Find out more
www.thebci.org

Thought Leadership

Emergency Communications Report 2021

F24

Leading the way to resilience

Contents

Foreword

2020 was a challenging year for most organizations, with many calling on remote working policies, communications practices and procedures that required higher levels of attention due to COVID. The BCI's Good Practice Guidelines highlights that to have a successful response, the ability to communicate effectively with both internal staff and external stakeholders is crucial. Throughout the pandemic, the fast sharing of accurate information has, and continues to be, vital: organizations have had to react quickly to lock downs and stay-at-home orders due to outbreaks, new laws were implemented by Governments overnight and some businesses had to change their strategic direction within a matter of hours. It is therefore of little surprise that nearly 80% of respondents rated one of the top and most valued benefits of a tool is its ability to quickly communicate with a large number of people.

Never before seen requirements to communicate with dispersed workforces has forced a notable change in how organizations manage their communications processes: enterprise messenger software (such as Microsoft Teams) has taken the place of unsecure free messaging applications in many organizations, and a previous reluctance by Management to implement specialist emergency communication tools and technology has been replaced with interest and support to invest in solutions. Indeed, 15% of organizations that did not have a tool pre-COVID are now actively evaluating tools for use within their organizations.

This year's report also demonstrates that despite the challenges 2020 brought, activation times have become quicker: 41% of organizations can now activate their plans within five minutes compared to 32% in 2019. This is testament to the widespread implementation of new technology solutions (such as SaaS), automating the updating of employee data in the systems, coupled with a board-driven interest in increased training and exercising.

We hope this year's report will provide useful reading for anyone in resilience-orientated professions, and that it can also serve as a means to benchmark your organization's existing technologies, processes and procedures. The findings from interviews carried out 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 participated in the survey and shared their experiences with the BCI, particularly at a time when their focus was still likely occupied by ongoing response activities.

Christopher Horne FBCI
Chair of the BCI

F24

Foreword

Last year I asked in this foreword "What can you really rely on?" and without a doubt the past year has challenged pretty much everything we have been relying on so far. Thus 2020 has also changed our perspective on crises significantly. For many businesses crisis situations luckily have been the exception before 2020. With the experience of the last year, it is not uncommon to see it as a kind of "luxury" if your company just needs to handle one crisis at a time.

The outbreak of the global pandemic has put crisis management as a top priority for all organizations and businesses are rising to the challenge of managing this extraordinary situation. Even though dealing with a global crisis as well as keeping the business running and potentially managing other incidents or crises in your organization is the opposite of "business as usual". As this year's report underlines, communication has become one of the most important and at the same time most challenging aspects in managing this "new normal". How can you manage a crisis that is constantly evolving and changing within weeks, days or sometimes even hours while working remotely and keeping every employee safe?

The relevance of technological solutions for efficient communications, collaboration and management has been proven in a large scale during the last year. The benefit of collaboration tools like Microsoft Teams, Slack and any other platform for daily business has made all this possible. However, those platforms are not the tools to use during crisis situations as they cannot offer the decisive requirements needed e.g. availability, accessibility, reliability, as well as functionality and documentation. It is precisely these requirements that often determine success or failure when it comes to dealing with crises and incidents. That is why a significant increase in relevance is even more true for secure software solutions to manage critical situations.

Looking at the results of this year's survey most organizations find that specialised solutions are vital to handle critical situations in the best possible way. Nearly three quarters (71%) now use a reliable and flexible Software-as-a-Service tool for emergency notifications or crisis management, which is an increase on the 66% of last year's report. In addition, this year's results indicate a strong awareness of the importance of a SaaS solution in organizations who were not using an emergency communication tool before the pandemic started. Additionally, the report shows that almost half (49%) of the organizations without an emergency communication tool are starting to address the topic internally or have already begun an evaluation process for a tool.

Thus, I am convinced that this year has spread the awareness of the added value software solutions — and especially secure SaaS solutions — have to offer in emergency communication and crisis management. At the same time the requirements have risen, for example the latest now being able to manage multiple incidents at different locations in parallel and in real time is a must have.

The times ahead are everything but secure and in this special situation we are even more delighted about our partnership with the BCI on creating this valuable and well-trusted Emergency Communication Report 2021. We hope you will gain a lot of new insights from the analysis. Enjoy reading the newest Report!

Christian Götz
Co-founder and Executive Board member
F24

Emergency Communications Executive Summary

Executive Summary

The pandemic has driven organizations' adoption of collaboration software (such as Microsoft Teams) in 2020 which looks set to stimulate adoption of more specialist emergency communication tools and technologies: The use of specialist tools and software for emergency communications took a slight dip in 2020 to 64.0% of organizations. The dip appears to be temporary however, with many organizations who have been using collaborative tools/ software for the first time in 2020 now seeking to extend investment into specialist emergency communications technology solutions.

The use of software-as-a-service continued to rise in 2020, with three-quarters of organizations now using it compared to 16% who use on-premise installed software: SaaS technologies not only have the advantage of being able to be deployed quickly across multiple devices, but also lead to plans being activated quicker. 54% of those using SaaS technology can activate their plans in five minutes or less compared to 36% who use on-premise installed solutions.

2020 — the year of the Virtual Crisis Room: Dedicated online collaboration tools/virtual crisis room technology were used for crisis team collaboration by 57.5% of organizations in 2020 compared to 54.5% who reported using a physical crisis room. With most organizations having very few staff on site in 2020, the move to virtual environments is to be expected. However, with the investment in this type of technology and many organizations reporting it to be a success, use of virtual alternatives to physical rooms looks set to continue, even as workforces move back into offices.

Cost remains the primary barrier to investing in emergency communications solutions: 30% of organizations who currently have no dedicated tools or software admit cost is the major barrier, particularly for smaller organizations. Those interviewed for the report however described an increased interest from senior management in investing in tools because of COVID-19 showcasing the need for such a tool to be employed.

Activation times are getting quicker: 41% of organizations can now activate their plans within the 2019 report-dubbed "golden five minutes" compared to 32% in 2019. Although some of this increase can be attributed to increased use of SaaS technologies, some of it is down to increased training and exercising of plans. Many organizations reported that COVID-19 has resulted in multiple activations this year which has helped to highlight issues causing delays in activation.

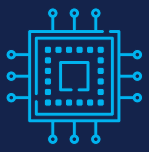
Has WhatsApp now had its day in terms of messaging solutions? Previous years' reports have highlighted an overreliance on messaging apps from the private environment for communication during emergency situations. Whilst WhatsApp, for example, is a tool that most are familiar with, does not have the functionality required for a safe and secure solution for communication. Indeed, just 18.7% of those who use a tool from the private environment (such as WhatsApp) are happy with their messaging solution, compared to 60.0% who use a dedicated tool.

The level of training and exercising carried out in organizations has remained unchanged in 2020 — boosted by real world activations: Three-quarters of organizations have still been training for emergency communications activations this year and 82% have been able to exercise plans. Real-life activations due to COVID-19 have also acted as a training tool in themselves and is likely to be a factor in faster response times and meeting response time targets.

The need to alert a high number of people quickly is the most valued functionality of a tool: Alerting and mobilising a high number of people very fast was the most valued functionality of emergency communications tools/software, selected by nearly 80% of respondents. COVID-19 has propelled this functionality to the fore due to the increased need to contact all staff quickly due to a disease outbreak or new laws coming into place overnight.

1. Hern, A (2021). UK regulator to write to WhatsApp over Facebook data sharing. Guardian [online]. Available at: https://www.theguardian.com/technology/2021/jan/26/uk-regulator-to-write-to-whatsapp-over-facebook-data-sharing [accessed 28 January 2021].

Top Tips for 2021



Now is a good time to approach senior management for investment in new tools and technology
The research for this report has shown that the pandemic has highlighted the importance of good emergency communications through senior management and some professionals are already reporting increased budgets for new technology in this area. Provide evidence how technology has improved/could have improved response during an emergency and, if possible, the cost savings that could have been realised.

Consider adopting a SaaS tool
Whilst there will always be exceptions, the use of SaaS technology clearly speeds up response times and allows emergency communications to be deployed quickly and easily across a range of devices. With many staff working remotely and using different devices (including personal devices), SaaS can help bring about universal adoption.

Continue to exploit the increased levels of collaboration COVID-19 has brought about
Members have reported that different departments across the business (including Business Continuity and Crisis Management) have been collaborating more during 2020 to bring about a cohesive response to COVID-19. Technology has played a large part in bringing about these levels of collaboration. Seek to continue these increased levels of collaboration.

Continue to evolve data storage processes
Many organizations continue to struggle when it comes to accessing data quickly and reliably, with many admitting to still using Excel spreadsheets for storing employee information. Information not only gets out of date quickly and can result in version control issues, but has the potential to breach data protection and GDPR laws. If information is still stored in a non-compliant way, consider acting now before legal issues are encountered.

Review travel policies
97% of organizations stopped international travel during COVID-19, but most companies have yet to update travel guidance to reflect new working practices post-COVID. With vaccines now being introduced globally, business travel is likely to start increasing during 2021. Make sure travel policies are updated according to ensure staff are safe when travelling and consider reviewing which countries your organization defines as "high risk".

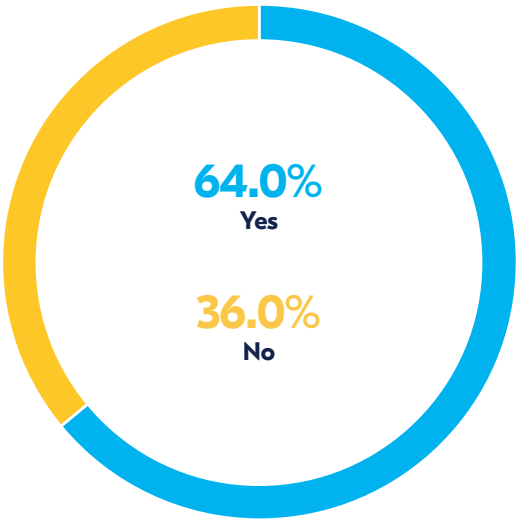
Training and exercising
Whilst many organizations have increased the amount of training and exercising this year, particularly due to the increased number of "real life" activations. With new systems and processes being adopted by most organizations post-COVID-19, ensure relevant training and exercising is carried out to make sure staff are up to date with new practices.

Communication Processes and Tools

The use of specialist tools decreased in 2020, but looks set to increase in 2021

The decline looks set to be temporary due to a change in usage of platforms in 2020.

Does your organization utilise emergency notification/ crisis management tools or software?



The pandemic has driven an increase in SaaS solutions for emergency communications tools

Three-quarters of organizations are now using SaaS technologies compared to two-thirds in 2019

Type of software/solution being used for emergency communications

15.4%
On-premise installed software

74.1%
Software-as-a-Service solution

Key communications challenges during an emergency

Cost remains the primary barrier to organizations adopting specialist tools and software

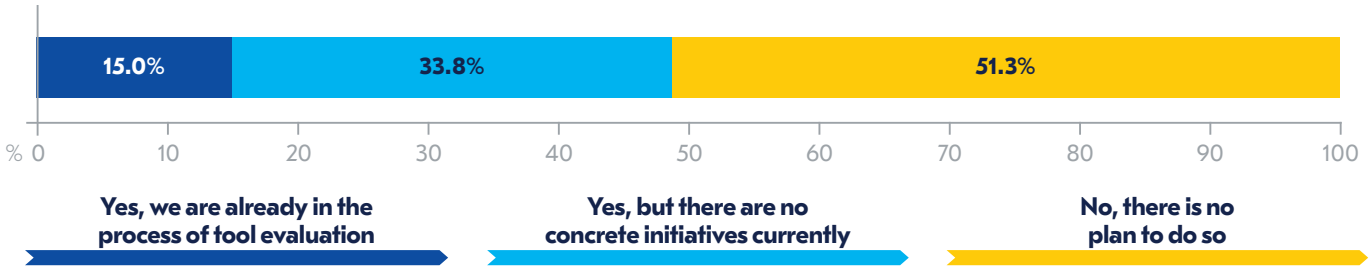
Many organizations also feel they are too small to warrant the need for a specialist tool

Reasons cited for not using/planning to use a tool/software for emergency communications

COVID is set to drive uptake of specialist emergency communications tools

Nearly half of organizations who did not have a tool pre-pandemic are now considering it

Will your organization use a tool going forward after the experience of the COVID-19 pandemic?

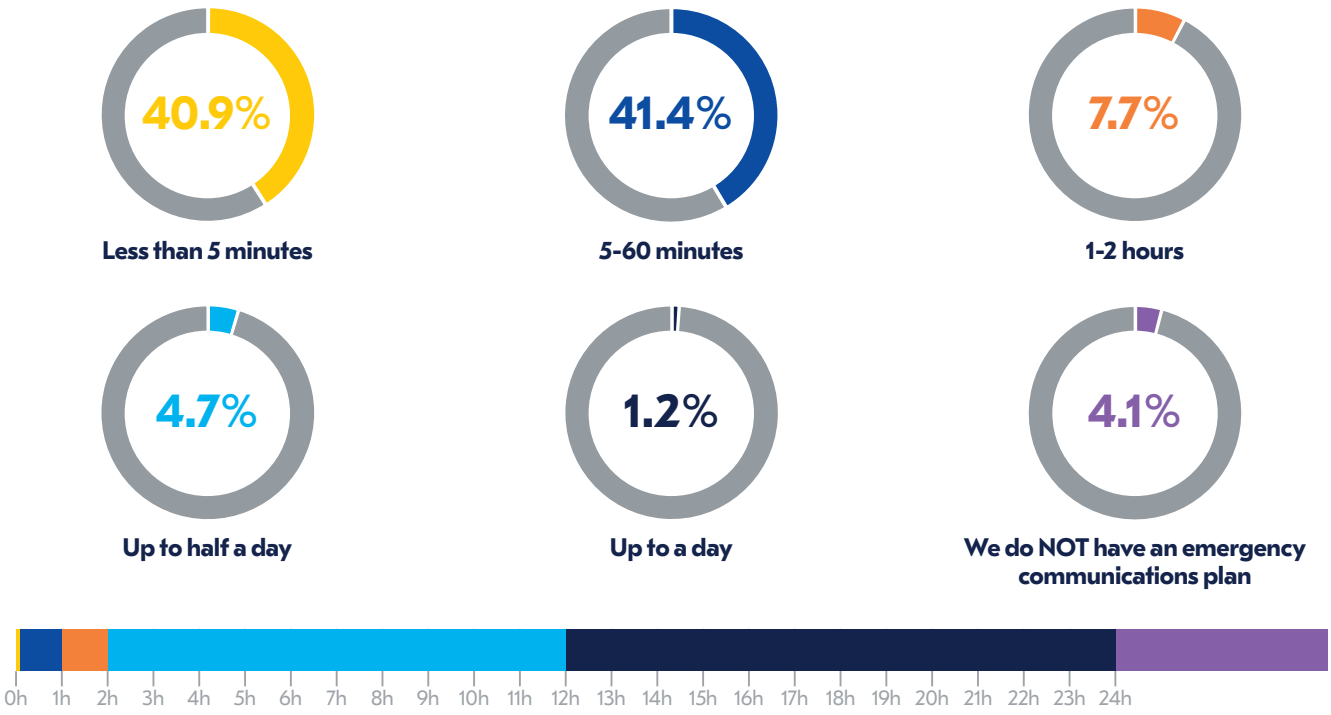


Timing

Activation times for emergency communications plans are getting faster

41% of organizations can activate their plans within 5 minutes compared to under a third in 2019

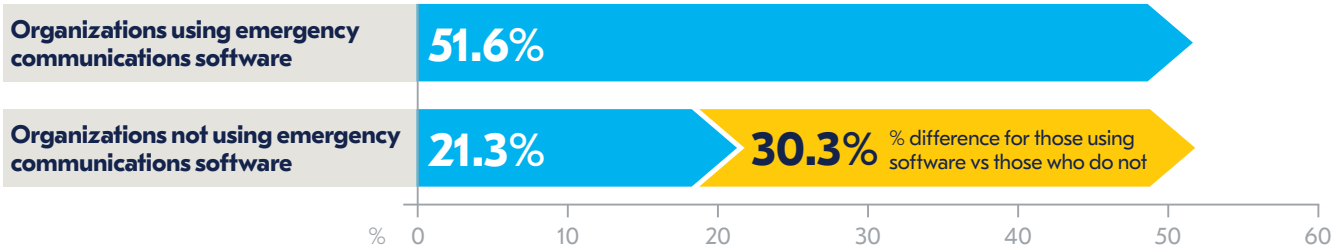
How long does it take to activate your emergency communications plan on average?



Use of specialist tools enables plans to be activated quicker

51.6% of organizations using specialist tools can activate their plans within five minutes compared to 21.3% who do not use specialist tools

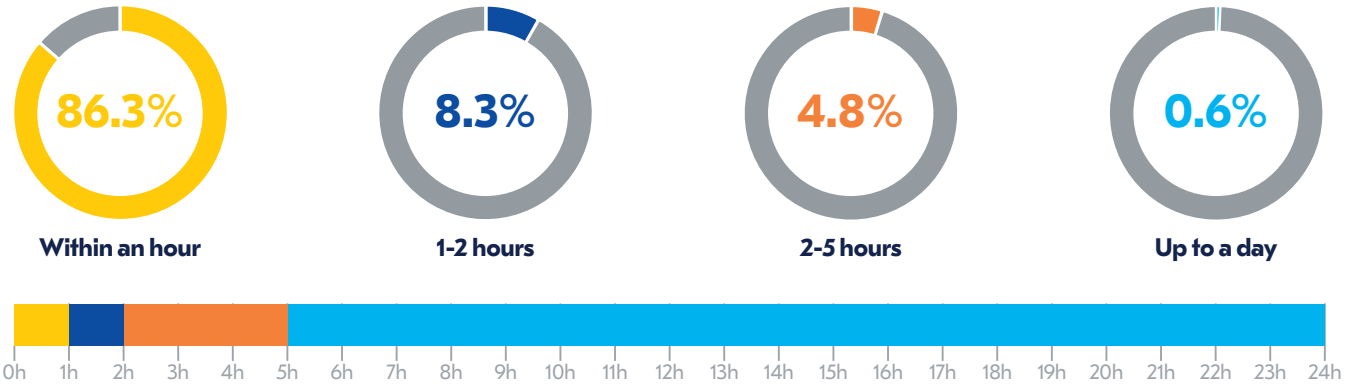
Percentage of organizations able to activate their plans within five minutes



87% of organizations can now provide initial information to Management within an hour

This compares to just 67% in 2019

How long does it take to provide initial information to top management?



Collaboration

The pandemic has increased the use of virtual crisis rooms for crisis teams

The use of virtual crisis rooms/dedicated tools for crisis management exceeded the use of physical rooms in 2020

How do you organize collaboration in your core crisis team?

WhatsApp's popularity as a messenger app in emergency scenarios is waning

Under a fifth of organizations are now using free messaging apps to communicate in an emergency

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

43.5%

An enterprise messenger, e.g. Teams, Slack, Skype

23.8%

A secure messaging app dedicated for the use within critical situations which is integrated into our emergency communications solution

19.1%

Free messaging apps from private environment e.g. WhatsApp, WeChat

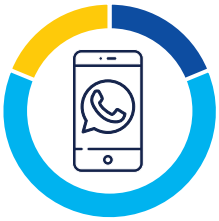
9.5%

We do not use messaging apps

Are you happy with the solution you are currently using?

An enterprise messenger

Secure messaging within emergency communications tool



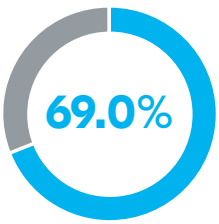
Free tools from the private environment

Incident Preparedness

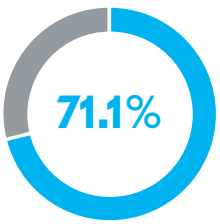
The number of organizations achieving their expected response levels has risen for the fourth year in a row

Continued investment in tools and training means nearly 80% of organizations are now reaching their response levels

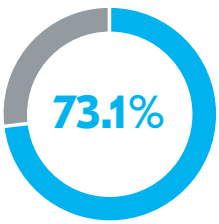
Percentage of organizations reaching their expected response rate



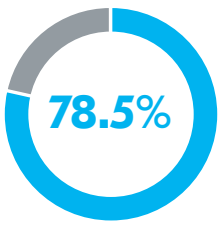
2017



2018



2019



2020

Training and Exercising

Despite the challenges presented to organizations in 2020, nearly three quarters have still been able to carry out training of communication plans at least once

73.1% of organizations have carried out training at least once a year

16.7%
Every three months or more frequently

19.2%
Every 6 months

37.2%
Every 12 months

7.7%
Less frequently than every 12 months

14.1%
We carry out training ad hoc

5.1%
Never

Over 80% of organizations exercise their plans at least once a year

Despite organizations reporting less of a need for exercising this year due to "real" activations, 83.5% still report exercising plans at least once a year.

