with care: whilst customers are likely to be sympathetic to a social media message by an organization who are reporting interrupted operations due to a hurricane, a similar message about a hacker infiltrating company systems is more likely to cause significant damage to an organization as it may be viewed as a fault of the organization, rather than a force majeure which is perceived as unavoidable.

Again, however, IoT devices (51.8% never used), third-party call centres (46.9% never used) and dark sites (46.5% never used) are not major methods. In this case, emergency communications management software is also rarely used, with almost half of respondents (49.8%) saying it is never employed for contacts with external stakeholders.

What methods of communication do you use to communicate with external stakeholders (e.g. customers, suppliers) during or shortly after a live incident?

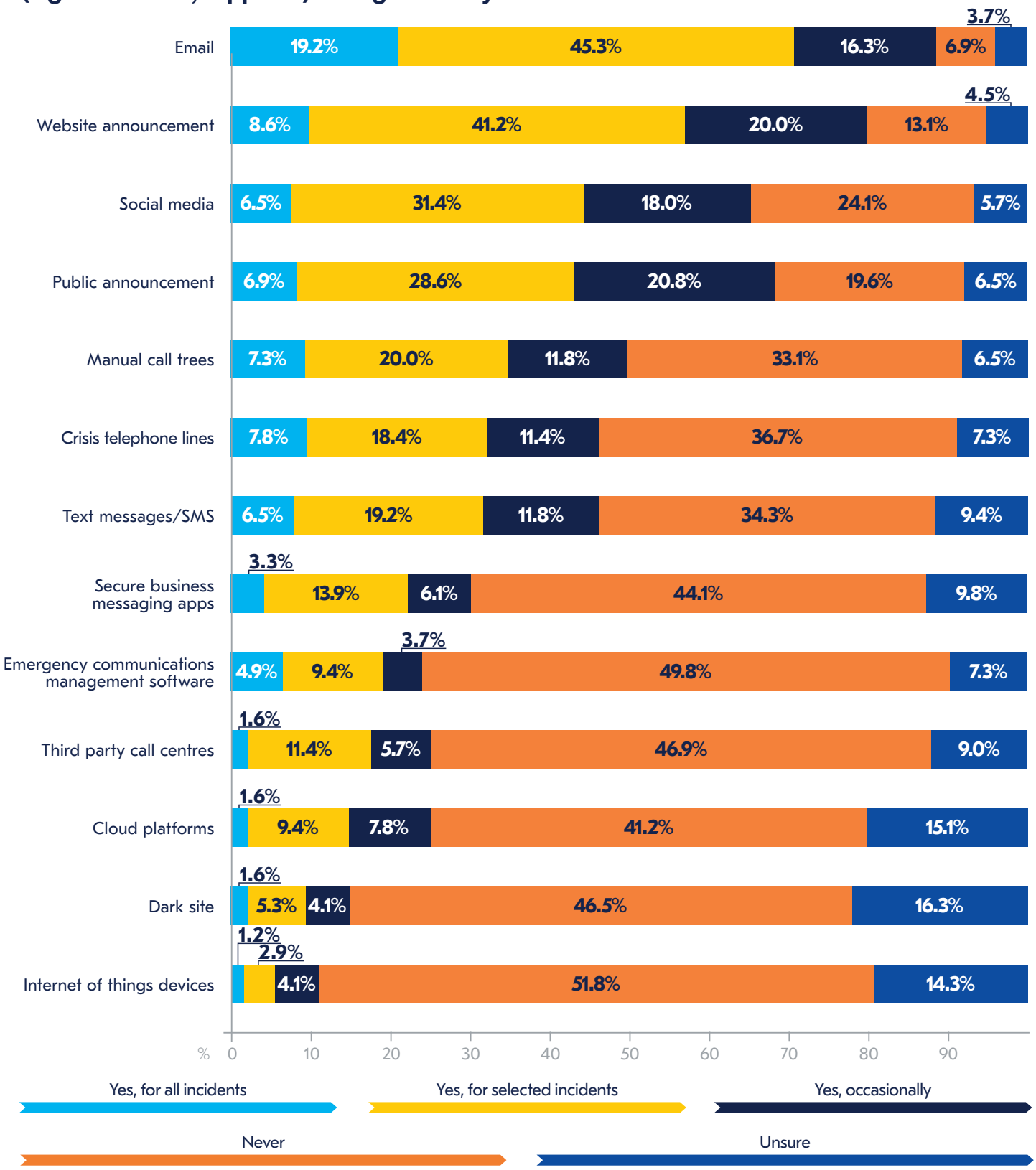


Figure 28. What methods of communication do you use to communicate with external stakeholders (e.g. customers, suppliers) during or shortly after a live incident?