7.2%
Monthly or more frequently

15.0%
Quarterly

17.7%
Twice a year

42.5%
Once a year

9.8%
Less than once a year

4.6%
Following an incident

3.3%
Never

International Travel

The pandemic has resulted in organizations becoming more risk averse in terms of international travel

60% of organizations now consider some of the countries they travel to as "high risk" compared to 47% in 2019

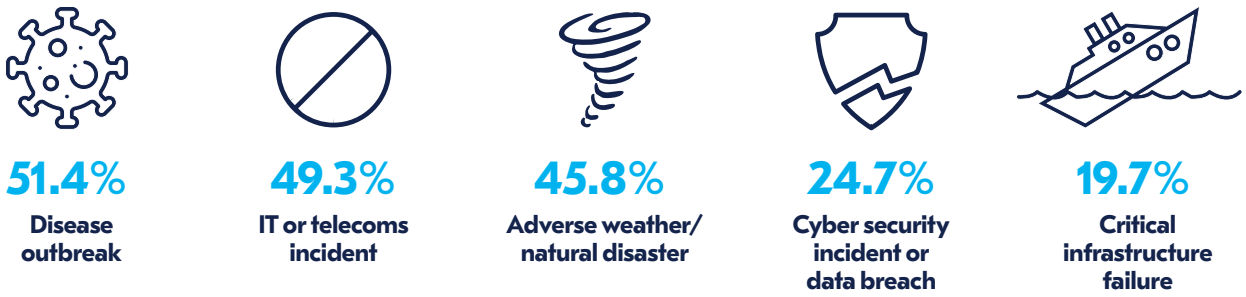
Percentage of organizations considering the countries staff travel to are high risk

Emergency Communications Plan Triggers

Disease outbreak entered the top five triggers for the first time since the report's inception

Over half of organizations activating their emergency communications plan in the past year because of the pandemic

Percentage of organizations reaching their expected response rate



Overview

The key findings of last year's Emergency Communications Report showed several positive key trends within emergency communications: more organizations than ever before were employing specialist emergency communications tools and software, the "golden hour" was becoming the "golden five minutes" with organizations able to activate plans quicker than ever before and regular exercising and training was fast becoming the norm.

This year, we have noted the positive trends continuing with COVID-19 proving to be a major facilitator to change: with many staff working remotely, emergency communications software is being used to alert staff to COVID-19 information, staff are becoming more proactive about keeping contact details up-to-date because they are concerned about missing vital information that would be more readily communicated in an office environment and others have reported that management have realised the importance of using a fully integrated emergency communications tool and are already actively investing in new, mainly SaaS, solutions — despite the financial constraints many organizations are currently suffering.

There are, however, other organizations who have found their current emergency communications solution was not adequate to cover the challenges faced during COVID-19. Whilst some sectors — particularly those which have been hit hardest by cost-constraints because of COVID-19 — have been forced to cut spending on advanced tools and solutions and temporarily reverted to collaboration software such as Microsoft Teams or WhatsApp, others have found that automatic alerting capabilities (e.g. weather or social media alerts) have not been sufficient to cover the intricacies of COVID-19.

Overall, however, 2020 has been a year to highlight the importance of technology for communication. Microsoft Teams has seen the number of daily active users rise from 20 million in November 2019 to 115 million in October 2020[2] whilst Zoom has been the biggest gainer in the Nasdaq Emerging Cloud Index with its shares rising by 483% in 2020[3]. The positive trends seen in collaborative software is also now moving to the emergency communications software sector: a start-up company in the emergency communications space raised $15m in funding at the height of the COVID-19 pandemic and successfully doubled its valuation. Furthermore, some of those we interviewed for this report told how their organizations were now looking to actively invest in new tools specifically for emergency communications because of the successful adoption of collaborative software such as Teams or Zoom.

This report will examine the trends noted above in detail, together with showcasing how particular organizations have adapted their own emergency communications procedures throughout the year.

2. McCraw, C. (2020). What the Growth of Slack and Microsoft Teams Means for Enterprises. Mio Dispatch, [online], Available at: https://dispatch.m.io/slack-microsoft-teams-enterprise-growth/ [accessed 15 January 2021].
3. Swatz, J (2020). In just one week, Microsoft adds as many users to its Teams collaboration software as rival Slack has in total. MarketWatch, [online]. Available at: https://www.marketwatch.com/story/these-tech-companies-with-telecommuting-tools-are-well-positioned-during-the-coronavirus-pandemic-2020-03-19 [accessed 15 January 2021].

Communication Processes and Tools

Communication Processes and Tools

- **Use of emergency communications tools and software has seen a slight fall in 2020, but this trend is expected to reverse in 2021. However, of those using a tool, usage of SaaS solutions increased significantly.**
- **Nearly three-quarters are now using Software-as-a-Service (SaaS) technologies for their emergency communications solution compared to two-thirds in 2019.**
- **Some organizations switched to collaborative tools such as Microsoft Teams for the first time in 2020 and now plan to move towards a specialist emergency communication tool in 2021.**
- **Onsite one-way communication tool usage has fallen this year because of remote working.**
- **SaaS tools help to increase response time in a crisis: 54% can activate plans within 5 minutes if SaaS tools are used compared to 36% who use on-premise installed software.**

This year, the number of organizations that report using emergency communication/crisis management tools and software has remained on a par with 2019 with 64.0% of respondents reporting that they do use specialist tool within their organizations (2019: 67.0%). The slight decline in numbers could be down to a change in usage of platforms during the pandemic: some interviewees reported they had moved to using a collaborative platform such as Teams due to their incumbent solution not being sufficient to manage emergency communications during the pandemic and planned to move "back" to a specialist tool again in 2021, being more selective with the criteria required.

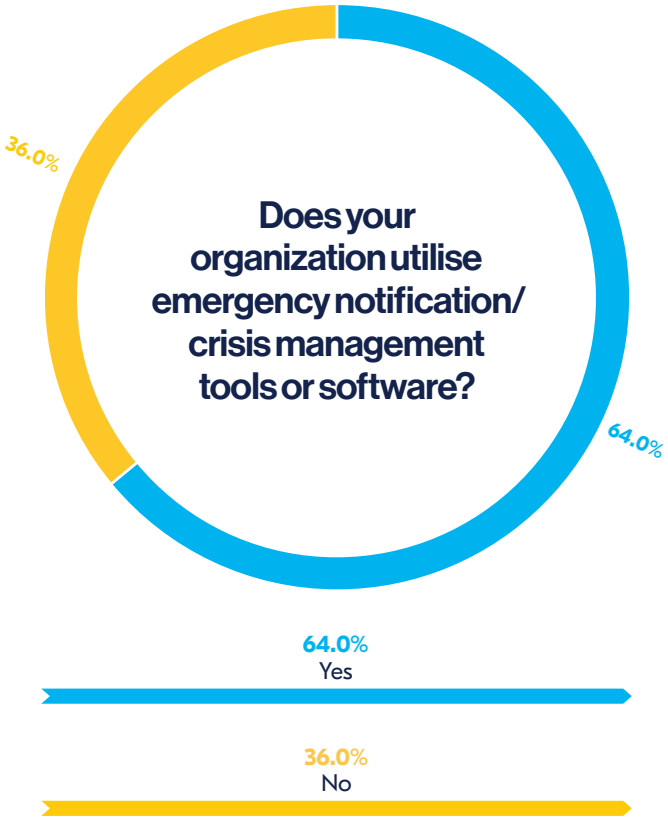


Figure 1. Does your organization utilise emergency notification/ crisis management tools or software?

This year, the tools and technologies used by organizations to manage their emergency communications has also seen a defined shift: whilst mobile phones and desktop/ laptop computers remain the primary devices to manage emergency situations for 95.2% and 97.8% of respondents respectively, desk phones have seen a dramatic drop from 55.2% in 2019 to 30.0% in 2020. Although this would be expected because of so many staff working remotely in 2020, it does show the further decline in importance of the desk phone and how traditional communication solutions, such as call-trees, will need to be reviewed to ensure they still work effectively with mobile devices.

Traditional onsite means of communications have also seen a fall in popularity this year: walkie-talkies and radios were only used in the management of 18.5% of emergency situations (2019: 36.5%), public address systems in 13.2% of emergencies (2019: 33.2%), on-screen display in just 12.8% of emergencies (2019: 21.6%) and pagers in 3.5% of situations (2019: 7.7%). Whilst the use of some of these tools will increase as organizations start to move back to physical environments, for those that continue to operate in a remote environment or change their working models significantly, we are likely to see a shift in how organizations allocate their budgets to different types of communications devices.

What devices are you using to manage emergency situations?

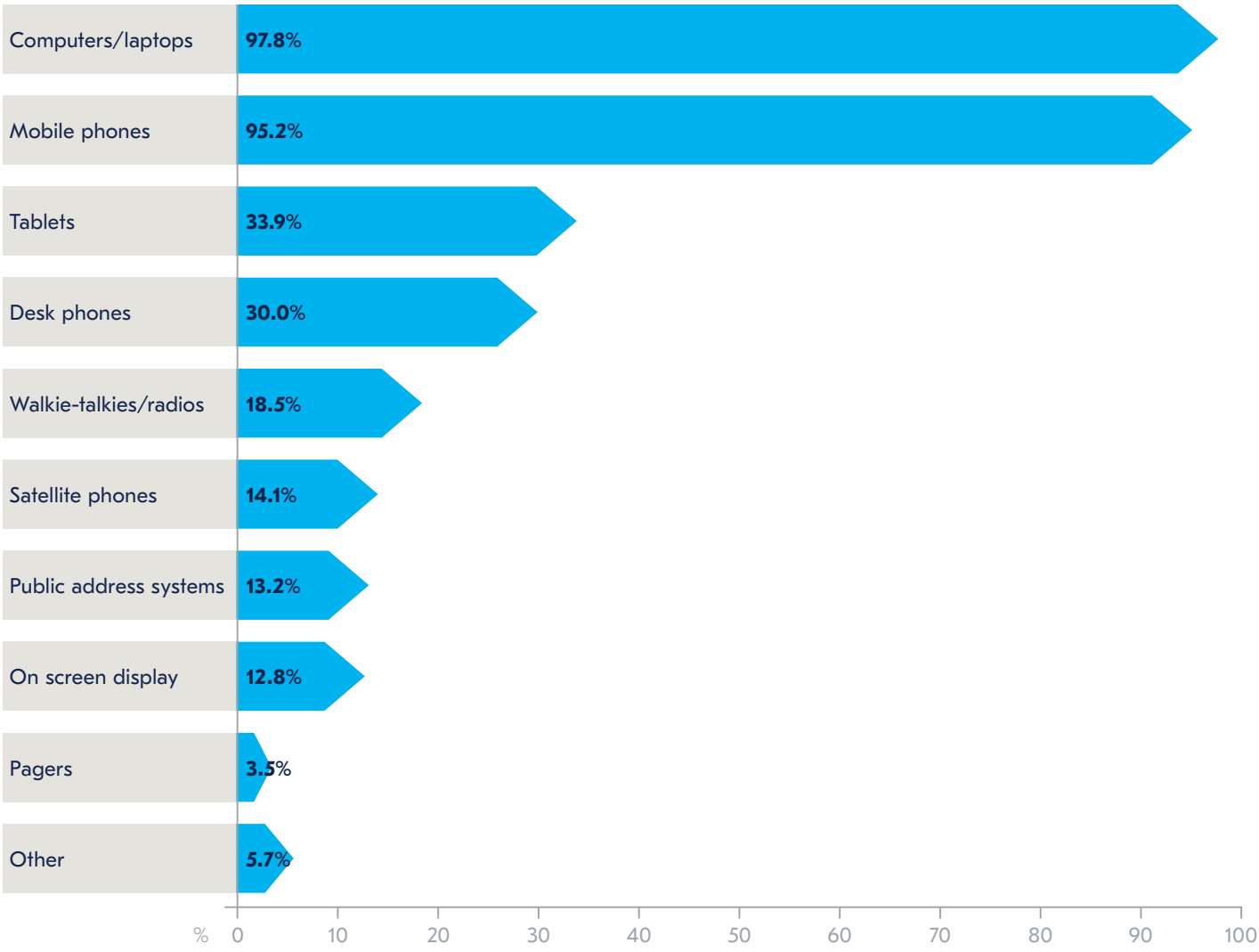


Figure 2. What devices are you using to manage emergency situations?

Another notable shift this year is the type of software organizations are using to manage their emergency communications plans. Last year, we saw an increase in the number of organizations switching to software-as-a-service (SaaS) solutions as they proved to be more effective at managing a response across different devices.

This year, the trend for using SaaS has increased even more, with 74.1% now using SaaS solutions as their emergency communications tool (2019: 65.9%). In a period where a crisis (such as COVID-19) has forced a long period of remote working, SaaS solutions can help to provide access from anywhere, across multiple devices and more flexibility than on-premise solutions which is a major factor behind this increase.

Figure 3. Percentage of organizations able to activate emergency communications plans within five minutes

Using a SaaS tool not only has the advantage of being easily deployed across multiple devices, but also results in emergency communication plans being able to be activated quicker. 54.1% of organizations using a SaaS tool can activate their emergency communications plan within five minutes or less (2019: 34.7%) compared to 35.7% who use on-premise installed software (2019: 32.9%). This was a trend first noted last year, but the gap has widened further in 2020.

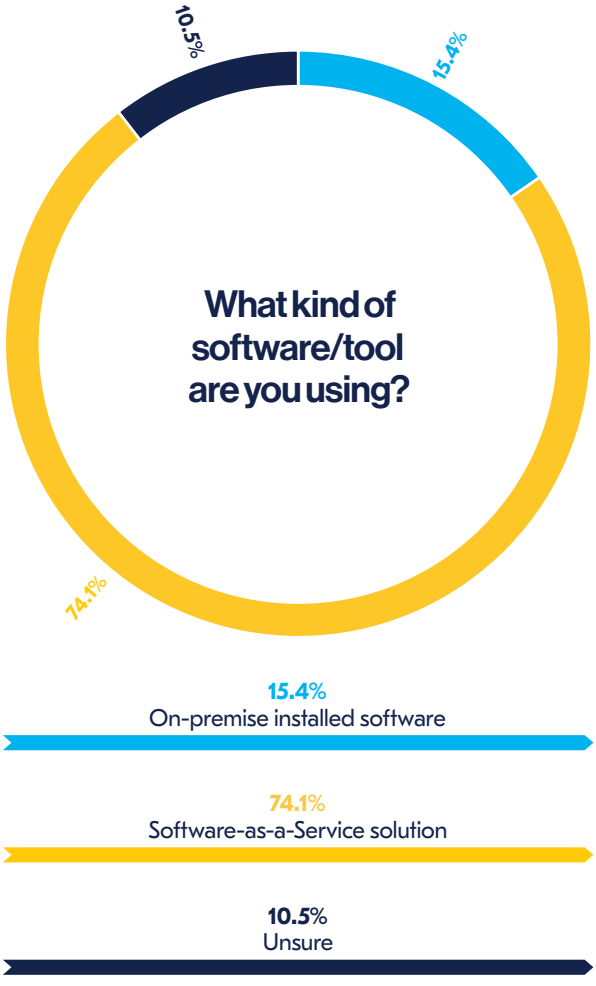


Figure 4. What kind of software/tool are you using?

Key communications challenges during an emergency

Key communications challenges during an emergency

- **The ability to alert a high number of people quickly is the most valued functionality of a dedicated tool.**
- **The need to contact staff at weekends during the COVID-19 pandemic (e.g. because of a forced office closure on Monday as a result of a COVID-19 outbreak) has seen organizations become more reliant on their tools as an accurate means of contacting people.**
- **Cost is the primary barrier to organizations investing in tools, although many are hopeful of increased investment post-COVID-19.**

The most highly valued function of a business continuity tool/software is the ability to alert a high number of people quickly. More than three-quarters of respondents (78.9%) cited this as a functionality used by their organization in a crisis. Indeed, interviews have revealed that some organizations which have used office collaboration tools as an alternative for an emergency communications tool have found that its use as a dedicated emergency communications tool is limited: users must be connected to a data network, SMS communication was not readily available, there is no way of knowing quickly who had seen a message and messages tended to be ignored as recipients are not aware of the importance.

Specialist emergency communication tools can help to ensure that employees are always reached: previous editions of this report have discussed how it can be difficult to communicate with employees at weekends, for example. Given many organizations have had the need to communicate with employees at weekends during COVID-19 (e.g. a change in law directly affecting the workplace or a COVID-19 outbreak which means the office will be closed on Monday), specialist tools have helped to overcome this problem.

> **"The last time I used it was on Sunday of this week because we had a confirmed case of COVID-19 in the office and we had to mobilise and inform all of those people that were in the office last week of the situation. We closed the office and had to have it deep-cleaned yesterday. [Our Emergency Communications tool] provided a means of alerting staff at the weekend to say that there had been an incidence of COVID-19 and that the office was closed for Monday or until further notice at the time. It really helped us to reach out to people because not everyone has their work devices on at weekends."**
>
> Group Business Continuity Manager,
> Financial Services, United Kingdom

Other popular requirements of a specialist emergency communications tool/software is as an enabler to communicate in teams (54.9%), additional crisis handling functionalities like task management (52.8%) and emergency planning capabilities (48.6%). Tools such as risk monitoring and management were only considered helpful for a fifth of respondents (21.1% and 23.9% respectively). This is corroborated by findings from interviews: some professionals found that they were preferring to rely on their own information sources for risk intelligence and early warning of potential hazards and found their reliance on this aspect of their emergency communications tool was being used to a lesser extent in 2020.

In which areas does your tool/software support you?

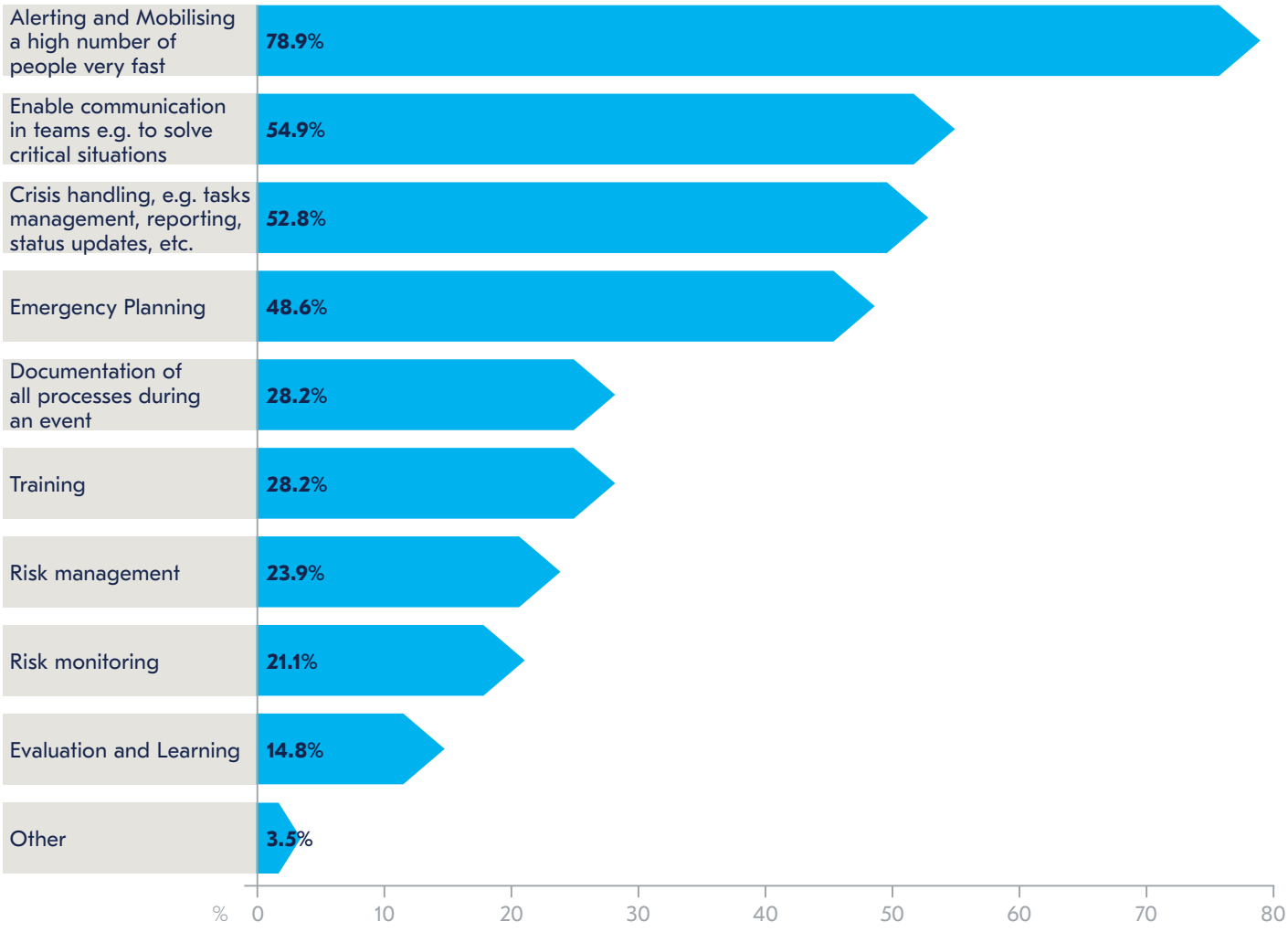


Figure 5. In which areas does your tool/software support you? (Tick as many as applicable)

For those organizations who either do not currently have or are not planning to have a dedicated emergency communications tool or software in place, the primary reason cited was either cost (30.0%) or that their organization was too small to warrant such a purchase (20.0%). These figures are similar to those recorded in the 2019 report (36.4% and 19.1% respectively). Smaller organizations are less likely to have a dedicated emergency communications tool and/or software: 46.3% of organizations with 250 employees or below have such a system in place compared to 69.6% of organizations employing over 250 staff. However, given nearly half of small organizations (48.1%) are still able to activate their emergency communications plan within five minutes compared to 39.5% of large organizations, it does demonstrate that such a tool may not be warranted for all small organizations due to less complex organizational structures and concurrent ability to cascade information quickly through the organization.

Nevertheless, with organizations' workforces becoming increasing remote as a result of COVID-19, smaller organizations may wish to re-evaluate the effectiveness of their current plans and consider adopting a tool to ensure the same degree of agile communications can continue in a remote environment.

Indeed, nearly half of organizations (48.3%) that currently do not have a dedicated emergency communications tool or software in place are now considering it, with 15.0% already in the process of evaluating tools. However, it is more likely to be larger organizations who are looking into purchasing a tool with just 3.6% of smaller organizations currently evaluating tools.

For some organizations, a crisis (such as COVID-19) can prompt an organization to purchase a new tool. Organizations who had not regularly rehearsed plans but found an increased need to contact staff during the pandemic due to changes in Government legislation, changes to company policy and outbreaks at company sites, provoked an investment in a specialist tool. A crisis, whilst not the ideal method, can help to get management buy-in for investment.

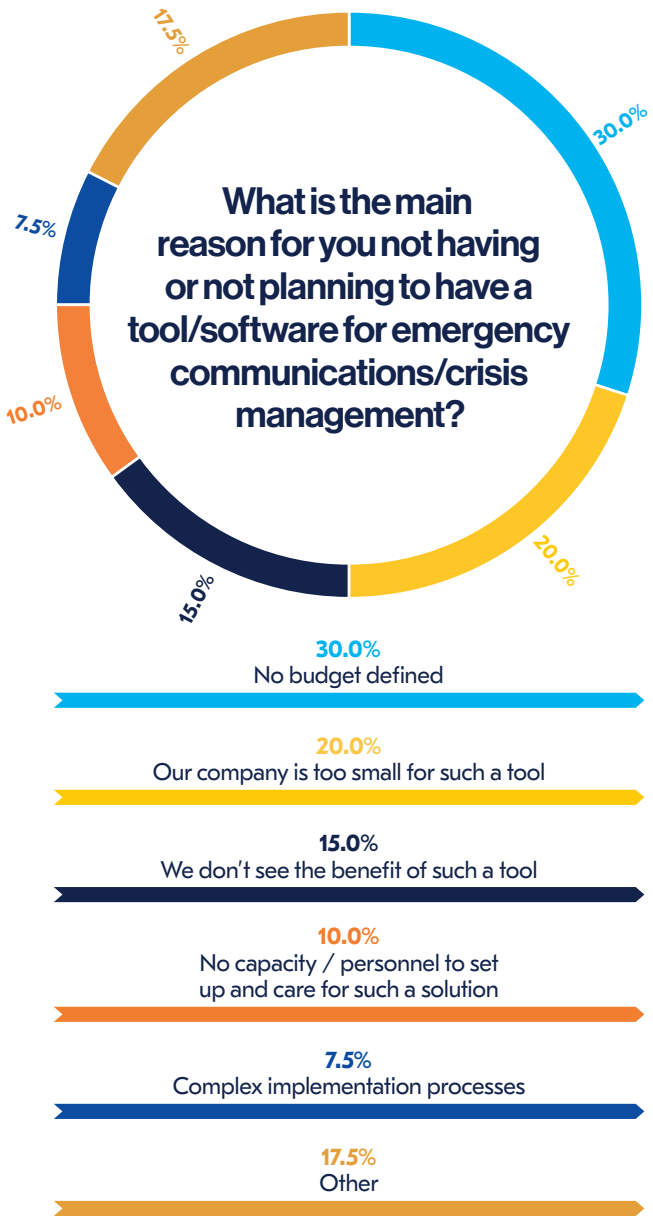


Figure 6. What is the main reason for you not having or not planning to have a tool/software for emergency communications/crisis management?

"When COVID-19 came along, we didn't have a specialist tool and relied on Skype to get hold of people during a crisis. When we started to send alerts out – and we have had to send a lot out this year – we had a lot of people who weren't getting the messages or just thinking they were spam and ignoring them. I'd been pushing for a tool for years with my boss but hadn't had the budget. We've now just got a tool and it was them who came to me to ask that we got one."

Business Continuity Manager, Manufacturing, Austria

"So just last week we had a fire alarm and the whole evacuation procedure did not at all go the way it should have. My first thought was 'Okay, we now have to implement a crisis communications tool." And so now we're now looking at it again. Since last week actually we started looking at our tool [which was not being used] again and figured out we may have to upgrade our license. But first and foremost, we're going to have to set up a plan that goes along with the tools."

Emergency & Business Continuity Management Professional, Financial Services, Germany

Other organizations have found that by ensuring Business Continuity has a direct reporting line to the board or has an advocate who sits on the Board, awareness of Business Continuity can be raised which is likely to result in an increased propensity to invest in the tools required to ensure a more effective response.

"BC is placed directly below our CRO. And [the CRO] is still fairly new in the company but really wants to drive [increased exercising], but also emergency management, operational risk management, money laundering, compliance in general. He's really driving that, and it's making a real difference. He also absolutely feels the need for formal exercising, and really wants to drive that. He is trying to convince the rest of the board that this is really a major issue as I believe there is still a bit of resistance, but I believe the awareness will increase over the next few years thanks to him. At the moment I think our biggest problem is resources, because even though there's now more awareness for the topics, we were also hit by the recession that came with COVID-19 which means it's currently very unlikely that we will suddenly get a large influx of new team members. That would be by far the biggest issue, because awareness is one thing, but we also need resources, and we now have awareness for so many topics. I'm really hopeful the CRO will be a driving force to change this."

Emergency & Business Continuity Management Professional, Financial Services, Germany

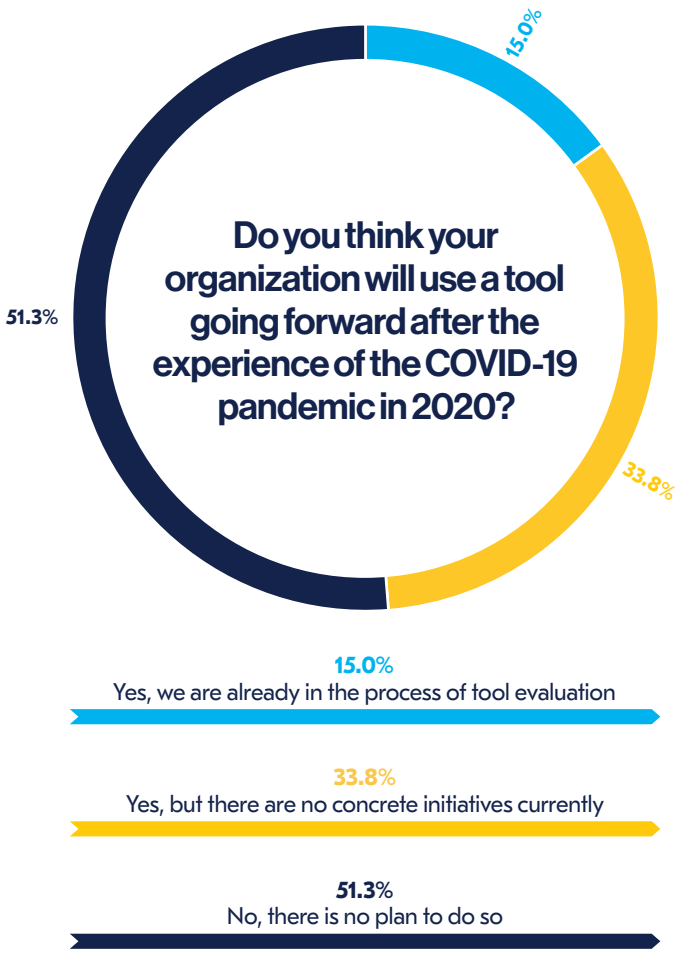


Figure 7. Do you think your organization will use a tool going forward after the experience of the COVID-19 pandemic in 2020?

Timing

Timing

- 40.8% of organizations can now activate their plans within the "golden five minutes" compared to under a third in 2019.
- Staff "immunity" to alerts because of so many real activations during the pandemic has meant more activations have taken over two hours in 2020 compared to 2019.
- Over half of organizations (51.6%) with a dedicated tool can activate plans within five minutes compared to just 21.3% for those without.
- The time taken to alert management has also decreased this year, although organizations are still wary of using automation to alert senior management due to the potential for misinformation being delivered.

Last year's report discussed how the "Golden Hour" was now becoming the "Golden Five Minutes" with nearly a third of organizations able to activate their emergency communications plans within five minutes. Despite the challenges brought by COVID-19 this year, we have seen activation times decrease further this year with 40.8% of respondents reporting that their emergency communications plan can be activated within five minutes (2019: 32.4%). 1.8% said that activation was instant due to being based on an IT event or rule.

Whilst this is a positive trend, there are some causes for concern at the lower end of the response range: this year, 5.9% of respondents admitted it took two hours or more to activate their emergency communications plans compared to 3.3% in 2019. Interviews revealed that many organizations had had to activate their plans more often this year due to incidents relating to COVID-19 and had found that activation times were slow due to staff not being physically present in the office. Others reported that due plans had been activated so many times, staff became "immune" to responding to emergency notifications.

We noted in last year's report that response time was much slower at weekends due to staff not being available on site. Although it was stated earlier that many organizations are increasing the use of tools during weekend and holiday periods to better communicate with staff on non-working days, there are still organizations that struggle with reaching expected response levels at weekends.

Using dedicated tools also facilitates the speed of activation of emergency communications plans. Over half of organizations (51.6%) that do use a dedicated tool/software can activate their plans within five minutes compared to 21.3% who do not have a such tools in place. When considering how many can activate their plans within an hour, 91.7% of respondents who had a dedicated tool in place could activate their plans in under 60 minutes, compared to under two-thirds (65.6%) who did not have such tools in place.

"[Response times] depend on the availability of the persons. I don't know why, but in the two days we have off during the week, more incidents happen. I would say 40% happen during the weekend. Ideally, we would ask that staff be more available, but this is always a problem. Some are more available; some are less available. It's also important to designate responsibilities. There could be four people in a security team of a specific country or region, but they fail to designate who is responsible during the weekend. Now we're coming to the holiday season, this can be where the failures happen."

Security Manager, Professional Services Organization, Switzerland

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	**51.6%**	**21.3%**	**+30.3%**
Percentage able to activate plan within 60 minutes	**91.7%**	**65.6%**	**+26.1%**

Figure 8. How long does it take to activate your emergency communications plan?

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

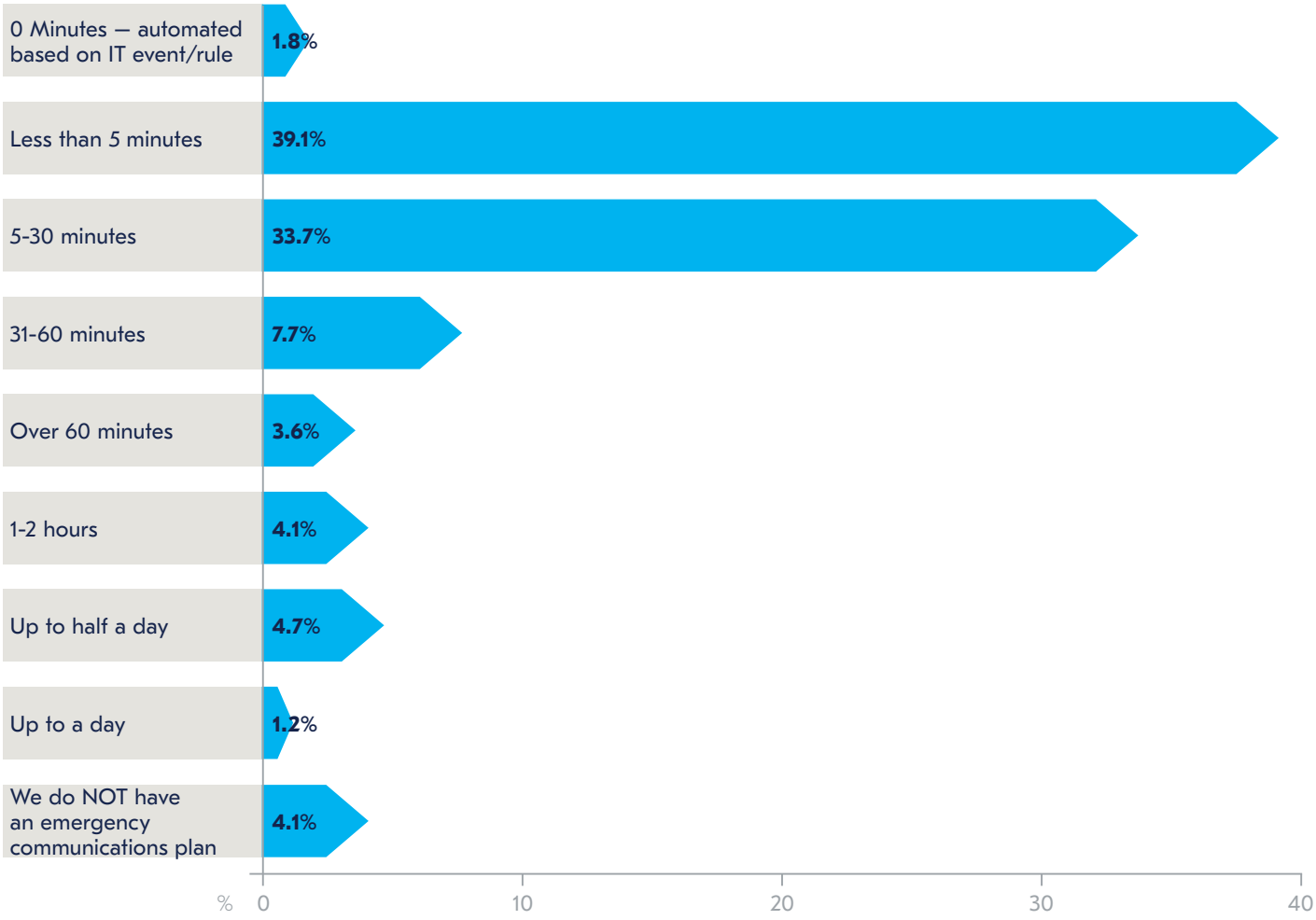


Figure 9. On average how long does it take to activate your emergency communications plan?

Another positive finding in this year's survey is the amount of time it takes to provide initial information on a crisis to top management. Last year, two-thirds of respondents (66.5%) reported they would be able to provide initial information to top management within an hour. This year, the figure has risen to 86.5% with 24.4% able to do so within five minutes. Furthermore, members have told the BCI that they have found senior management much more engaged than previously with crisis and emergency communications because of fears relating to COVID-19.

"I've struggled for years to get properly heard, but now they're calling me up most days and asking about our response to COVID-19. They are suddenly taking an interest in what me and my team are up to and we've even been invited to some senior management meetings. Once we have got through COVID-19, I will be ensuring this interest continues to be maintained.

Crisis Manager, Engineering, Australia

Managements' concerns around COVID-19 extend beyond that of the welfare of staff: there is the potential for serious reputational and financial impact if a response is not dealt with correctly. Although the number of organizations who can pass information to senior management was increasing anyway, the increase of 20 percentage points this year shows that COVID-19 has helped to accelerate this positive trend even further.

Again, the speed of communication to Management depends on whether an organization is using a dedicated tool. Some organizations are finding that escalation to Management can be made without any staff intervention through use of an automated IT event or rule.

However, such automation should be used with caution: staff intervention would normally be advised so only key information can be passed to senior management and ensuring false notifications are disregarded. Too much information intervention or false information is likely to lead to notifications being ignored. Whilst the presence of emergency communications software and/or tools can help to ensure information gets to Management sooner, the differences are less pronounced than those noted when comparing activation times — almost certainly due to the requirement for manual intervention. 88.8% of those with software can alert management within an hour and 25.3% in five minutes compared to 82.0% and 22.3% respectively for those with no software.

How long does it take to provide information to top management?

	Organizations using emergency communications software	Organizations not using emergency communications software	% difference for those using software vs those who do not
Percentage able to alert management within 5 minutes	25.3%	22.3%	+3.0%
Percentage able to alert management within 60 minutes	88.8%	82.0%	+6.8%

Figure 10. How long does it take to provide information to top management?

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

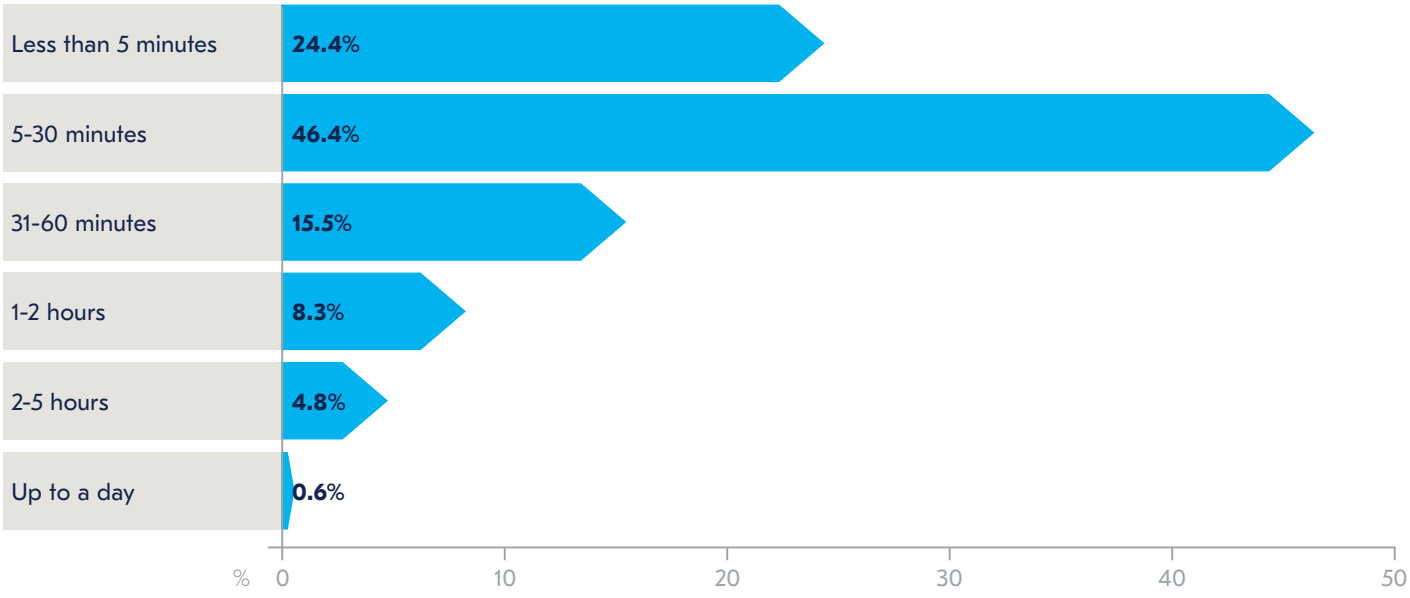


Figure 11. On average, how long does it take you to provide initial information on a crisis to top management?

Collaboration

Collaboration

- Organizations are moving away from messaging tools from the private environment (such as WhatsApp) to enterprise tools (such as Microsoft Teams).
- Organizations using secure messaging apps integrated into their Emergency Communication processes are most satisfied with their tool (60%), significantly more than those using enterprise messengers (41.1%).
- Virtual crisis rooms have seen their popularity rise during the pandemic due to increased remote working practices and are now being used by three out of five companies.
- Because organizations have had to collaborate remotely this year, the usage of tools such as Microsoft Teams has increased, leading to some organizations now using it as a temporary solution to emergency communications.
- With organizations using enterprise collaboration tools such as Microsoft Teams, Emergency Communications tools should ideally integrate effectively into existing tools and processes, whilst those in charge of implementing solutions should ensure existing tools and processes integrate effectively in the emergency communications tool solution.

Communications within the Crisis Management Team require different tools from communication with the wider organization. Within the Crisis Management Team, messenger tools from the enterprise environment (e.g. Microsoft Teams, Slack) and conference calls are the primary methods used for communication with 63.5% and 62.9% of respondents respectively using these tools.

Some interviewees explained that whilst they did not widely use collaborative software before the pandemic outbreak, they are now exploiting technologies such as Microsoft Teams which, in many instances, is also reducing the number of organizations that use tools such as WhatsApp for wider communications.

"People had been saying, 'Oh, there's this great thing called Teams, and we should use Teams.' And we were just starting to consider it. Now, because of COVID-19, there has been a massive change of culture and change of behaviour, and everything is Teams now. Everything."

Risk Manager, Education, Ireland

"We just got rid of WhatsApp and switched all comms to Teams. I've never been comfortable with the security side of WhatsApp and as everyone's using Teams all the time during the pandemic, it's made sense to switch to it as a better solution. Although we're formally recommending it for all departments, we've found most have just switched to it anyway. It's made life easier for me!"

Business Continuity Manager, Manufacturing, Austria

Whilst it could be expected that use of these tools will be high due to universal adoption across all machines in organizations, it might be expected that dedicated crisis management technology would have much less widespread use across organizations. However, this appears not to be the case: virtual crisis rooms and/or dedicated online collaboration tools for crisis management have been used by 57.5% of respondents. Given that slightly less (54.5%) report having used a physical crisis room during the past year, the role of the virtual crisis room has come into its own during the COVID-19 pandemic. Indeed, organizations which offer dedicated crisis room technologies have been major beneficiaries in industry awards this year: a virtual crisis management room which improved emergency care in difficult-to-access buildings won first prize in Indra's *Innovator* awards[4] whilst another tool, DACB Situation Room, helped win DAC Beachcroft the Business Development Innovation Award at the 2020 Legal Innovation Awards[5]. Although many crisis teams will have moved to a virtual environment as a direct result of the pandemic, we expect usage to continue even as the threat of COVID-19 begins to wane. Many organizations will have made significant outlay for new technologies such as virtual crisis rooms during COVID-19 and would want to continue to capitalise on the investment going forward.

In terms of keeping the process simple and cost efficient, some organizations might consider using tools that support across several areas, e.g. notification of staff as well as collaboration in teams and crisis handling. This has already proved to be a successful strategy in many organizations (see graph No. 5, page 22)

4. Various (2020). Intrapreneurs, key piece for job reconfiguration. Entrepreneur Europe, [online]. Available at: https://www.entrepreneur.com/article/362029 [accessed 15 January 2021].
5. Allnutt, H (2020). DAC Beachcroft's Cyber & Data Risk team scoops another award for its suite of digital crisis management tools. DAC Beachcroft, [online]. Available at: https://www.dacbeachcroft.com/en/gb/news/2020/october/dac-beachcroft-s-cyber-data-risk-team-scoops-another-award-for-its-suite-of-digital-crisis-management-tools/ [accessed 15 January 2021].