Annex

Demographics

6 Dec 2021 to 4 Jan 2022

Survey dates

373

Respondents

65

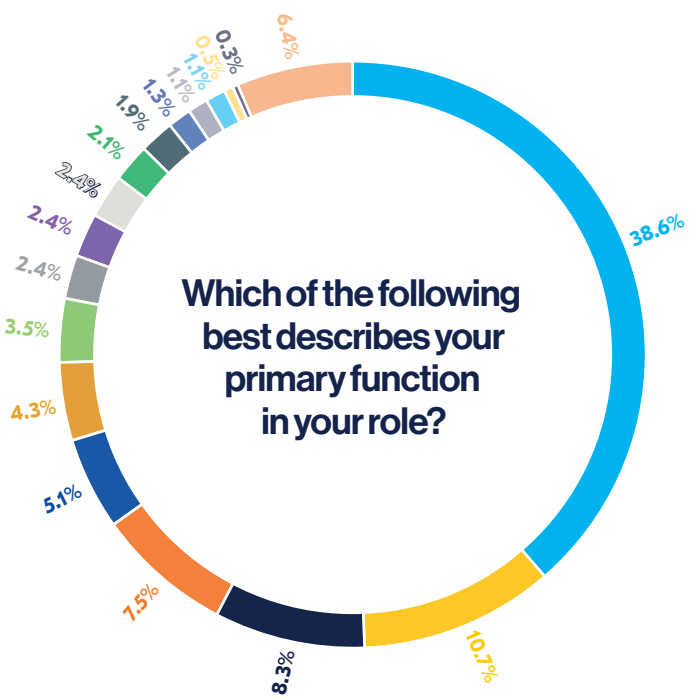
Countries

16

Sectors

10

Respondent Interviews



38.6% Business continuity

10.7% Risk management

8.3% Organizational resilience

7.5% Crisis management

5.1% Emergency planning

4.3% Operational resilience

3.5% IT disaster recovery/ IT service continuity

2.4% Health and safety management

2.4% Quality/Business improvement

2.4% Physical security

2.1% Top management

1.9% Operations/facilities

1.3% Information security

1.1% Line of business or service directorate

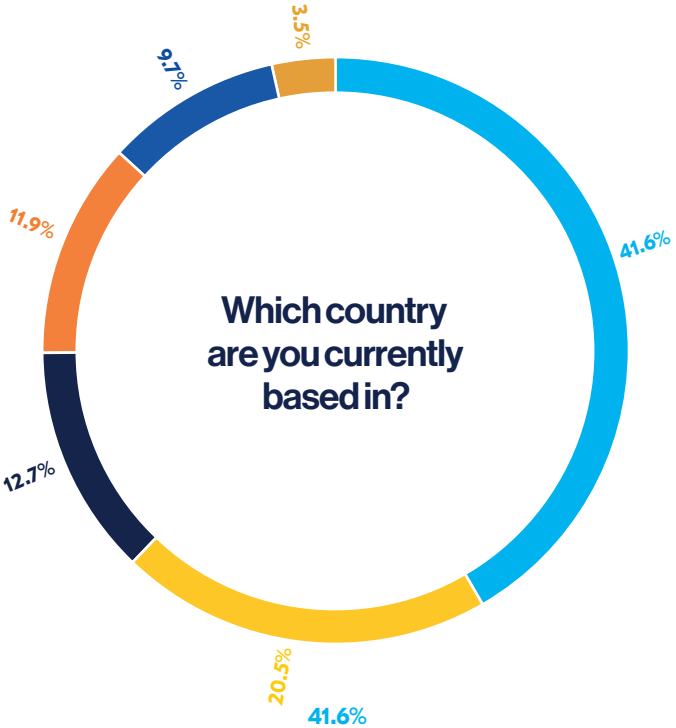
1.1% Internal audit

0.5% Communications

0.3% Supply chain and logistics

6.4% Other

Figure 29. Which of the following best describes your primary function in your role?