How do you organize collaboration in your core crisis team?

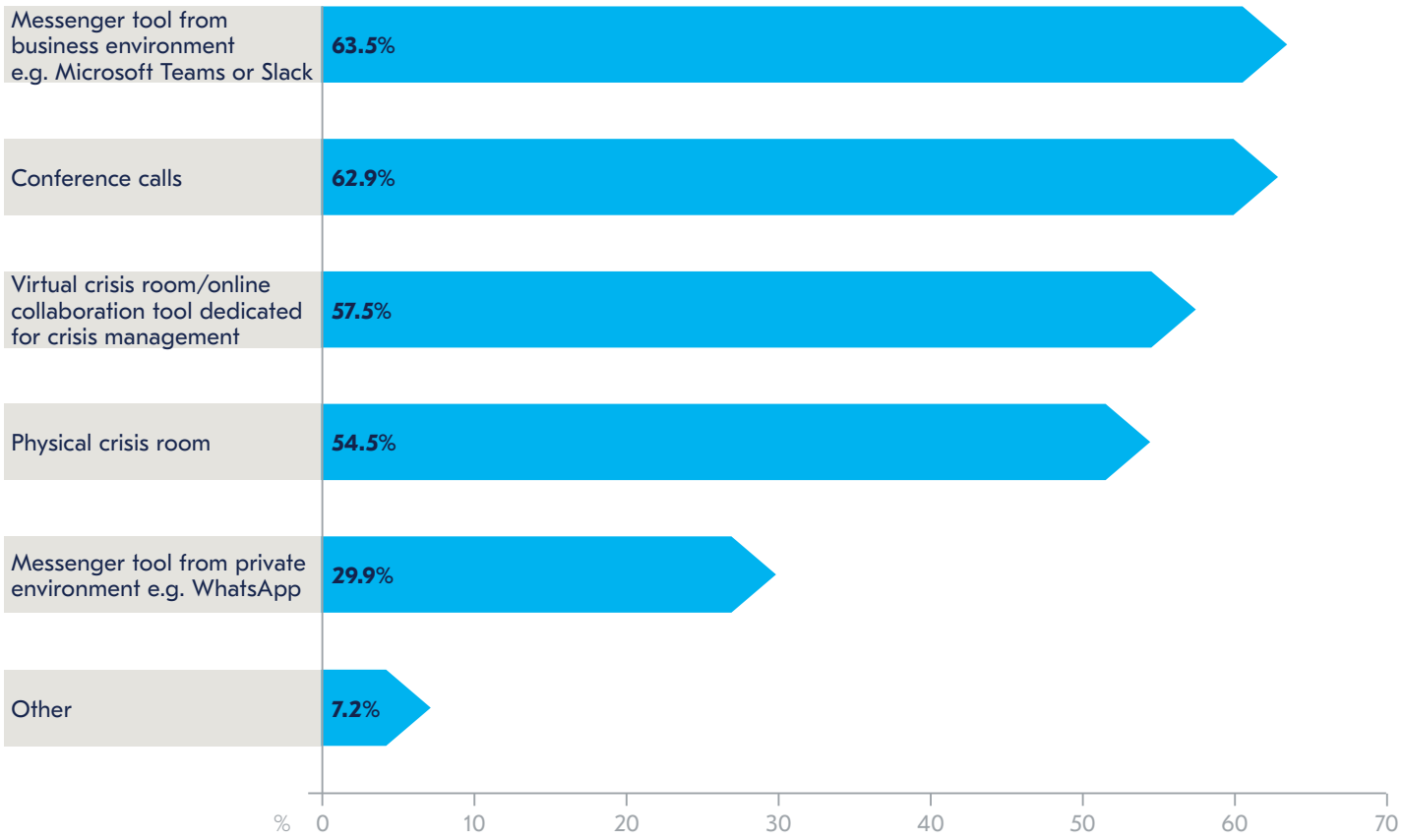


Figure 12. How do you organize collaboration in your core crisis team? Please tick as many as applicable:

As expected by the answers from other questions, the primary challenge for emergency communications management is the ability to gather, validate and share accurate information with 89.6% of organizations selecting this as one of their top two challenges. Communicating with staff is the second challenge for many organizations, with 83.6% selecting it as one of their top two challenges. Getting staff to follow planned procedures is the third rated challenge. All these challenges are obstacles that many organizations could resolve through increased training and exercising which organizations are hopeful of increasing as the pandemic starts to wane.

What are your key challenges during emergency notification/crisis management? Please select your top three challenges.

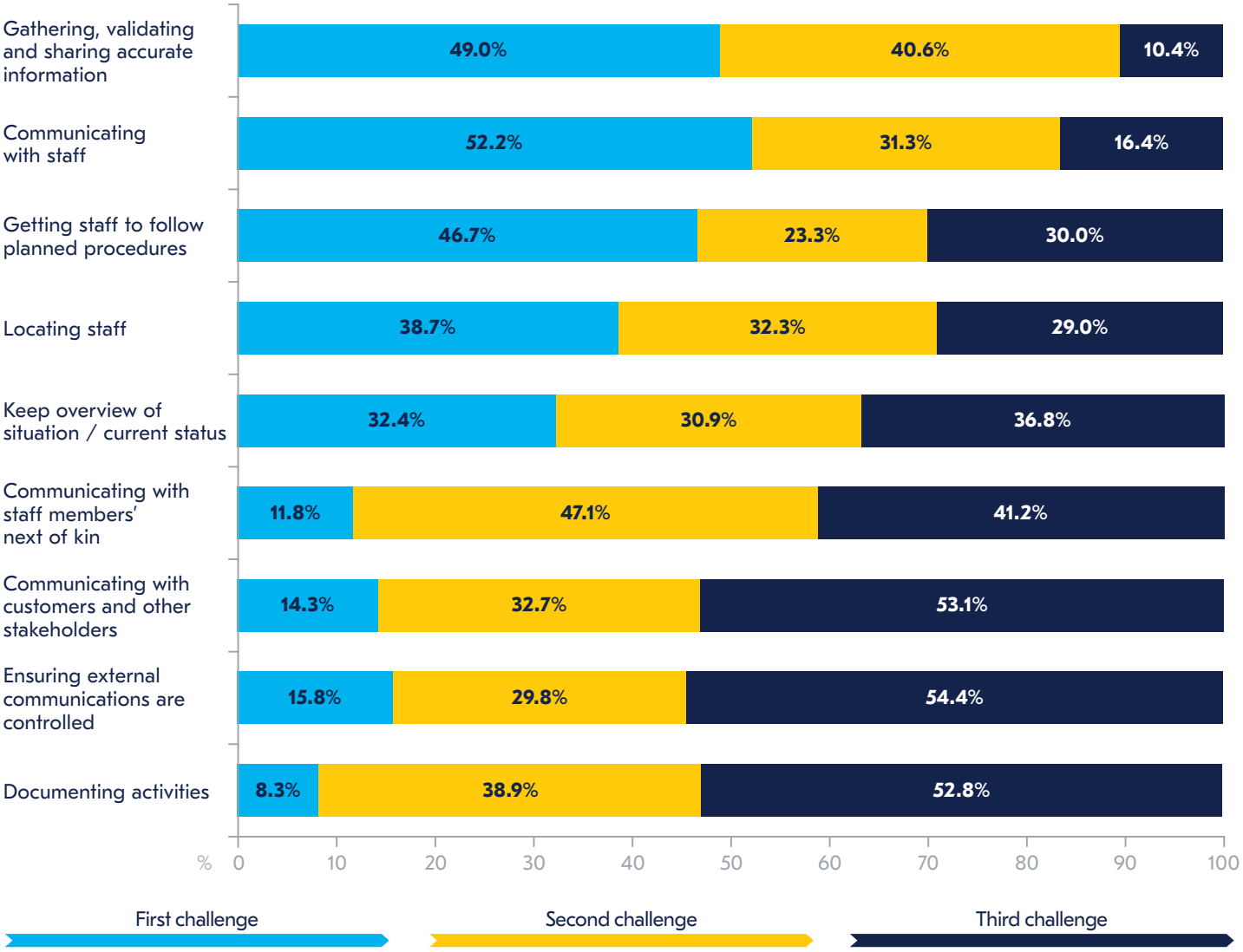


Figure 13. What are your key challenges during emergency notification/crisis management? Please select your top three challenges.

When it comes to primary messenger apps for communication in emergency scenarios, the most frequently used solution (43.5% of respondents) is enterprise messaging services such as Microsoft Teams or Slack. Just under a quarter (23.8%) use a secure messaging app which is integrated into their emergency communications solution with just under a fifth (19.1%) continuing to use free messaging apps such as WhatsApp. Some respondents reported that whilst communications during a crisis were handled by dedicated tools, tools such as WhatsApp were frequently used to support local or team-based transmission of non-confidential information.

An interviewee highlighted that in the tool used by their organization had created templates on the group text system which sped up communication during an incident.

"[During an incident], the chair of the emergency management team used her phone and either sent individual texts or sent a group text on the group text system. You'd compose it in advance: we'd already made readymade templates, 'Emergency management team meeting now, or in a half an hour,' and they'd be there. So that really works well, that's why we can activate our plans in less than five minutes because the templates would be prepared and you just slot in the date and time, and anyway we could also do by Teams as well. We would also give out similar alerts on Teams which were very effective."

Risk Manager, Education, Ireland

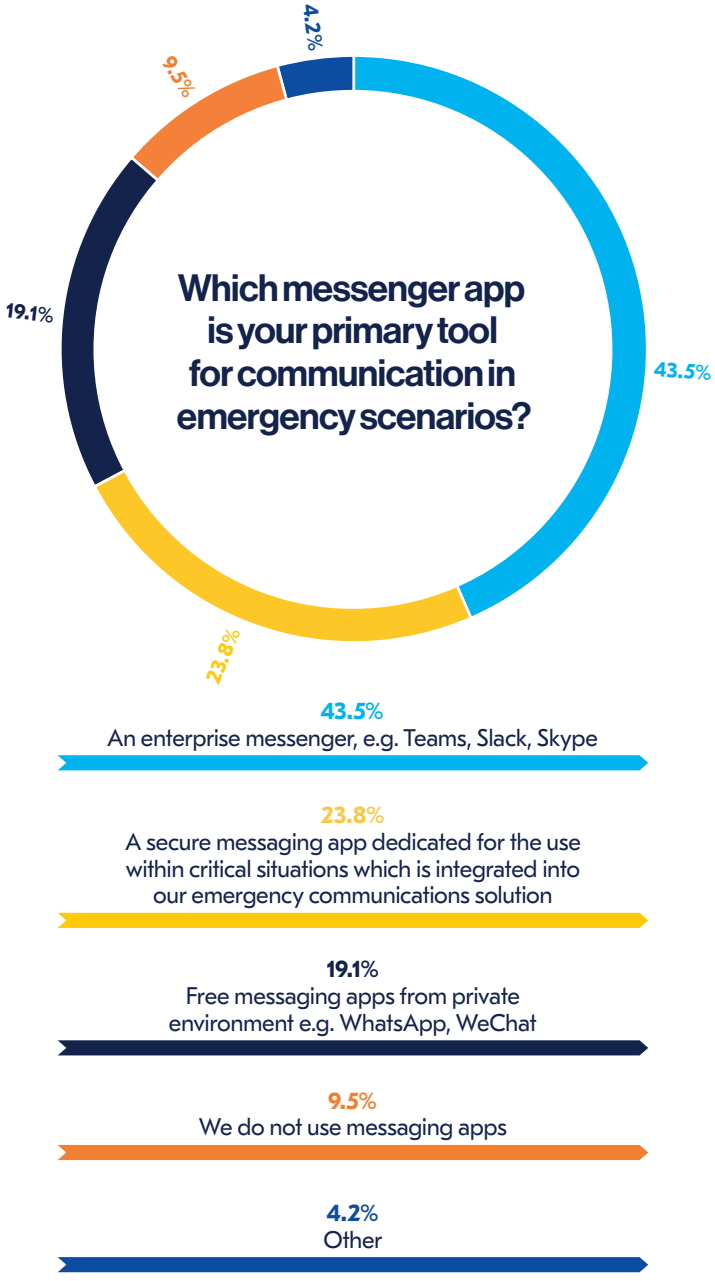


Figure 14. Which messenger app is your primary tool for communication in emergency scenarios?

Satisfaction with Tools

When it comes to the satisfaction of the messenger app during crisis situations, those using the secure messaging capabilities within their emergency communications solution are the most likely to be satisfied with their communications solution: 60.0% of users reported to be happy with just 2.5% dissatisfied. Despite some limitations within an emergency communications scenario, 41.1% of those who use enterprise messaging tools remained happy with the solution with 5.5% "not happy". Users of free messaging apps were the least likely to be satisfied with the solution: just 18.8% of users reported to be "happy" with this as their primary communication tool, with an equal number dissatisfied.

The limitations of free messaging apps — and also enterprise messenger apps to a certain extent — as an emergency communications tool have been highlighted over the past few years in the BCI Emergency Communications report:

a. The lack of confirmation to show whether a message has been delivered successfully or read leading to a lack of audit trail;

b. Confidentiality risks (e.g. staff forwarding information to outside parties or receiving information erroneously);

c. Messages being ignored as they became lost in a stream of messages;

d. Security concerns and data privacy;

e. Users becoming indifferent to messages within free tools due to the crossover with their personal life.

There is also the potential for the functionality of tools to be reduced or fail to work when there is a network outage or during times of peak use. Organizations have, however, become more aware of the limitations of free apps because of heightened communications taking place during COVID-19: interviewees told us how they had stopped using free tools and were instead turning to enterprise tools, with others already testing dedicated emergency communication tools to exploit the secure messaging capabilities.

Although dedicated tools offer the most functionality, there are examples where organizations have successfully adopted third-party tools to manage emergency situations very effectively, even though it is unlikely to replace a dedicating tool in terms of alerting capacity, for example. An interviewee explained how the organization had universally adopted the Google suite of products in the organization and used it during crises to set up Gold meetings, manage documentation and even obtain details of who has viewed particular information.

"Within five to 30 minutes of an incident occurring we have a gold meeting set up, and we tend to do that very, very well. I believe this is because, as a group, we actually use the Google Suite of products as part of that process. We have Chat and we use Forms as the platform for a document management system; we even have a learning management system within that. We can also use it to gather details of who's viewed a particular communication. Google Forms have also been invaluable in ensuring stock of PPE: we just had a Google Form that everybody in all our various different places throughout the country would access and complete their stock count in the morning. We'd then know exactly what levels they've got and the spreadsheet can be immediately reviewed in our bronze meetings."

Head of Safety, Health, Risk & Resilience, Security, United Kingdom

Are you happy with the messaging app you are currently using?

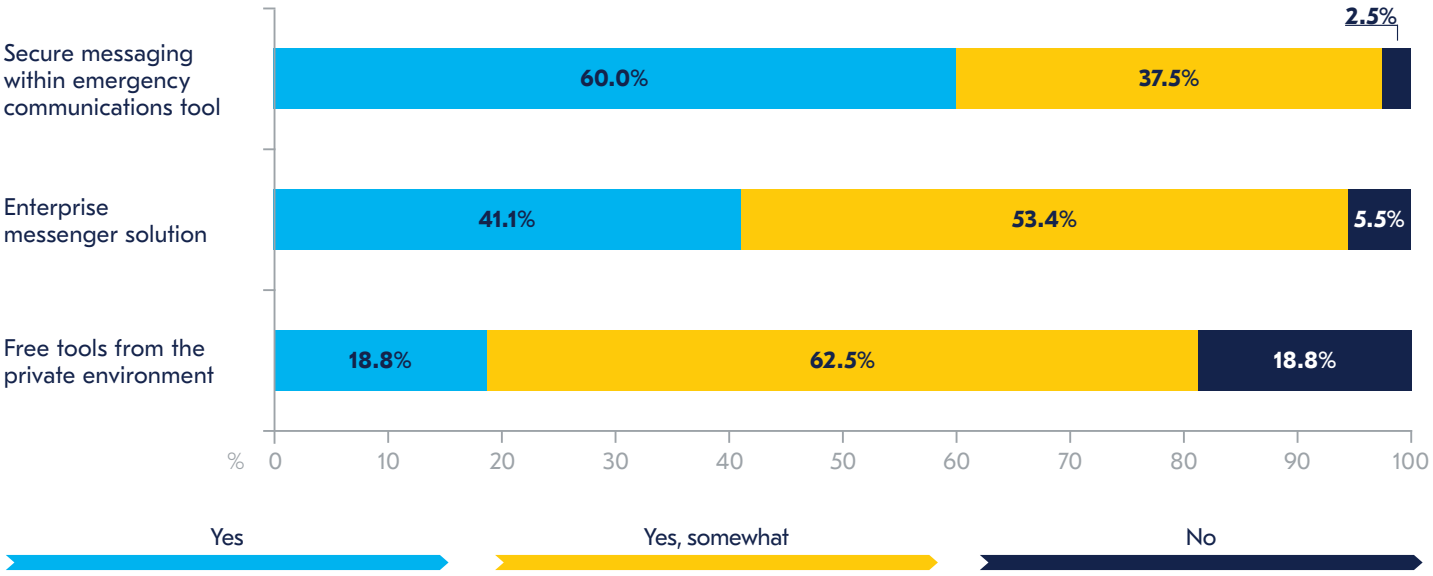


Figure 15. Are you happy with the solution you are currently using?

Functionality of Tools

Professionals were also questioned about the importance of certain aspects of functionality within their emergency communications tool. Interestingly, the pandemic this year has had little impact on the importance of various aspects of their emergency communications tool. "Constant exchange of information to enable decision making" and "enable expert teams to collaborate easily and in real time" take the top two spots once again, with 80.6% and 77.0% regarding this as "critically important" or "very important" aspects of their tools — a similar proportion to the previous year.

Collaboration during an emergency remains crucial to ensure a co-ordinated, multi-departmental response as well as ensuring that designated people across the organization can be kept informed of the situation and action effective responses in their geography or in their departments.

One of the aspects which is rated lower than might be expected is "integration with other apps/technology used by the organization". Interviews this year revealed that some professionals were frustrated that emergency communications technologies were not being used effectively by staff — particularly by senior management — due to being not well integrated into existing systems on installation or due to a lack of understanding by staff. Whilst some organizations had managed to get round this by holding company wide campaigns, others found staff "lapsed" into using non-dedicated technologies such as Microsoft Teams within emergency scenarios.

Others found the cost and/or required staff time to implement a new tool prohibitive. An interviewee highlighted that they had explored the viability of continuing use of a new tool during COVID-19, but the cost, coupled with the training required to l earn a new platform, made its continuation prohibitive.

"The cost of the Software-as-a-Service solution was very high annually. Our budgets are all restricted at the moment, too. We had to keep everything updated on it. It all sounds very simple, but you still need a person to take responsibility for it and it just didn't work. I'm not disparaging the product or the idea, but when push comes to shove, Microsoft is king and everybody is familiar with Teams, everybody knows how to use Microsoft applications and you use the same password to get into it instead of having a new password for a different system."

Risk Manager, Education, Ireland

"The Software-as-a-Service system was also not compatible with Microsoft so any technical issues required us to get them to sort it instead of our own computer/IT services staff. I know a lot of Microsoft now has gone into a cloud as well and you don't necessarily get your own guy doing it, but universities very much approach things on a 'do you know a colleague in the computer centre who can drop down and fix it for you now?' type approach. That works for Microsoft products but not for a different platform. We also gave an inhouse helpdesk but they don't know non-Microsoft applications."

Risk Manager, Education, Ireland

COVID-19 has resulted in changing requirements for tools

Survey respondents were also asked if their way of using an emergency communications software/application had changed as a direct result of COVID-19. There were several themes that arose:

1. **The requirement for a fully automated tool:** Respondents commented that staff absences or increased remote working meant there had been times when a response had not been as quick as hoped. Using a fully automated tool would have helped prevent such a slow response.
2. **Importance of good information:** One respondent said that COVID-19 had resulted in an overload of "uncorroborated fake news" that was difficult to filter. The ability of a tool to share accurate information from fully corroborated sources was more valued than in previous years.
3. **Adaption of tools for remote working:** With many organizations invoking remote working this year for all or some staff, many found they were having to use tools differently this year. Without staff being in the office, the need for an audit trail for communications was more valued than before. Also, for those companies where staff were able to opt in, location-based services were being used more readily to help organizations to locate staff effectively in the event of a COVID-19 outbreak, for example.
4. **Movement to SaaS:** Organizations were increasingly moving to SaaS-based tools this year as software was easier to manage across multiple platforms, particularly when staff were off site and, in some cases, using their own devices for working. Cloud-based technologies meant tools could continue to be used as there was often no need to install additional software on machines. This tallies in with the evidence of this report which shows a sharp increase in the use of SaaS-based tools in 2020.
5. **More budget:** The idea of being able to get more budget may come across as surprising to some in a year where organizations have been working harder than ever to ensure strong balance sheets when faced with the challenge of COVID-19. Research carried out for the BCI's The Future of Business Continuity and Resilience[6] report however showed that the importance of Business Continuity, Crisis Management and other resilience disciplines had been showcased to the Board as a direct result of the pandemic. Many practitioners reported they had had budgets increased this year as a result.

An interviewee reported that one of the major changes they had made during the pandemic was with their decision log: the log had served as a learning tool of the various steps adopted throughout the pandemic as the organization sought to follow guidance from national and local health authorities. This would impact into communication strategy going forward.

> **"The decision log has seen major change: our pandemic flu policy has changed in line with all of our lessons that we've learned. The decision log is now being used as almost like a learning tool of the various steps that we have gone through in line with the Public Health England and Public Health Wales guidance that has come out."**
>
> Head of Safety, Health, Risk & Resilience, Security, United Kingdom

6. BCI, The (2020). The Future of Business Continuity and Resilience. The BCI. Available at: https://www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html [last accessed: 15 January 2021].

How important are the following aspects for your alerting and emergency communications? (Scale 1-5)

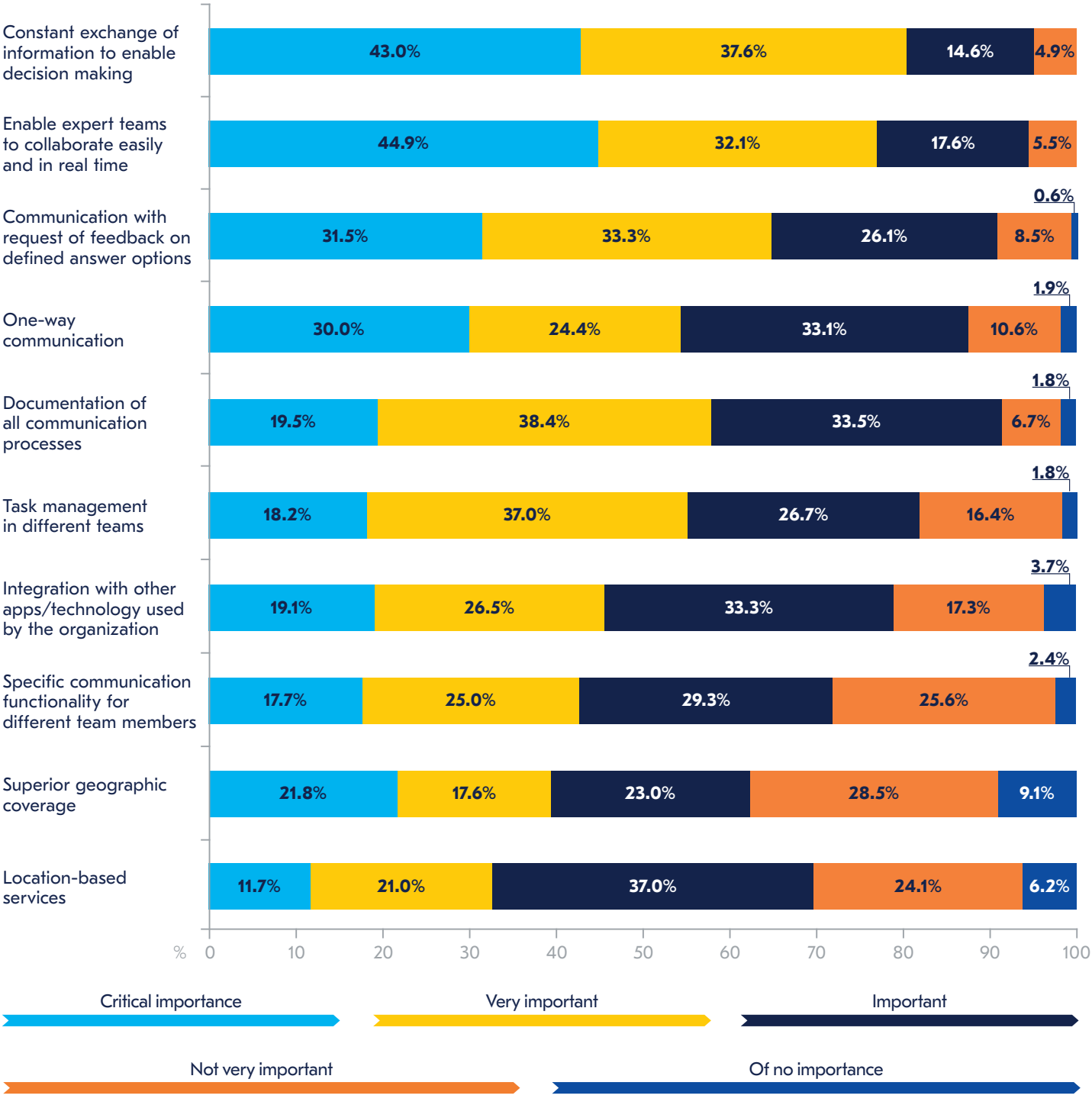


Figure 16. How important are the following aspects for your alerting and emergency communications? (Scale 1-5)

Despite the rising popularity of specialist messaging apps for emergency communications, 62.7% of respondents claimed to either "not" be happy or only "somewhat happy" with the actual messenger app they are using, showing that there is considerable room for improvement of applications used for emergency communications in organizations.

The cause for most disappointment was the lack of integration with alerting scenarios: 49.0% of the group of respondents who were not happy or only somewhat happy reported this as a reason for their dissatisfaction. As noted earlier in this report, interviewees for this project reported that they were dissatisfied with the inability to integrate tools into their own suite of products, whereas others reported dissatisfaction with tools' ability to directly integrate into specific emergency scenarios with their own organizations. An anonymous respondent summed up these sentiments succinctly within the survey: "[It is] difficult to integrate alerting tools, communication tools, and BC tools under one hat." This shows that there is a need for solutions supporting across several of those areas simultaneously and being integrated with each other seamlessly.

A lack of functionality was cited by 39.8% of respondents, increasing to 61.5% for those who did not use a dedicated emergency communications tool within their organization and rely on enterprise messaging apps or tools from a private environment. Data protection issues was also a concern for those without specialist applications: 86.7% for those who did not use specialist emergency communications tools expressed concern over data privacy.

A further concern which has come to the fore this year is global adoption: 14.3% of the "somewhat" or "not" happy group said that different tools were used in different countries which meant their emergency communications were difficult to manage on a global basis. The "Other" responses also highlighted issues in this respect, too: users in some countries (such as China) were unable to open messages, whilst others reported that different communication styles in certain geographies were incompatible with the solution employed by the organization. Global adoption was also inhibited by lack of population coverage by networks in certain geographies.

In some organizations, multiple systems were in use across different departments which lead to compatibility issues and the tools unable to work in tandem. Frequently, organizations were aware of the issues but changes to incumbent departmental policies were difficult to change or enforce.

"Our first problem is that we have business continuity software which is not integrated with our emergency response or emergency agent system. We have two different tools which do not talk to each other. The second problem is that production leaders have WhatsApp groups and they communicate using these groups. This is very efficient, although it is obviously not the official tool and can cause security breaches."

Business Continuity Manager EMEA, Manufacturing, Belgium

Why are you not or only somewhat happy with your current messaging app?

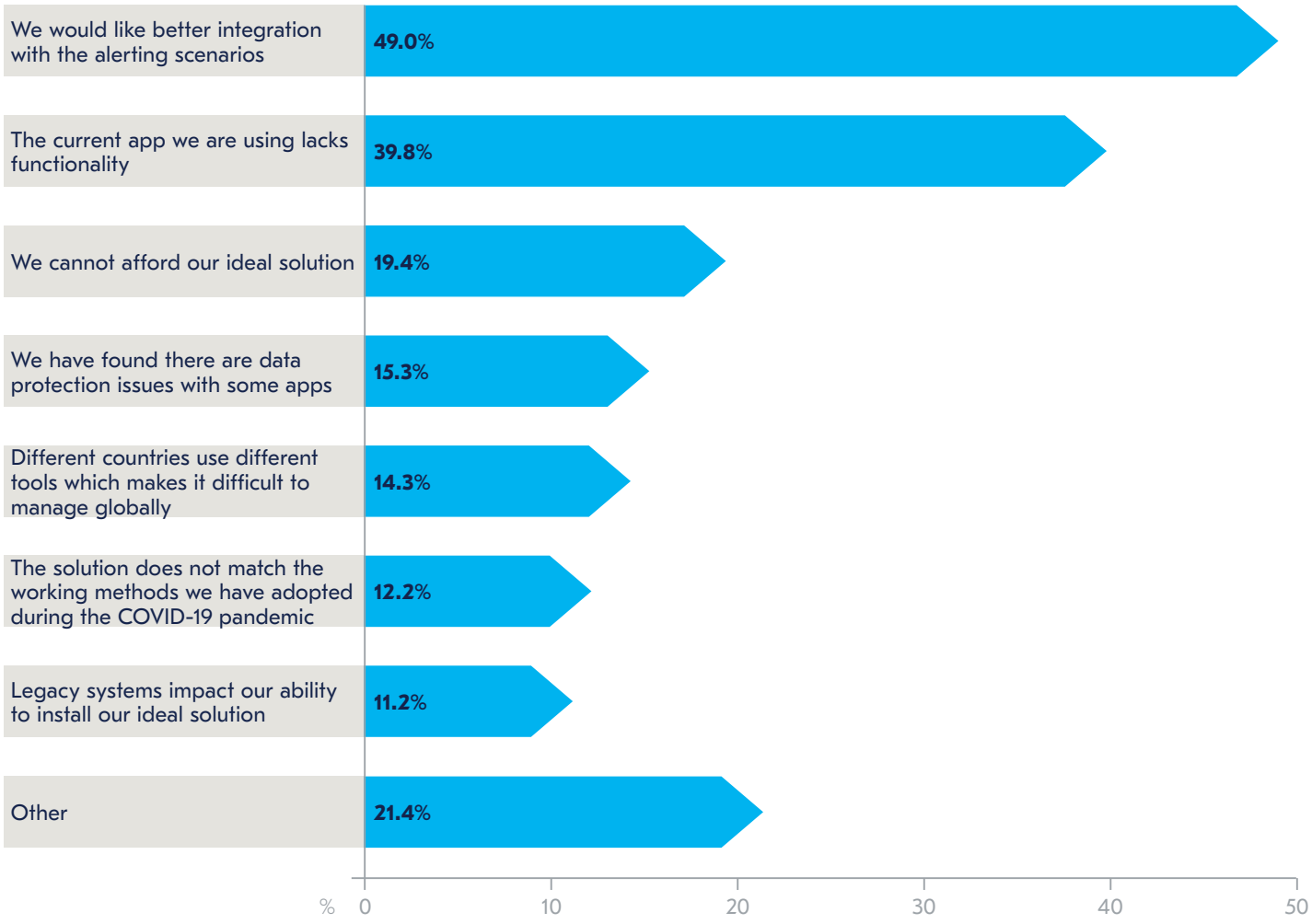


Figure 17. Reasons why respondents were only "somewhat happy" or "not happy" with their current messaging app

Incident Preparedness

Incident Preparedness

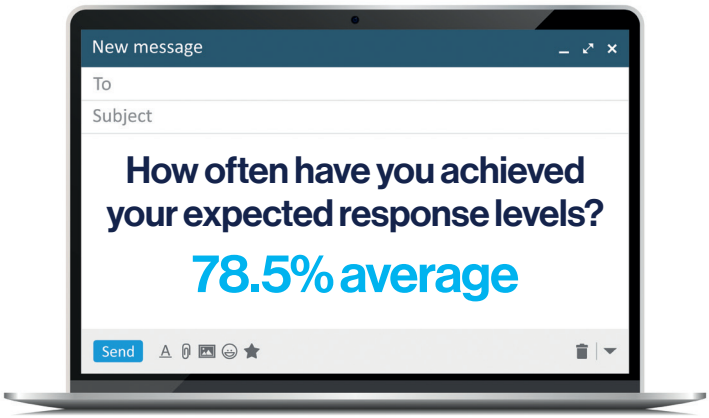
- **The number of organizations able to achieve their expected response times has risen for the fourth year in a row to 78.5%.**
- **A lack of up-to-date staff contact information and a lack of understanding by staff are still the primary reasons for response levels not being met.**
- **Senior Management are frequently the failure point in many organizations: many have been involved so heavily in the COVID-19 response, they have not attended training sessions.**
- **Excel continues to be heavily used by organizations to store contact information which not only leads to poor reliability of information but has GDPR and data security implications.**

Despite the challenges 2020 has brought, the number of organizations who have been able to achieve their expected response levels has risen for the fourth year in a row to 78.5% (2019: 73.1%). Whilst some of this increase can be attributed to the additional investment in emergency communications tools and technologies and an elevated interest in training and exercising, some of this will also be down to the type of incidences which organizations have experienced this year. With many staff working remotely in 2020, the challenges which an organization may experience in a typical year (such as damage to office premises after a hurricane, an office IT or telecoms outage) have had less impact in many organizations.

Despite the positive trend, however, interviews highlighted that organizations had experienced delayed response times due to staff working remotely and not actioning messages in a timely response. Many organizations have already worked to rectify this problem however, whilst others reported that staff had been more reactive during the pandemic due to a heightened awareness of emergency procedures because of the pandemic.

"We'd normally only get say 50%, maybe 60%, replying when we sent out a bulk message from our system. People are scared of COVID-19, really scared, and now when we send out a message we get responses into the 90% region. We've also run some campaigns for people to update the system with their private contact details and a lot of those who refused before are now adding them."

Crisis Manager, Engineering, Australia



Previous editions of this report have showed how it is frequently human error, rather than technology error, that causes failure of communication during an emergency. This year, the same trend has continued. For those respondents who reported they had failed to meet their emergency communications response targets, 42.4% said it was due to a lack of understanding from participants and 38.6% was because of lack of accurate staff information. These two reasons have remained at the top of the table for the past three years, although the top two choices are reversed compared to last year.

A lack of understanding from participants suggests a lack of training of staff, as well as a lack of engagement. This year, interview respondents suggest that as training had had to be run remotely, staff had been less engaged, and many had not attended sessions due to being heavily involved in the organization's response to COVID-19.

"We tried doing some training on [Google] Hangouts but hardly anyone turned up, which was a shame. Particularly Management who are so worried about keeping the business going, they don't want to commit time to things like training. We'll pursue it as we begin to recover but for now, we can continue to run, try and make it clear how important they are, and hope people turn up. Far from ideal, but we are doing our best."

Crisis Manager, Engineering, Australia

One interviewee reported that, for a response to be effective, staff needed to be able to be confident working autonomously and be comfortable using technology; being prepared to learn where required. In many instances, it was senior management who became the stumbling block and were most likely to require handholding through the process. Such difficulties highlight the need to ensure that training and exercising should be a mandatory requirement for all senior staff.

"It's been quite a time for me in Business Continuity because it's made people aware of the need to be capable of working remotely and be resourceful. Unfortunately, some people haven't been that resourceful, and they needed a bit of handholding through. However, nine-tenths are the more senior people in the organization. They often don't seem to be able to think for themselves when it comes to IT."

Operational Resilience Manager, Financial Services, United Kingdom

"A lot of the capability of software depends on the comfort zone of the senior management team with technology. Are they comfortable to have this application on their phone without having somebody beside them to show them which button to press? They're not all tech savvy."

Risk Manager, Education, Ireland

The lack of accurate staff information continues to be a major issue, with many organizations still relying on resources such as Excel to store staff information. Whilst Excel is an easy tool to use, respondents claimed that information was not updated regularly enough and multiple versions of the same spreadsheet were often created. As well as leading to communication challenges, this also poses data privacy and GDPR concerns.

The first technical challenge — unavailability of mobile network — was only cited by 24.2% of users as a reason for failing to meet response targets with internal IT failure a problem for 16.7% of users. Interestingly, despite previous questions showing that global compatibility between local emergency communication solutions was a problem for some, problems communicating internationally was only cited as a reason for failure in 10.6% of cases with language barriers the least likely cause for failure at just 9.1%.

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

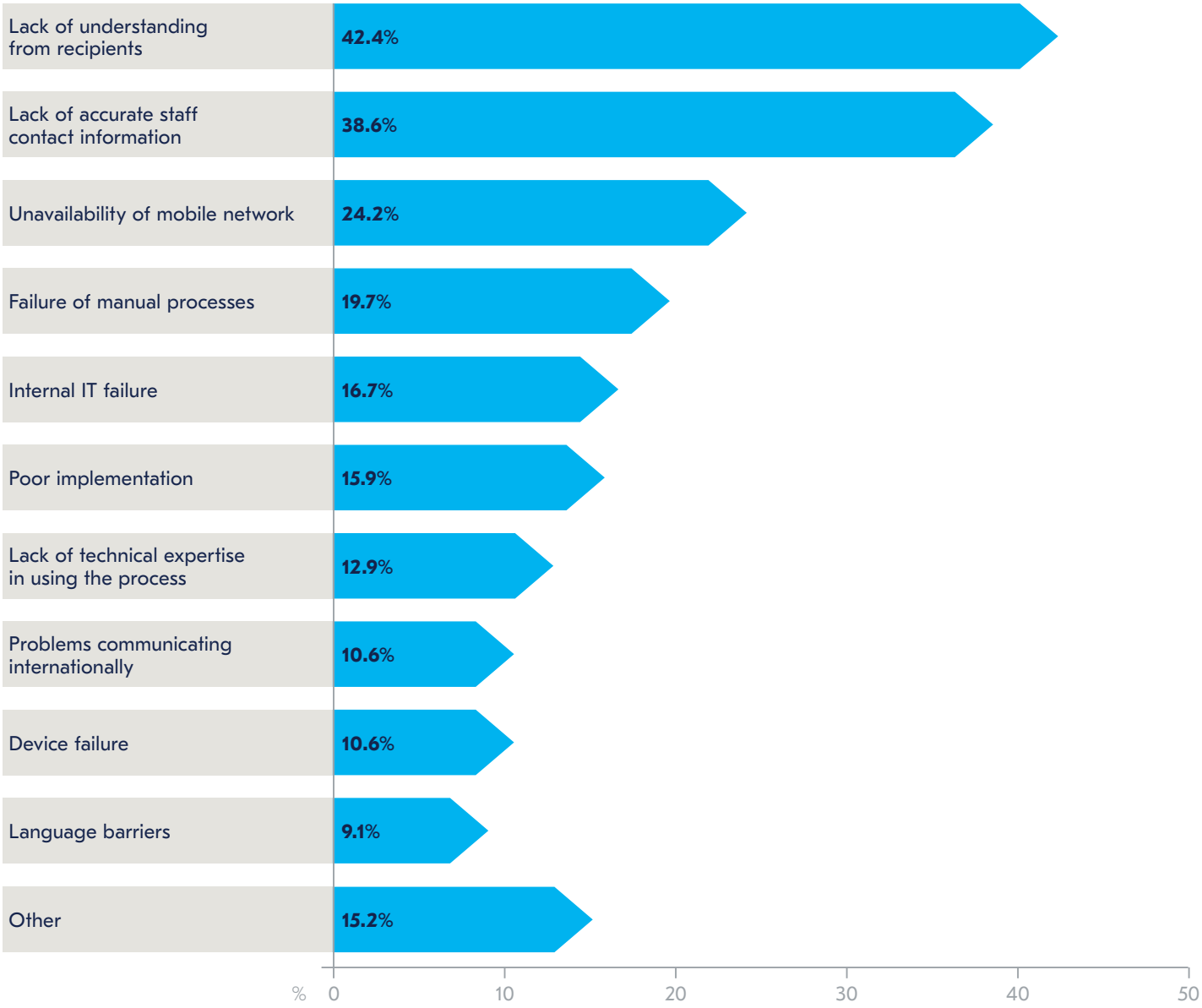


Figure 18. If you failed to achieve your accepted response levels, what caused the failure? Tick as many as applicable:

Exercising Emergency Communications Plans

Exercising Emergency Communications Plans

- **Despite being a difficult year, nearly three quarters of organizations have still been able to carry out training for emergency communication plans at least every twelve months.**
- **Carrying out so many "real life" activations of plans this year has resulted in many organizations feeling less of a need to carry out exercising.**

2020 has been a difficult year for most organizations, but nearly three-quarters have still been able to carry out training programmes for emergency communication plans at least every twelve months: 16.7% have carried out training at least every three months, 19.2% every six months and a further 37.2% every year. Such frequency of training will be responsible, at least in part, for the improved activation speeds of emergency communications response times noted in this year's statistics as well as leading to a more effective response.

Although many organizations have had a significant proportion of staff working from home in 2020, these statistics show that the lack of ability to carry out face-to-face training has far from inhibited organizations' ability to run training programmes. Those interviewed for this report said that Management had been actively requesting for more training to be carried out because concerns about the cascading of information during COVID-19, whilst others had received extra funding this year for new tools and software (primarily as a direct result of COVID-19) which had required them to carry out additional training programmes.