41.6% Europe

20.5% North America

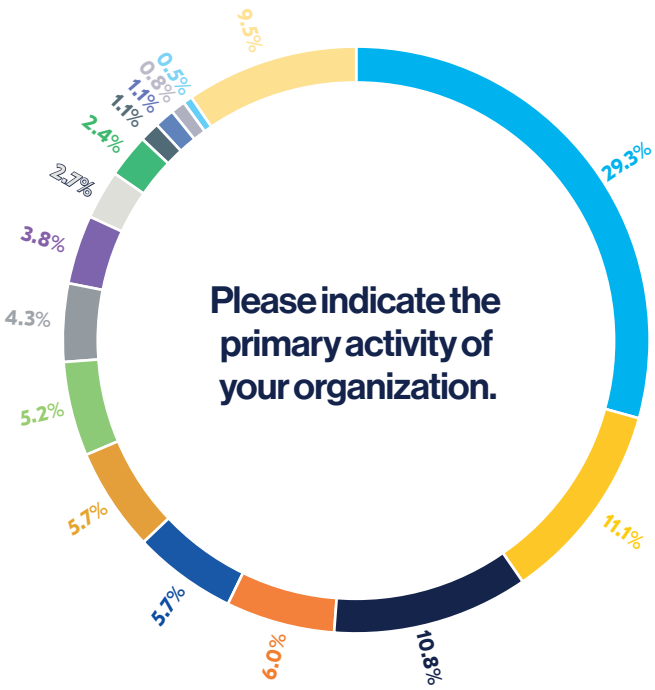
12.7% Asia

11.9% Middle East & Africa

9.7% Australasia

3.5% Latin America

Figure 30. Which country are you currently based in?



29.3% Financial & Insurance Services
11.1% Public Administration & Defence
10.8% Professional Services
6.0% IT & Communications
5.7% Transport & Storage
5.7% Health & Social Care
5.2% Manufacturing
4.3% Education
3.8% Energy & Utility Services
2.7% Telecommunications
2.4% Engineering & Construction
1.1% Retail & Wholesale
1.1% Support Services
0.8% Media & Entertainment
0.5% Mining & Quarrying
9.5% Other

Figure 31. Please indicate the primary activity of your organization.

7.9% 1-10
0.8% 11-20
1.4% 21-50
1.1% 51-100
5.2% 101-250
6.8% 251-500
8.4% 501-1,000
25.5% 1,001-5,000
9.8% 5,001-10,000
17.1% 10,001-50,000
7.9% 50,001-100,000
8.4% Greater than 100,000

Figure 32. Approximately how many employees work at your organization?

About the Authors

Rachael Elliott (Head of Thought Leadership)

Rachael has twenty years' experience leading commercial research within organizations such as HSBC, BDO LLP and CBRE. She has held the position of Head of Thought Leadership at the BCI since September 2018 and, during that time, has developed the research programme to include reports under the wider remit of resilience, as well as tackling more contemporary subjects such as climate risk and pandemic resilience. 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 research@thebci.org

David Lea (Analyst)

David Lea has extensive experience of covering the business environment and the challenges to it, primarily in Europe. He spent 14 years as an analyst with consultancy Control Risks, advising clients on threats as diverse as terrorism, natural disasters, the crises in Greece and the wider eurozone, the attempted coup in Turkey and Brexit. He has also worked in cyber security for Santander, and as a country specialist for Europa Publications. He is now a freelance writer, researcher and analyst, based in Spain, and tweets @DavidLeaEurope.

He can be contacted at research@thebci.org

About the BCI

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

Contact the BCI **+44 118 947 8215** | **bci@thebci.org**
10-11 Southview Park, Marsack Street, Caversham, RG4 5AF, United Kingdom.

About F24

F24 is the leading Software-as-a-Service (SaaS) provider for incident and crisis management, emergency notification and business communications in Europe. The highly innovative F24 solutions for alerting and crisis management help companies and organizations around the world with efficiently and successfully managing incidents, emergencies and crises. F24 also offers solutions for high-volume communication of critical or confidential content in the corporate environment. 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

Correct as of November 2021

BCI 10-11 Southview Park, Marsack Street,
Caversham, Berkshire, UK, RG4 5AF

bci@thebci.org / www.thebci.org

F24

bci Leading the way to resilience