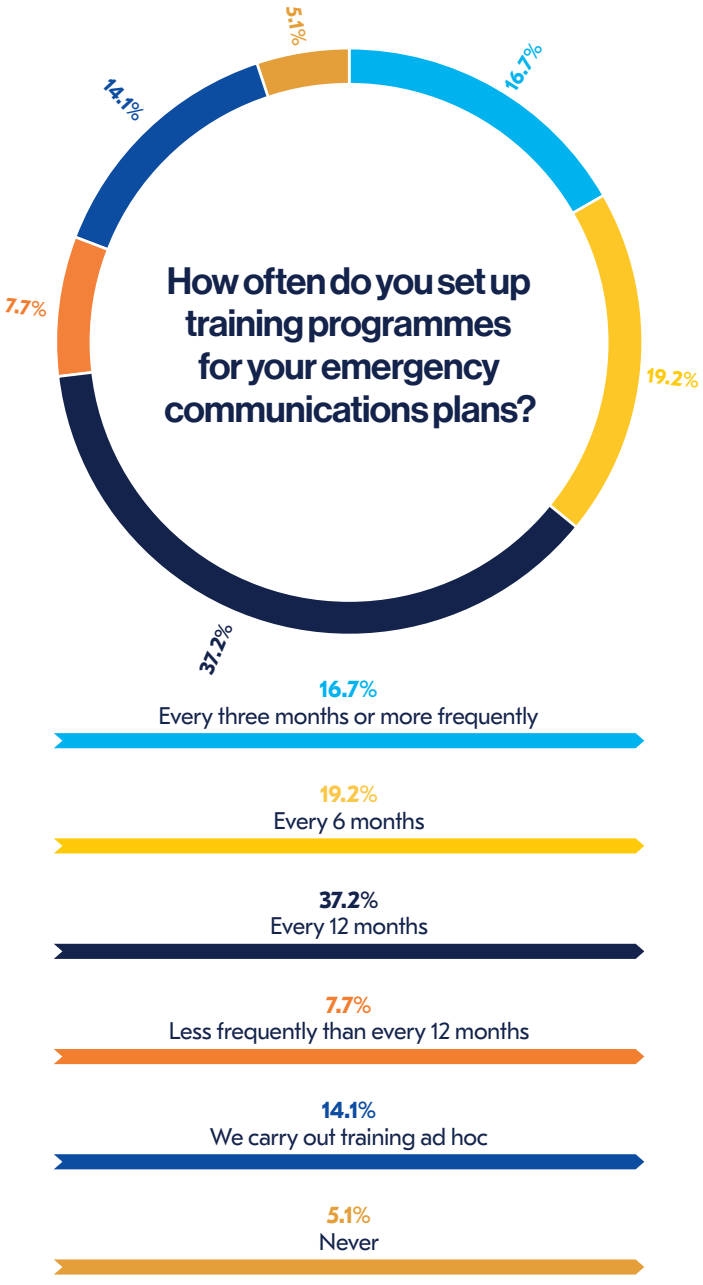


Figure 19. How often do you set up training programmes for your emergency communications plans?

Many organizations have had to activate their emergency communications plans more frequently this year because of COVID-19: new infections occurring in the workplace or critical suppliers no longer being able to meet contractual requirements, for example, have led to an increase in the use of emergency communications systems.

Whilst this has had the benefit of uncovering flaws within plans, it has also meant that staff have become better trained as a result of real activations. Many organizations have used these "extra" activations as a springboard to refining their emergency communications plans and providing additional training to staff. Nearly a quarter (24.5%) also carry out additional training after an incident has occurred, with a further 43.2% carrying out additional training after an incident if it is required. 15.5% claim to do this "rarely", with only 16.8% saying they "never" carry out additional training. Some respondents revealed in interviews they had been carrying out less scheduled training this year because their plans were having to be activated so frequently they did not believe it was needed.

"Some of the reason for not joining the online session was probably a bit of a fatigue with real incidents occurring and having to follow procedure. We've probably had to activate our plan five or six times in the last six months, so that's more than made up for the lack of training. We are looking to change things after the pandemic which will require training, but for now we are hopeful that so many activations mean everyone knows what they have to do."

Crisis Manager, Engineering, Australia

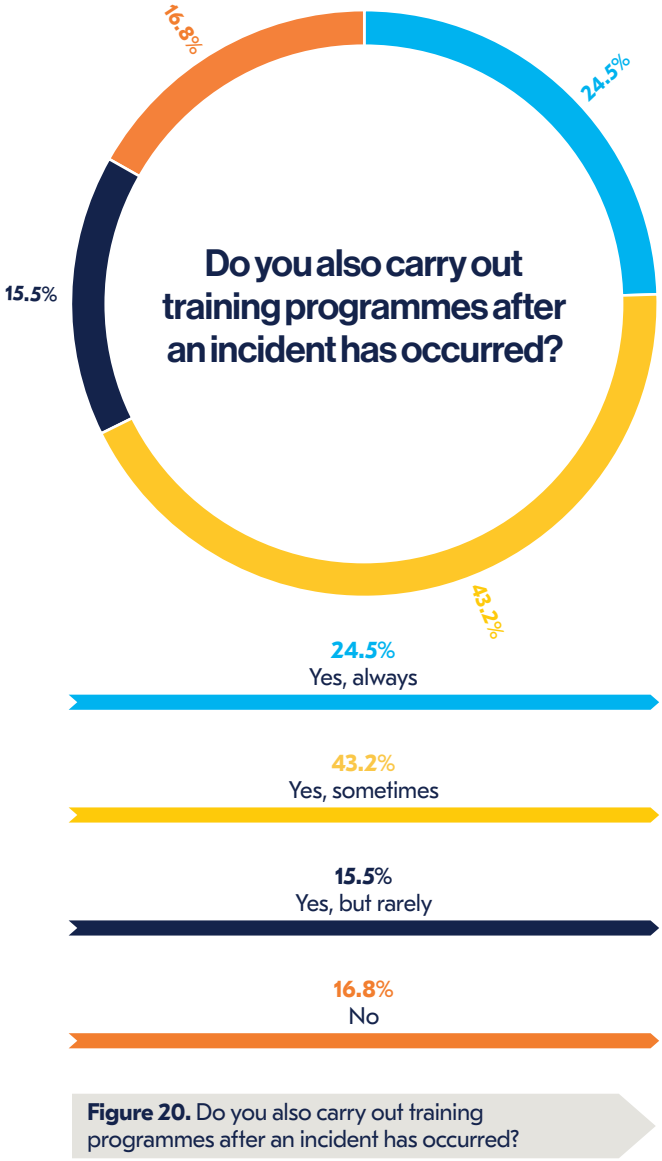


Figure 20. Do you also carry out training programmes after an incident has occurred?

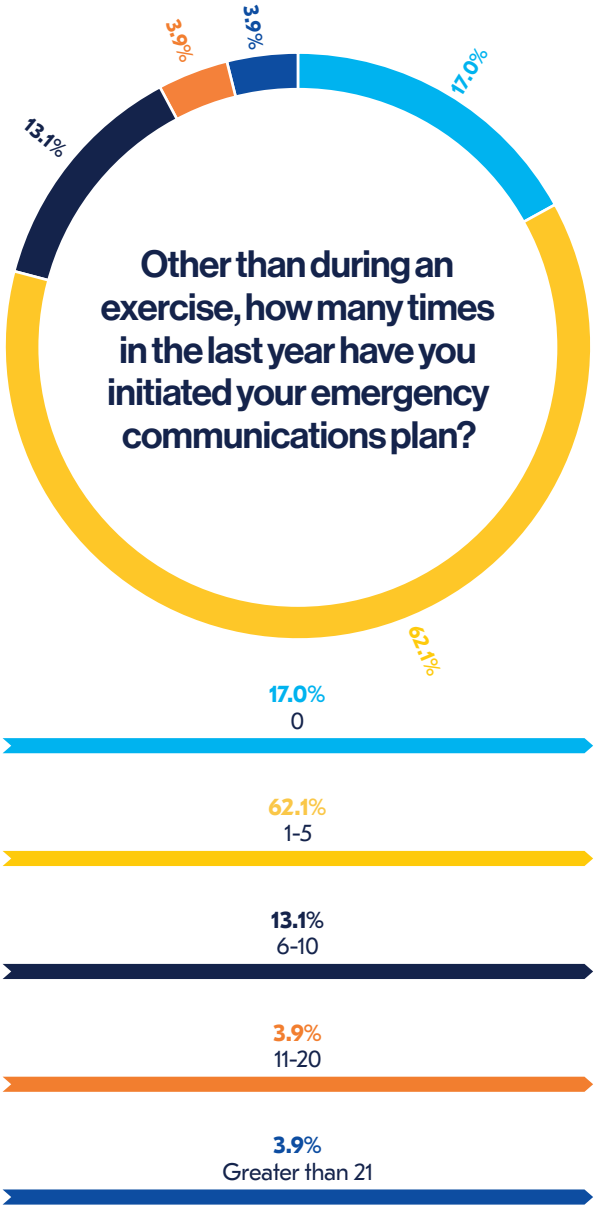


Figure 21. Other than during an exercise, how many times in the last year have you initiated your emergency communications plan?

Indeed, the figures show that whilst the number of organizations who had activated their plans five times or less fell slightly in 2020 to 79.2% (2019: 85.2%), the number of organizations who activated their emergency communications plans *more* than five times a year increased to 20.9% (2019: 14.9%). Those interviewed said that whilst they were having to activate their plans for site-related issues less frequently this year, COVID-19 had been the cause of multiple activations over the course of the year.

Exercising of plans has been impacted in a similar way to training this year. Whilst the number of organizations who carry out training at least once a year has remained stable between 2019 (82.2%) and 2020 (82.3%), the number of organizations who have exercised their plans more frequently than twice a year has fallen this year to 39.9% (2019: 53.2%). As mentioned in the previous section, many organizations felt they had less of a need to run training programmes this year because plans were having to be exercised so frequently in real life situations.

Nevertheless, many organizations continue to be mandated to carry out training at least once a year: guidance from NHS England, for example, is that NHS Trusts carry out a communications exercise at least once every six months[7] whilst the International Air Traffic Association (IATA) recommends exercising plans at least once a year but ensuring that plans are reviewed and updated every six months[8].

Aside from this, nearly one in five organizations (17.7%) exercise their plans less than once a year. Failing to exercise plans mean problems will fail to be identified and is more likely to lead to failure when a plan is activated. Indeed, the BCI's Good Practice Guidelines highlight how exercising should be an ongoing process as part of an organization's overall 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

Although some organizations are reporting Management are requesting more exercising because of COVID-19, some organizations are still encountering significant difficulties when trying to run exercising as people do not make themselves available for exercising. Whilst private organizations may find it easier to mandate exercising for all staff, organizations such as universities encounter very real challenges due to the number and variety of people on site e.g. educational staff, operational staff, Management, students.

> **"We don't want to do any exercises on communications alone even though we probably should, but we haven't done that yet. And we do try to: we had a period where we hardly any scenario training at all because people weren't available. Then we set up a plan and said we were going to carry out x number of exercises per year but that's got completely scuppered now with COVID-19. Since COVID-19 we haven't had any scenarios about anything else because COVID-19 has just taken over the university and the whole world. It's not enough, but that's all we can do. We might do a debrief but our training could be better."**
>
> Risk Manager, Education, Ireland

7. Emergency Preparedness Alliance & Response (2019). NHS Core standards for emergency preparedness, resilience and response guidance. NHS Publication, [online]. Available at: https://www.england.nhs.uk/wp-content/uploads/2019/07/core-standards-for-eprr-guidance-v5.0.pdf [accessed 15 January 2021].
8. IATA (2018). Crisis communication and reputation management in the digital age: A guide to best practice for the aviation industry. IATA Guidance Document, [online]. Available at: https://www.iata.org/contentassets/86b7f57b7f7f48cf9a0adb3854c4b331/social-media-crisis-communications-guidelines.pdf [accessed 15 January 2021].

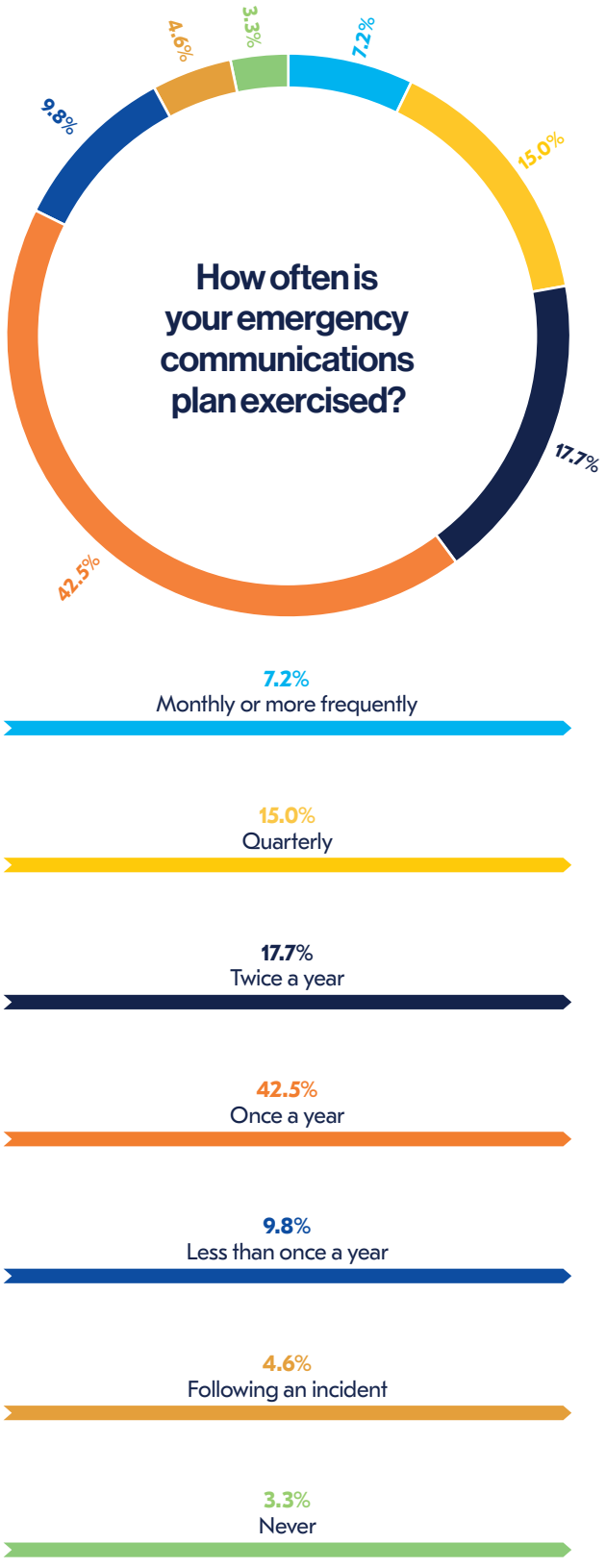


Figure 22. How often is your emergency communications plan exercised?

However, whilst some organizations have not felt the need to carry out as much exercising this year, others have carried out additional exercising for the same reasons organizations have been carrying out additional training programmes: new plans and policies have been put in place in many organizations resulting in the need for additional exercising to be carried out, others have had Management take a greater interest in training and exercising programmes which has resulted in investment in new tools and software which requires additional exercising and working from home has meant organizations have had to ensure plans are failsafe in a remote environment.

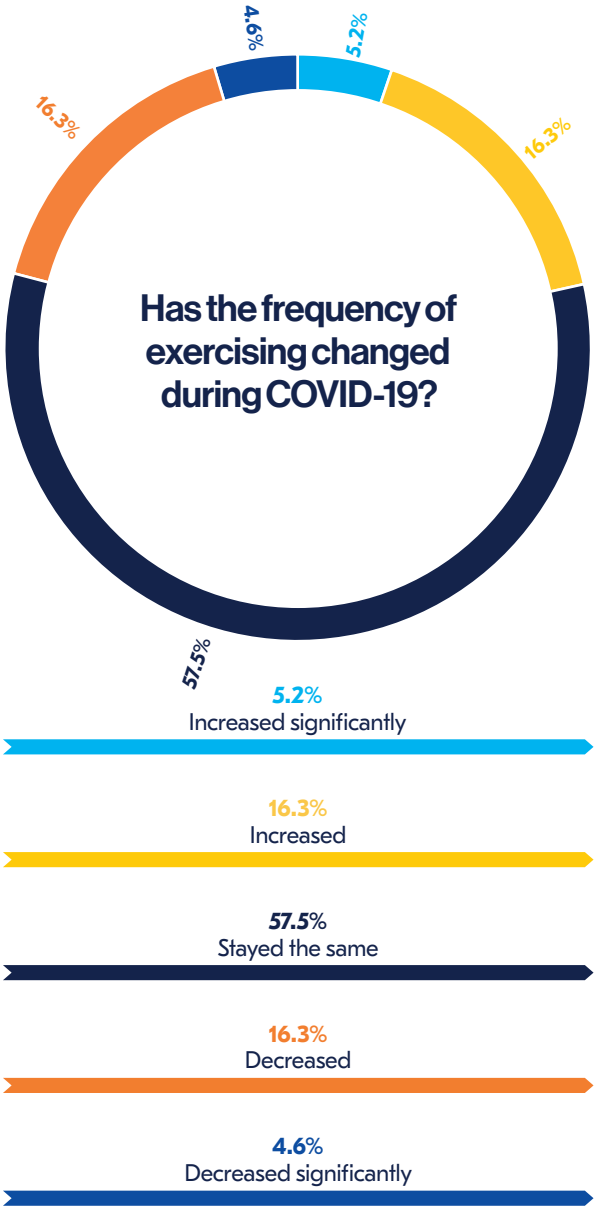


Figure 23. Has the frequency of exercising changed during COVID-19?

International Travel

International Travel

- 97% of organizations cancelled work related travel because of lockdown measures in 2020.
- This has meant many staff travel policies (including safeguarding travelling staff) have not been reviewed during the year.
- For organizations where staff travel has still been happening, many organizations have updated their policies accordingly and included guidelines for COVID-19-safe travel.

International travel has been a feature in the BCI Emergency Communications Report since its inception. Travelling staff place additional demands on emergency communications systems and processes: staff may be travelling to regions where network coverage is minimal, others may be travelling to high-risk countries where additional security procedures may need to be implemented, some will need to ensure their own software will work effectively with local systems and, in some circumstances, some emergency communications solutions may not be allowed to be legally used in some geographies.

Survey respondents reported that on average in a normal year, 22.5% of staff would travel internationally. This year, however, most organizations have halted staff travelling internationally due to COVID-19.

A survey of HR executives by Gartner revealed that 97% of organizations cancelled work-related travel because of lockdown measures[9], figures which tally with the BCI's Coronavirus — Organizational Preparedness reports in Spring 2020. There has therefore been less focus this year on ensuring that emergency communication plans are effective for travelling staff, and more on ensuring staff can be contacted when operating in remote environments.

However, with vaccines now being delivered across the globe, the possibility of business travel becoming a reality again is becoming greater. This means organizations will start to look again at the risk profile of the countries they are travelling to. Interestingly, the COVID-19 pandemic has increased the number of countries which organizations consider to be high risk: in 2019, 46.9% of organizations said they have staff travelling to high-risk areas. This year, the figure has increased to 60.1%.

Does your organization consider some or all of the countries they travel to as high risk?

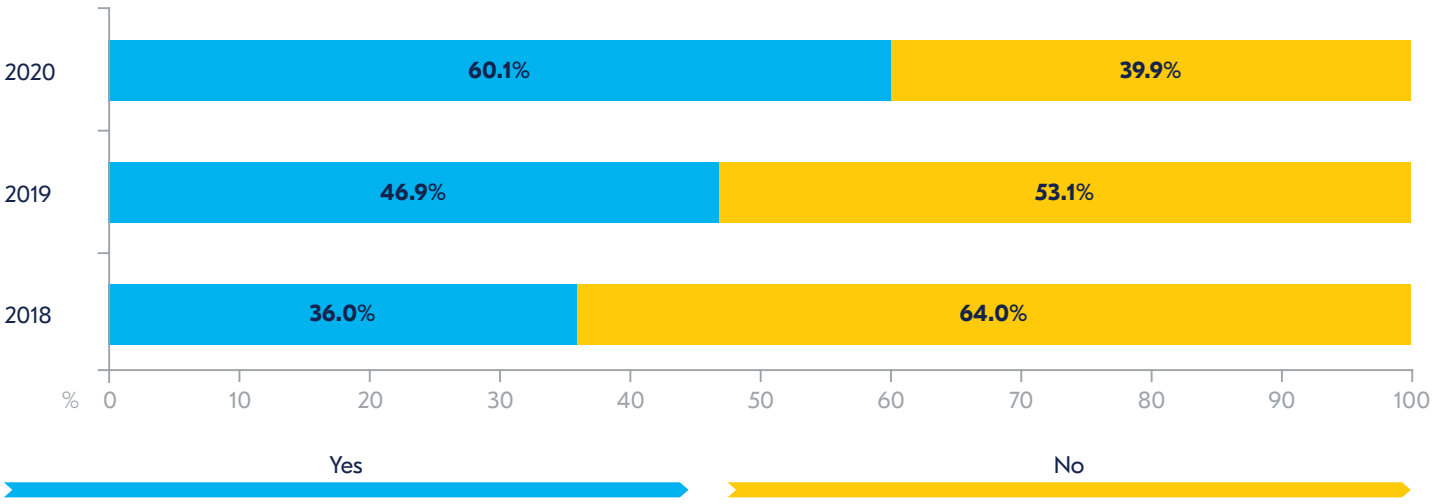


Figure 24. Does your organization consider some or all of the countries they travel to as high risk?

9. Baker, Mary (2020). Gartner HR Survey Reveals 88% of Organizations Have Encouraged or Required Employees to Work From Home Due to Coronavirus. Gartner [online]. Available at: https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88--of-organizations-have-e [last accessed 15 January 2021].

Furthermore, 83.9% of organizations admitted that their organization's view of high-risk countries had increased because of the pandemic. Although such a result is to be expected due to the global impact the pandemic has had, it is likely that COVID-19 will prompt many organizations to review the risk profiles on countries staff are travelling to. The same was evident in last year's report: the Venezuelan crisis, Hong Kong protests and isolated terrorist incidents in Europe and North America had all lead to organizations becoming more aware of the dangers of staff travelling to certain destinations.

We would therefore consider it likely that organizations will start reviewing how their emergency communications software and tools can help to support them for travelling staff as restrictions start to be lifted. Tools such as geofencing, for example, are likely to see more interest as organizations seek to track the location of staff. Even as the threat of COVID-19 starts to wane, organizations are likely to look for tools which will help travelling staff to access pertinent information such as hyperlocal data regarding diseases.

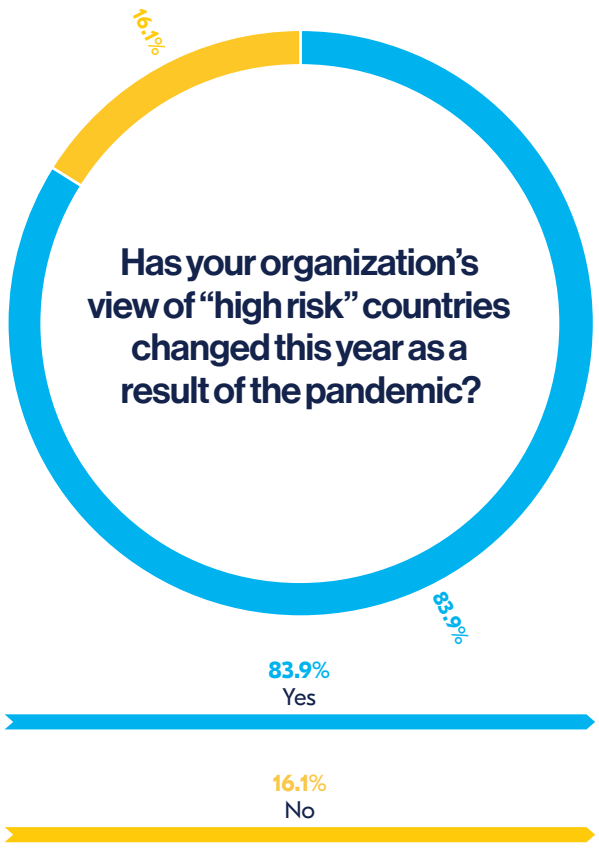


Figure 25. Has your organization's view of "high risk" countries changed this year as a result of the pandemic?

Despite the decline in staff travelling abroad in 2020, there has been a significant uptick in the measures organizations are taking to ensure the safety of staff travelling remotely. Last year, less than half of organizations (43.9%) ensured all travellers and remote-based employees fulfilled their duty of care obligations. This year, the figure has risen to two-thirds (66.2%). Furthermore, over half of organizations (55.2%) admitted to having a comprehensive travel risk management plan in place which includes emergency communications within that plan. Last year, just 39.3% of organizations reported having this in place.

The measure which has seen the least increase this year is ensuring the organization has reliable contact information for staff travelling abroad. Just over half (52.2%) of organizations reported they do this compared to 48.2% in 2019 — where it was the highest rated option. The muted improvement in this area is almost certainly because organizations have not had staff travelling this year, so there has been no need to ensure reliable information has been updated. The previously mentioned options, however, are likely to form part of larger strategic plans which will have been under discussion during COVID-19.

"Travel policy will change because of COVID-19. We are already talking about it and I'm speaking to HR to make sure we get contact information for anyone who does go abroad. Overall though, I don't think people will be travelling as much in our organization. We've already cancelled our travel insurance policy and will now be ensuring on a single employee basis."

Crisis Manager, Engineering, Australia

The survey reveals how COVID-19 is already resulting in organizations using additional measures to protect the safety of travelling staff: 42.7% of organizations are ensuring employees follow additional measures when travelling because of COVID-19. For some, this means providing guidance to employees regarding sanitisation measures whereas for others, they are mandating employees to use country-specific COVID-19-tracing apps and/or using additional add-ons on their existing emergency communications tool.

How does your organization ensure the implementation of effective emergency communications plans for travelling or remote-based staff?

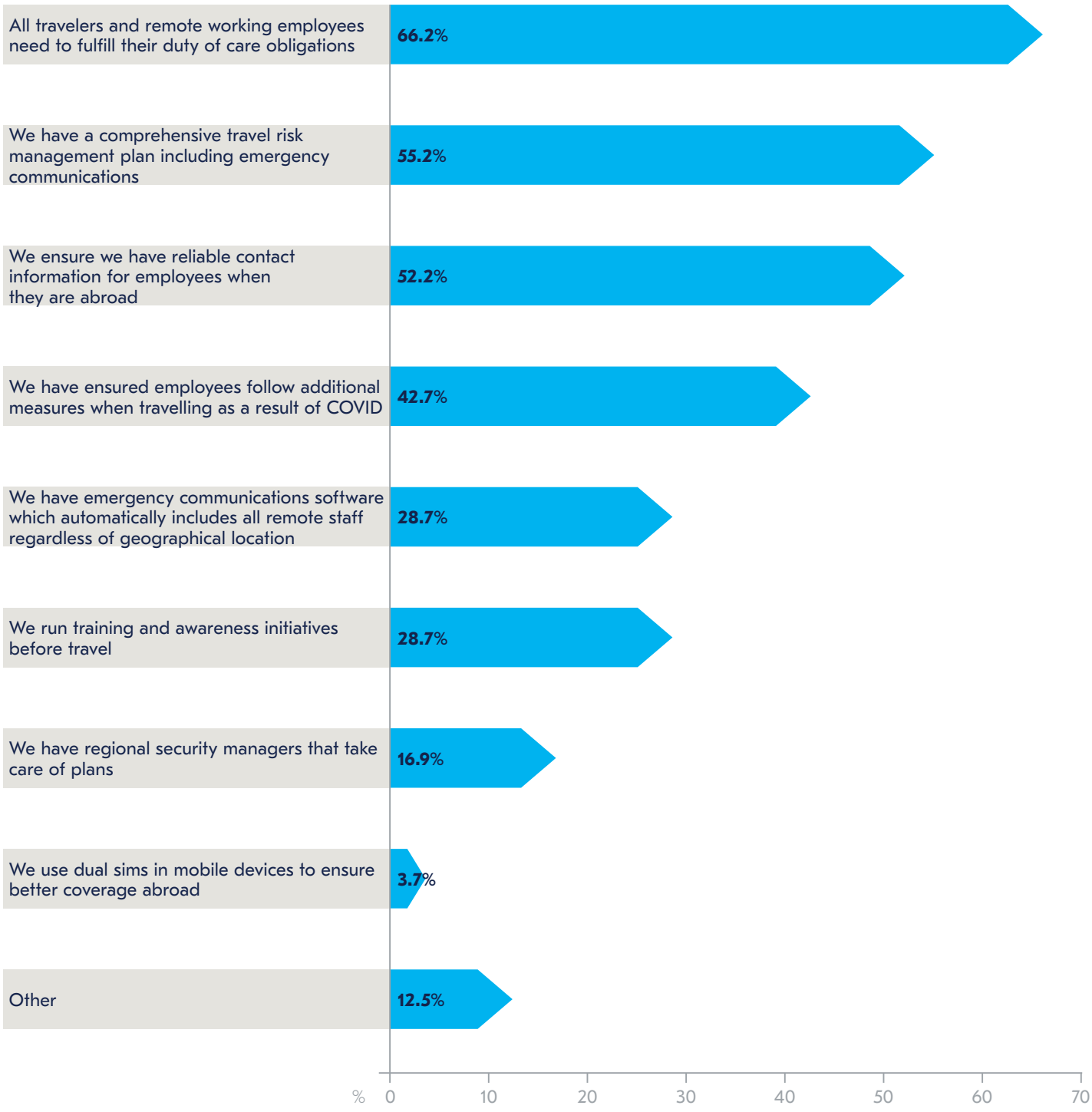


Figure 26. How does your organization ensure the implementation of effective emergency communications plans for travelling or remote-based staff? (please tick all those that apply).

Management of Emergency Communications Systems and Processes

Management of Emergency Communications Systems and Processes

- Although Business Continuity is the department most likely to be responsible for managing the emergency communications process, organizations are increasingly managing it collaboratively with Crisis Management frequently taking joint responsibility.
- Senior management often take on the strategic management of emergency communications processes, with Business Continuity assuming the operational management.

Whilst the IT department are normally responsible for ensuring the installation and implementation of an emergency communications tools and software, ongoing management of the emergency communications process is most frequently the responsibility of the Business Continuity department — although this is far from universal. Business Continuity is responsible for emergency communications in over a third (34.9%) of organizations, whilst Corporate Communications are responsible for it in 14.5% of organizations.

It appears that Business Continuity is responsible in fewer organizations than last year: in 2019, BC was responsible in 45.7% of organizations. However, most of the change is taken up by the "other" category in the question which was selected by 18.7% of respondents. Most responses show that management of emergency communications has become a much more collaborative approach: widely selected approaches are joint management by BC and Crisis Management, management by a Crisis Management Team (consisting of multiple departments) or management by two departments (such as BC/Corporate Communications, BC/IT, BC/Board). Other organizations had different departments manage specific parts of the plans: strategic management of emergency communications was typically done by the board — often in collaboration with corporate communications, whereas the operational management was typically carried out by BC and/or Crisis Management.

The increased level of collaboration between Business Continuity and other departments will be partly attributable to organizations adopting better organizational/operational resilience strategies across their organizations. However, some of the increased collaboration this year is likely to be due to a better awareness and appreciation of the work of the Business Continuity department during the COVID-19 pandemic: respondents to the survey felt that the relevance/importance of BC in their own organizations had increased by an average of 70.9% in 2020.

"The importance of business continuity has definitely been increased in the organization. My role has changed since April and more recently because of my visibility around the resilience piece, I'm no longer reporting to my line manager and now report to his line manager. We've been taken out to actually deal with the resilience issue to the person above my MD."

Head of Safety, Health, Risk & Resilience, Security, United Kingdom

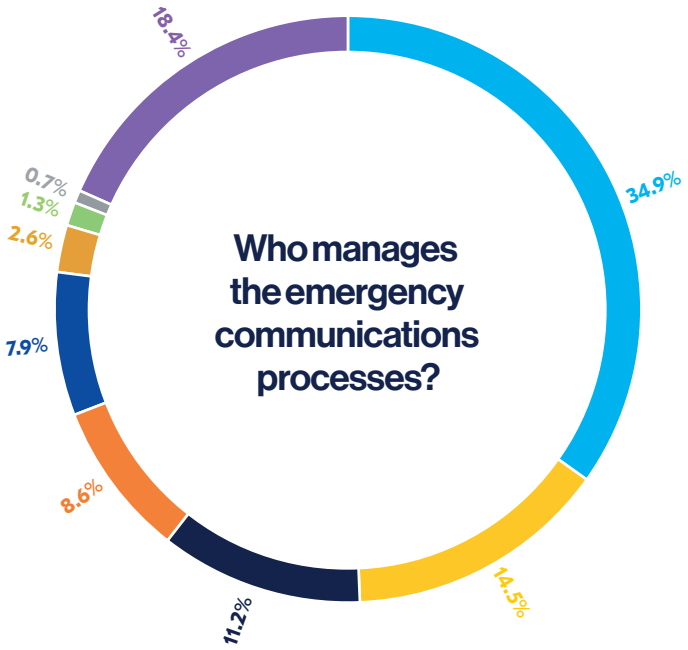
"There has been a definite change in the organization's view, not only to emergency communications, but to every asset of business continuity. I see a huge increase of interest in the process, the emergency response, what they need to know on the alert system and so on. I think COVID-19 helped to educate that business continuity might have been a silent process running somewhere deep down in the organization, but when it comes to it, it's a very important one and not having it in place before an emergency, like a pandemic, appears can be disastrous. If you are in Business Continuity now, your career is worth its weight in gold. Before the pandemic, I was reporting to the Vice President of operations and now, during the pandemic, I'm reporting to the President of the organization."

Business Continuity Manager EMEA, Manufacturing, Belgium

Not all organizations have managed to successfully collaborate: an interviewee explained how the emergency communications tool was owned by security who had different requirements of the tool than those in Business Continuity, for example. This has led to different tools being employed across the organization based on the need of that particular department.

"One of the downsides is that the maintenance of the tool is not by Business Continuity, it's by security. And these people complain because they say that they have too many returns of email addresses, which are personal and are no longer valid. Or they take phone calls from people who say 'Hey, I don't work for [company name removed] anymore, why do I still get the messages?' and so on. So it's not that we don't talk to each other, but the need of the mass notification tool which security is using is different from what business continuity would use it for. And therefore it is a little cumbersome, but it's not unworkable. I mean, we can reach our communities, but not with one mass notification tool. We use different tools in different layers of the organization."

Business Continuity Manager EMEA, Manufacturing, Belgium



34.9%
Business continuity management

14.5%
Corporate communications

11.2%
Board or executive/leadership team

8.6%
Risk management

7.9%
Security management

2.6%
IT

1.3%
Human resources

0.7%
Facilities management

18.4%
Other

Figure 27. Who manages the emergency communications processes?

Emergency Communication Plan Triggers

Emergency Communication Plan Triggers

- Disease outbreak accounted for over half (51.7%) of emergency communication plan activations in 2020 compared to just 2.7% in 2019.
- Increased phishing attacks this year has resulted in an increase in alerting for cyber security incidents or data breaches.
- Fire-related incidents have fallen this year: just 12.7% of activations were because of fire compared to 19.1% in 2019. This is likely to more workplaces being closed as a result of the pandemic.

In the 2019 Emergency Communications report, Disease Outbreak accounted for 2.7% of emergency communication plan activations and languished second from last in the reasons for emergency communication plans being triggered. Unsurprisingly, this year it has soared to the top of the list with the same category accounting for over half (51.7%) of emergency communication plan activations.

Interviewees for the report discussed how COVID-19 has helped to make employees more aware of the need to actively respond to messaging when an emergency communications plan is activated. Many attributed this to individuals' fear of the illness which meant they were more likely to respond. Overall, however, professionals reported seeing an uptick in 2020 in employees' responsiveness during other incidents which they attributed primarily to COVID-19.

However, the survey reveals that despite the increased activations for COVID-19, emergency communication plans still had to be activated regularly for other reasons: 49.3% of activations were due to an IT or telecoms incident (2019: 49.6%) and 45.8% because of adverse weather or natural disaster (2019: 50.2%).

One notable increase this year is activations due to a cyber security incident or data breach. With employees working remotely and IT departments' time, particularly at the beginning of the pandemic, taken up with ensuring employees have the equipment and relevant tools to work from home, cyber criminals targeted employees' fears of COVID-19 with a series of sophisticated phishing attacks. In the first quarter of 2020, KnowB4 reported that phishing attacks increased by 600%[10]. In May 2020 in the UK, Her Majesty's Revenue & Customs (HMRC) had 5152 phishing scams reported by the public, up 337% on March when lockdowns first came into place[11]. CheckPoint Research also noted that in November 2020, there were 1,062 "potentially malicious" domains registered relating to vaccines: more than the previous three months put together[12].

It is therefore not surprising that this year, just under a quarter (24.7%) of activations of emergency communications plan activations were because of a cyber security incident or data breach — an increase of five percentage points on 2019 (19.7%).

There were two other notable differences this year: the first being that 10.6% of activations were due to new laws or regulations (2019: 3.5%). Whilst the US Presidential elections and the UK's departure from the European Union being partially responsible for some of the increase in new laws and regulations, Governments around the world have been changing guidance and laws daily in some countries because of COVID-19. The gravitas of some of the changes and their concurrent immediate impact on workplaces has seen plans activated multiple times over the past year.

The other notable difference this year is in activations for fire-related incidents. Fire was only responsible for 12.7% of activations; a significant decrease on the 19.1% recorded in 2019. Full statistics have yet to be compiled for workplace fires in 2020, although early evidence suggests a decrease in workplace fires in 2020. Furthermore, the UK Fire & Rescue service reported a 7.3% decrease in non-dwelling fires for the year ending 30 June 2020 compared to the same year previously[13].

Triggers for emergency communications plans change year on year and shows the need for professionals to be increasingly aware of how black swan or grey rhino events (such as COVID-19) can result in a need for plans to continue to be activated when unexpected events occur.

10. https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600
11. Coker, J (2020). HMRC Investigating Over 10,000 COVID-Related Phishing Scams. Inforsecurity Magazine [online]. Available at: https://www.infosecurity-magazine.com/news/hmrc-investigating-covid-related/ [last accessed 15 January 2021].
12. Scroxton, A (2020). Surge in Covid-19 vaccine phishing scams reported. Computer Weekly [online]. Available at: https://www.computerweekly.com/news/252493523/Surge-in-Covid-19-vaccine-phishing-scams-reported [last accessed 15 January 2021].
13. Lader, Deborah (2020). Fire & Rescue Incident Statistics; June 2020. UK Home Office [online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/933935/fire-statistics-data-tables-fire0102-121120.xlsx [last accessed 15 January 2021].

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

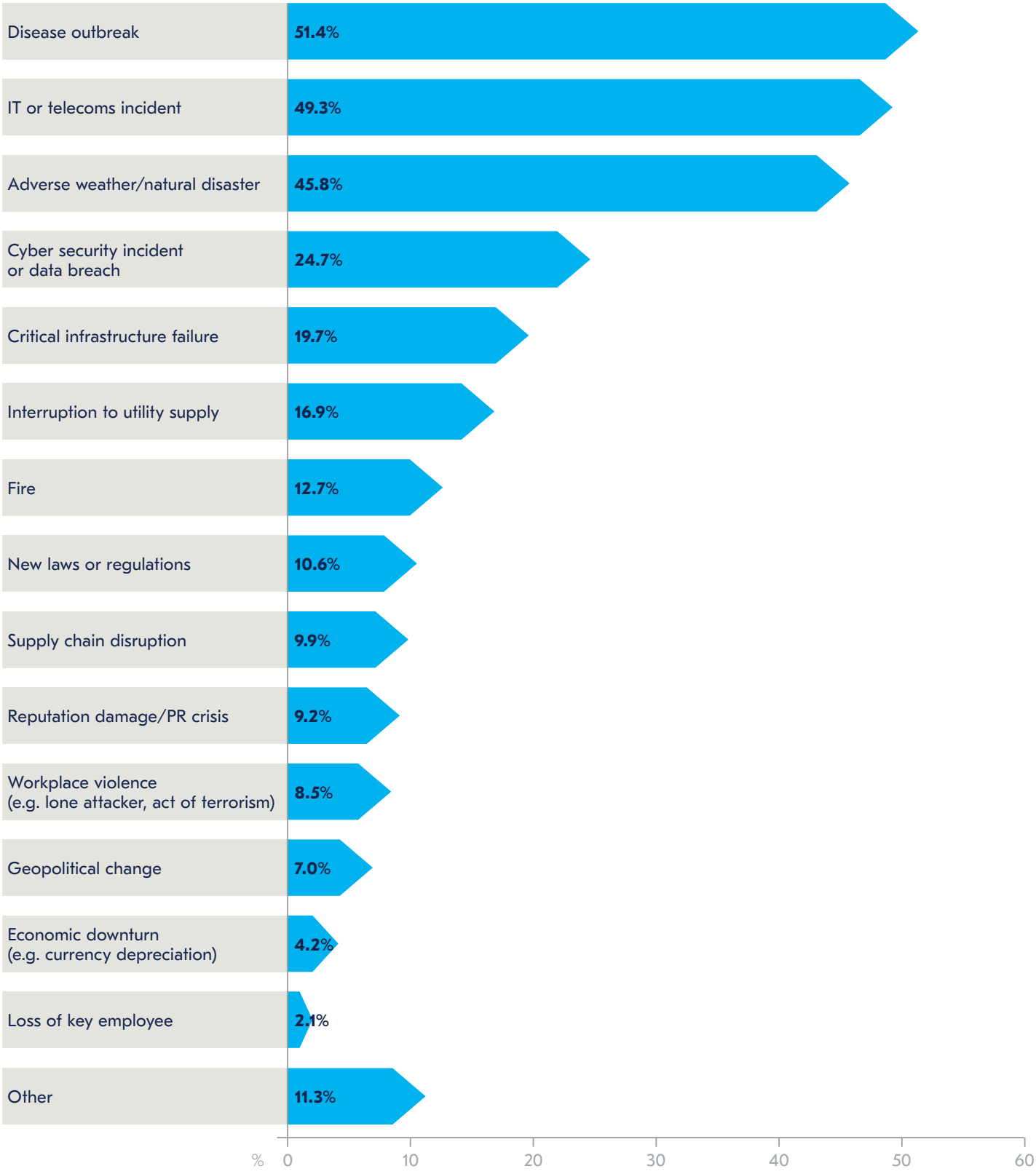


Figure 28. Which of the following triggered your emergency communications plan in the past twelve months? Tick all those applicable.

Information Access and Reliability

Information Access and Reliability

- Communicating with staff was the primary concern for organizations in 2020: just over half (52.2%) admitted communicating with staff was their primary challenge during an incident, but only two-thirds (68.2%) kept employee contact details up to date.
- An increase in fake news this year has been a challenge to organizations: unofficial news sources are more frequently being used for information than official ones.
- There has been an uptick in the number of organizations collaborating with emergency services this year but there have also been multiple examples of poor collaboration resulting in a bungled response to an incident.
- Organizations are increasingly looking to automate the updating of data on emergency communication systems by syncing with HR records. 49.0% of organizations report this is now standard practice compared to 43.0% in 2019.
- Adoption of Internet-of-Things (IoT) devices as part of an emergency communications plan has not seen any increase in 2020: many are still wary of the effectiveness when all data needs to be fully checked by a human before it is escalated.

Fake news has always been a concern, but the sheer scale of fake news in 2020 has become a global issue. Fake news authors seek to capitalise on the public's mistrust of official sources on information and prey on those who consume news media through online sources. The American Journal of Tropical Medicine and Hygiene estimated that in the first three months of the year, around 800 people died and 5,800 people were admitted to hospital globally because of consuming erroneous information[14]. The World Health Organization itself also admitted the "infodemic" was spreading faster than the virus itself, undermining the global response and jeopardising efforts to control the pandemic[15].

From a corporate perspective however, information reliability goes far beyond concerns about fake news: employee contact details need to be updated regularly to ensure all staff can be reached in a crisis, cross-departmental collaboration and community collaboration helps organizations to share pertinent information between departments and other local businesses thus ensuring an organization receives real time and accurate information from relevant parties.

Because the importance of accurate information collation has risen to the fore in 2020, this year's survey went into greater depth to determine the information sources being used, and the products and processes behind this information collation.

Tools and Software

When it comes to using specific tools and software to analyse the risks faced by their organization, 40.4% of organizations use third party risk monitoring software, and just over a quarter (27.0%) use software developed in-house. Many respondents reported that risk monitoring was still a manual process within their organization, or that risk monitoring was not done by a single tool but via a suite of different tools and methods across the organization.

Processes and Procedures

The previous year's Emergency Communications Report raised concerns that despite over half of respondents saw communicating with staff as a key challenge during an emergency, less than two-thirds (61.7%) ensured that employees' contact details are kept up to date. This year, the picture has seen little improvement: just over half (52.2%) admitted that communicating with staff was their primary challenge during an incident, but only just over two-thirds (68.2%) said that ensuring employees' contact details were kept up to date was a routine process. The seven-percentage point improvement is, however, encouraging and does demonstrate that organizations have been taking steps to improve their processes for gathering and holding staff information. Indeed, evidence from interviews carried out for this report suggest that frequent activations of systems this year due to COVID-19 have helped to ensure records are kept up to date.

> **"From my point of view, it's imperative that the emergency communication platform is kept up to date with staff names, numbers, telephone numbers, and everything else. So, it's been a good exercise to use it during the pandemic just to verify the staff are getting the messages, if nothing else."**
>
> Group Business Continuity Manager, Financial Services, United Kingdom

Others have made a concerted effort to ensure staff access can identify reliable sources of information during an incident: 43.9% of respondents said they actively trained their staff to help them identify credible information sources. This is up from the 32.9% reported in the 2019 report suggesting organizations are making tangible steps to help staff identify incorrect and malicious sources of information.

Risk monitoring is also becoming more standardised in organizations as they seek to incorporate it as part of their standard processes: 43.9% of respondents reported that their organization was now incorporating professional monitoring of risks and events into their processes compared to less than a third (32.1%) in 2019.

14. Coleman, A (2020). 'Hundreds dead' because of Covid-19 misinformation. BBC News [online]. Available at: https://www.bbc.co.uk/news/world-53755067 [last accessed 15 January 2021].
15. WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, IFRC (2020). Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation. World Health Organization [online]. Available at: https://www.who.int/news/item/23-09-2020-managing-the-COVID-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation [last accessed 15 January 2021].

Collaboration

By collaborating with other organizations within the local area, sector peers, local/regional Government and emergency services, organizations can be ensured of receiving relevant information in a timely manner: something which is crucial, particularly during an incident. 71.3% of organizations now collaborate with emergency services where possible (2019: 57.3%), 70.3% with local authorities or local government (2019: 49.6%), 56.8% with other organizations in the affected local area (2019: 39.4%) and 51.4% with sector peers. Each type of collaboration has had a notable increase from the previous year. Although some of this can be contributed to slight variation in the survey sample, respondents also explained how they were actively pursuing greater collaboration with other organizations in 2020 because of COVID-19.

If an organization has failed to establish a good relationship with local emergency services, it can lead to a bungled response in a crisis. An interviewee explained how not having a designated point person to communicate with emergency services and this, coupled with not have a designated method of communication to staff, heavily impacted the organization's ability to manage the crisis.

"People were starting to evacuate the building but were standing around outside and didn't really know where to go. They could also enter other parts of the building as the fire services said it was safe to use apart from one wing. I didn't quite understand the reasoning behind this because my assessment of the situation would have been to evacuate the entire building, but I needed to rely on the expertise of the fire services. The problem was communication between the fire services and us. We physically had to go to them and ask them what's going on because there was no designated person for communications with the fire services or with the police. There was also no designated way to communicate to the employees; and there was no designated way to communicate with management. I called them on their cell phones, because naturally I had the numbers for such an occasion. But there was no way for us to let people know via a central authority whether they should evacuate, whether people should go home or whether people should even come to work, so we had to improvise."

Emergency & Business Continuity Management Professional, Financial Services, Germany

Media & Digital

When it comes to accessing information, official news sources are only ranked as fourth in the table (66.2% of respondents use this in an emergency), with unofficial social media being used more readily for information gathering (68.2%). Social media, if used correctly, can help to provide a real time view of a situation as it unfolds whereas news networks will normally only publish news stories when information has been fully corroborated. Whilst information on social media channels should be used with care and corroborated as much as it can be, in the event of a situation such as a riot or active shooter, mining a tool such as Twitter could, in extreme circumstances, save lives.

Official social media accounts can also provide a medium between uncorroborated unofficial social media stories and material from news networks. Twitter accounts such as the Surrey Road Policing Unit in the UK[16], the Queensland Fire and Emergency Services in Australia[17] and the City of New Orleans Twitter account in the United States[18] have received praise for how they have used their social media accounts in emergency situations to provide relevant, timely and accurate information in a crisis. Only 38.5% of respondents claimed they use such information sources during an emergency or crisis scenario, and it is one which many organizations could explore more to increase the amount of information they have during an incident.

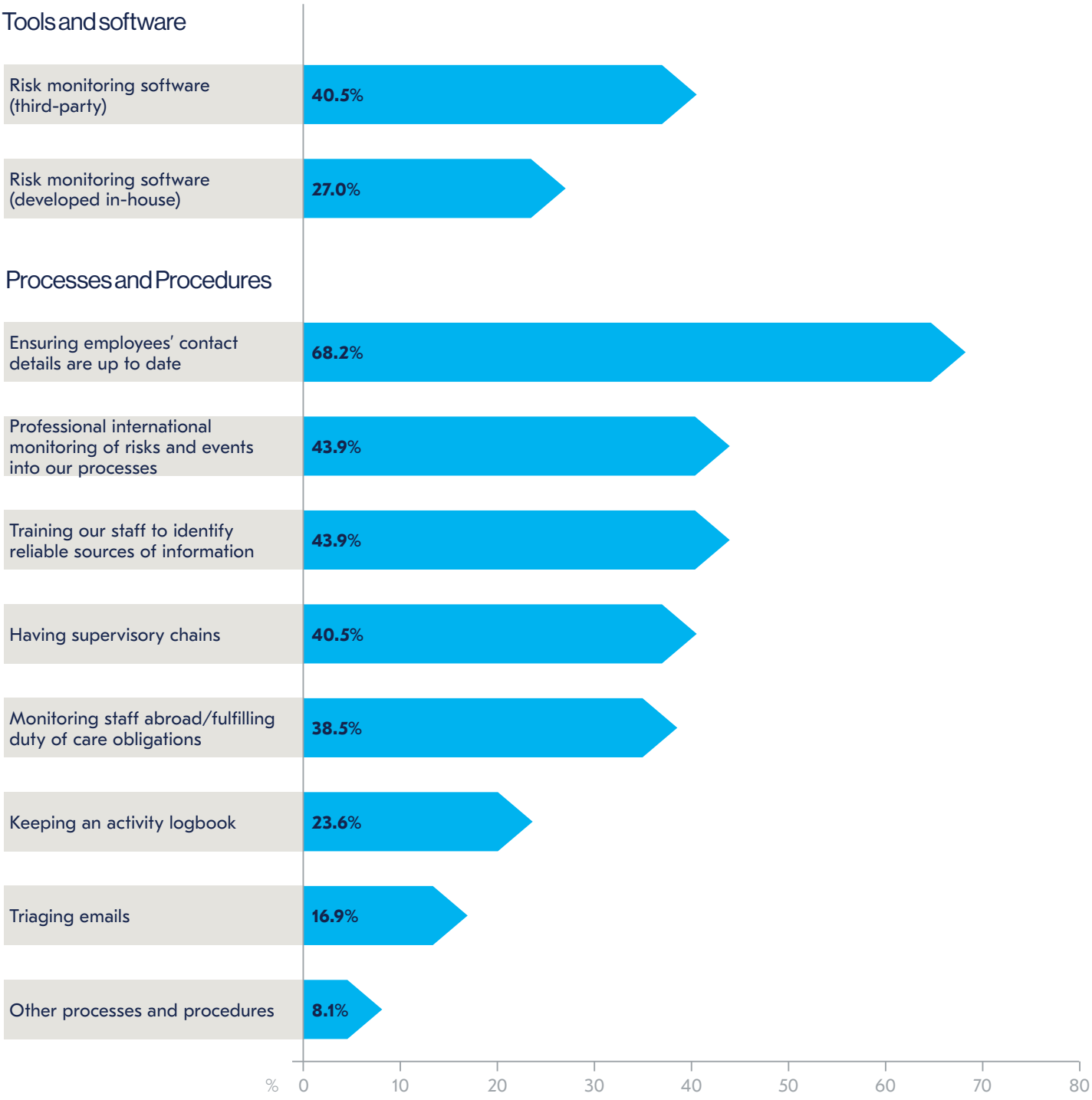
Some Business Continuity professionals have taken it upon themselves to actively scan news, Government and other websites before the business day starts to make early decisions about how operations should be managed in a particular day. Using a single person can help to provide a filter to unwanted or fake news and ensures a single point of contact in the business for information enquiries to be made to.

"Every morning, I log on and go to the Worldometers website, then I'm going onto the Bermuda government's website, and then Atlanta government's website, and then checking what the local restrictions are, what the local number of cases are, and what the local landscape is like. This is so I can try and work with staff in the various locations to make informed decisions about how we're continuing our operations."

Group Business Continuity Manager, Financial Services, United Kingdom

16. 2021. Surrey Road Cops Twitter. [online]. Available at: https://twitter.com/SurreyRoadCops [last accessed 15 January 2021].
17. 2021. Queensland Fire and Emergency Services Facebook. [online]. Available at: https://www.facebook.com/QldFireandEmergencyServices [last accessed 15 January 2021].
18. 2021. City of New Orleans Twitter. [online]. Available at: https://twitter.com/CityOfNOLA [last accessed 15 January 2021].

How do you ensure the acquisition of relevant sources of information in the context of managing an emergency case/crisis scenario? plan in the past twelve months?



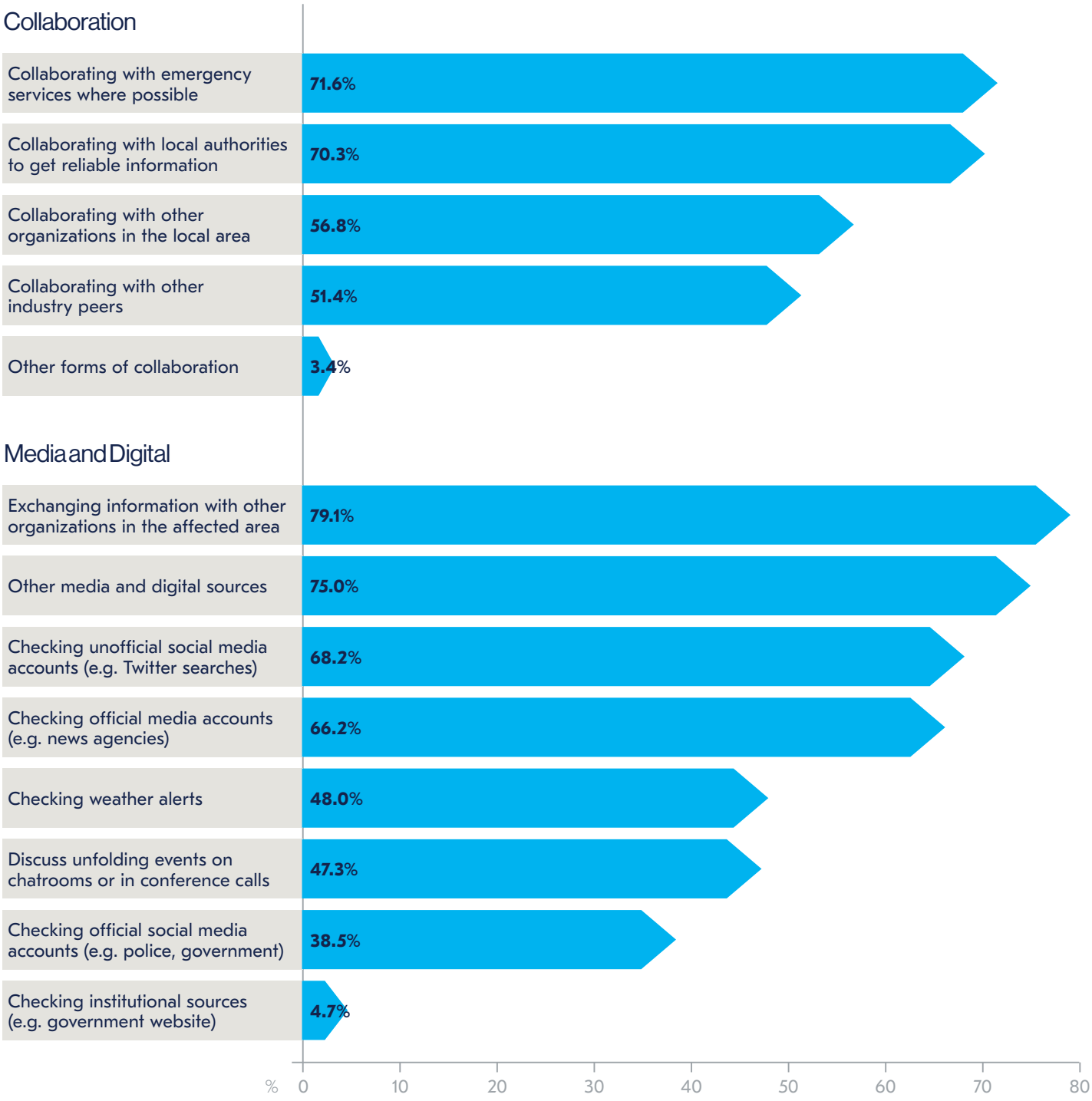


Figure 29. How do you ensure the acquisition of relevant sources of information in the context of managing an emergency case/crisis scenario?

The report has already discussed the importance of ensuring staff contact information (permanent, contract and temporary) is kept up to date to ensure all staff can be reached during a crisis. Whilst just 68.2% of organizations claim to do this, if the information is not obtained regularly enough, is stored in a way it is inaccessible during a crisis or breaks data privacy laws, an urgent review is likely to be needed.

Ensuring emergency communication systems are linked to HR records can mean secondary data does not need to be gathered for an emergency communications system which means there is less chance of errors than if information had to be reinputted into the system. Organizations are increasingly seeking to automate this process, and 49.0% of organizations now have systems which integrate with HR systems and automatically update (2019: 43.0%). A further 48.3% admit to being in regular communication with HR to ensure data is up to date (2019: 44.0%). Although frequent dialogue and/or automating systems with HR ensures systems are accurate, it does place a reliance on HR to ensure they keep their contact details up to date. Some interviewees told how their HR departments relied on staff proactively contacting them when they had a change of contact details. This is something which is unlikely to happen unless a prompt is given.

Other respondents reported issues with systems which only allowed alerts to be sent out to company email addresses or company telephones which meant staff frequently did not receive messages during an incident. This, coupled with staff opting out from receiving messages and other data privacy/ GDPR issues led to further issues with their emergency communications plan.

"We have a tool in place, but the downside of this tool is that it does not reach people who do not have a [company name removed] registered email address. It's a tool that reaches people which have either a [company name removed] email address or a [company name removed] cell phone. If you don't have this, then the tool will not reach you. It is because a lot of people do not want to share their private details. We are facing GDPR issues and the only country we have had success in is in Turkey."

Business Continuity Manager EMEA, Manufacturing, Belgium

More organizations are now using automated prompts from their emergency communications systems to remind staff to keep contact details up to date: nearly a quarter (24.1%) are now utilising such a tool, compared to 20.4% in 2019 and one-third of organizations (33.1%) report running regular test alarms with corrective actions afterwards. Interviewees told us that the sheer number of activations they had had to make in 2020 because of COVID-19 had served a similar purpose in highlighting where contact information was invalid.

Nevertheless, despite COVID-19 serving as a prompt for many to keep their details up to date, many organizations are still finding that staff are not doing so. One interviewee appeared to be fairly exasperated with the lack of response during a test and told how he would continue to carry out multiple tests until all accuracy had improved.

"It's a bit of a palaver at the moment, as you can imagine. You send the test out and 60% people respond within the next couple of days, and then you spend weeks tracking down the other 40%. When asked 'Why haven't you responded?' they come up with various reasons: 'I've changed my mobile phone, I forgot to give you the new number,' 'I thought it was spam,' or 'I didn't recognise the number, so I deleted it,' 'I didn't know I had to respond,'. All sorts of things, really. So, you have to keep pushing, pushing, testing, testing."

Group Business Continuity Manager, Financial Services, United Kingdom

Such a scenario also demonstrates how it is helpful to have an accurate overview of those people who have been notified so weeks are not spent tracking the non-responsive people.

Encouragingly, the number of organizations who use Excel or another type of spreadsheet to hold contact information has fallen this year. Just over a third (36.6%) of organizations still use Excel to store contact details, compared to 42.6% in 2019. Whilst Excel is a tool which most staff use regularly and find it easy to update information, it can result in issues with version control and information being different from that held on HR systems. Furthermore, in the event of a system outage, an Excel spreadsheet held on a centralised drive may not be accessible, and any printed copies would need to be stored in a way that was not in breach of GDPR or data protection guidelines.

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

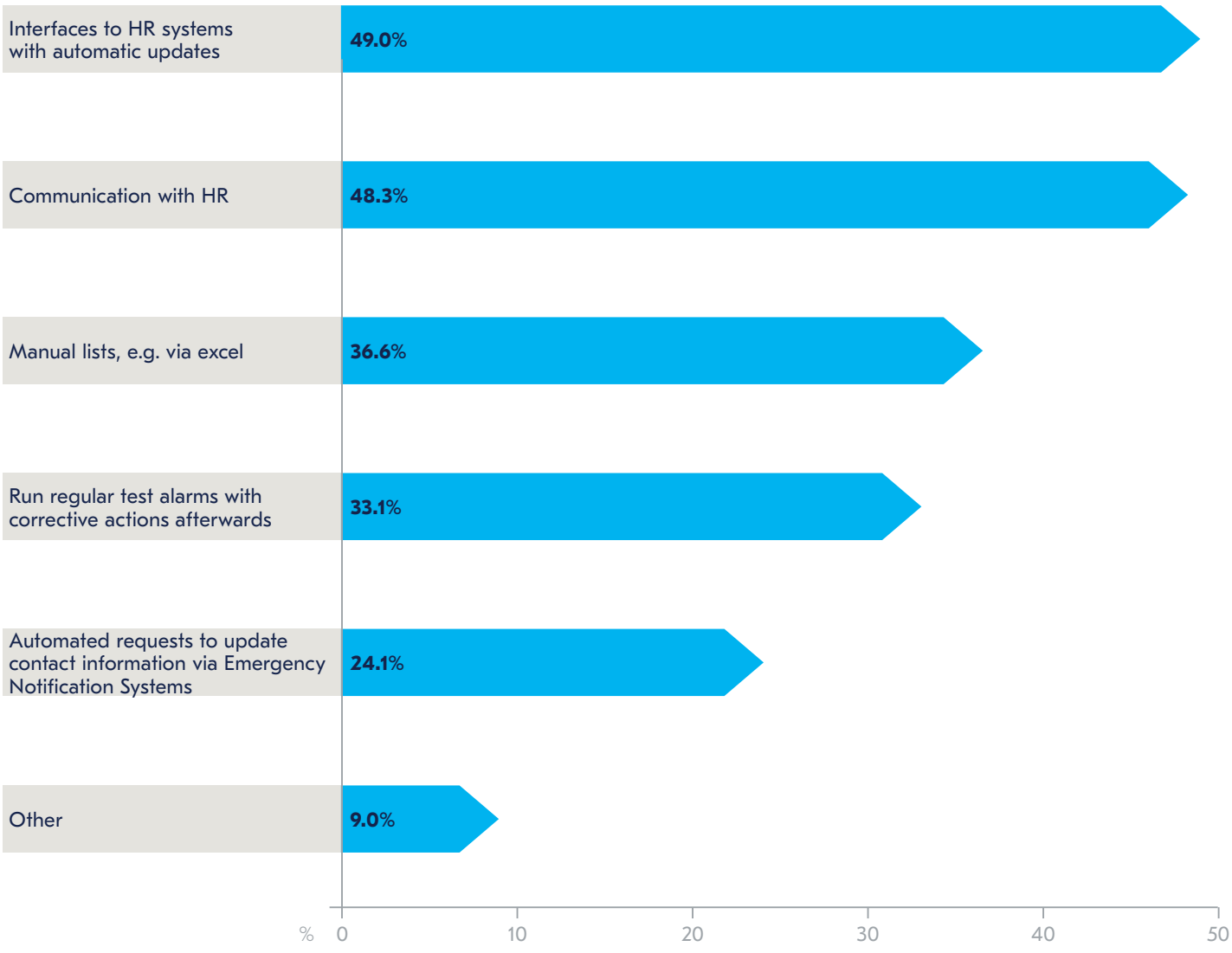


Figure 30. How do you ensure contact data of employees, experts, etc. is up to date?

Automation of processes has already been discussed, and one method which organizations use to help automate processes is by using Internet of Things (IoT) devices within their emergency communications plan. However, although there has been a greater update of emergency communications tools and software this year, the use of Internet of Things (IoT) technology has failed to see any uplift at all. Over half (53.3%) do not plan to make use of IoT within their emergency communications plan, and just 5.9% claim that IoT devices are well embedded into their processes. Whilst a further 17.8% use IoT devices in limited areas of their plans and a further 17.0% are planning to use such devices, there has actually been a decrease in the number of organizations employing the technology. Some of this is likely to be because of a changed working environment: many IoT devices will be used within office environments and, without staff on site, there has been no need to use them. However, for many professionals, the primary problem with using IoT devices is that information provided from systems needs to be fully checked by a person before it provides an alert. This would normally fall to an operations manager, a facilities manager or security staff.

"[A device such as a fire sensor automatically sending out an alert] should go to a building manager in capacity as Chief Warden to then assess and decide the next action. A building management system sending out unverified alarms to building occupants requires a great deal of thought and parameterisation."

Consultant, Australasia

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

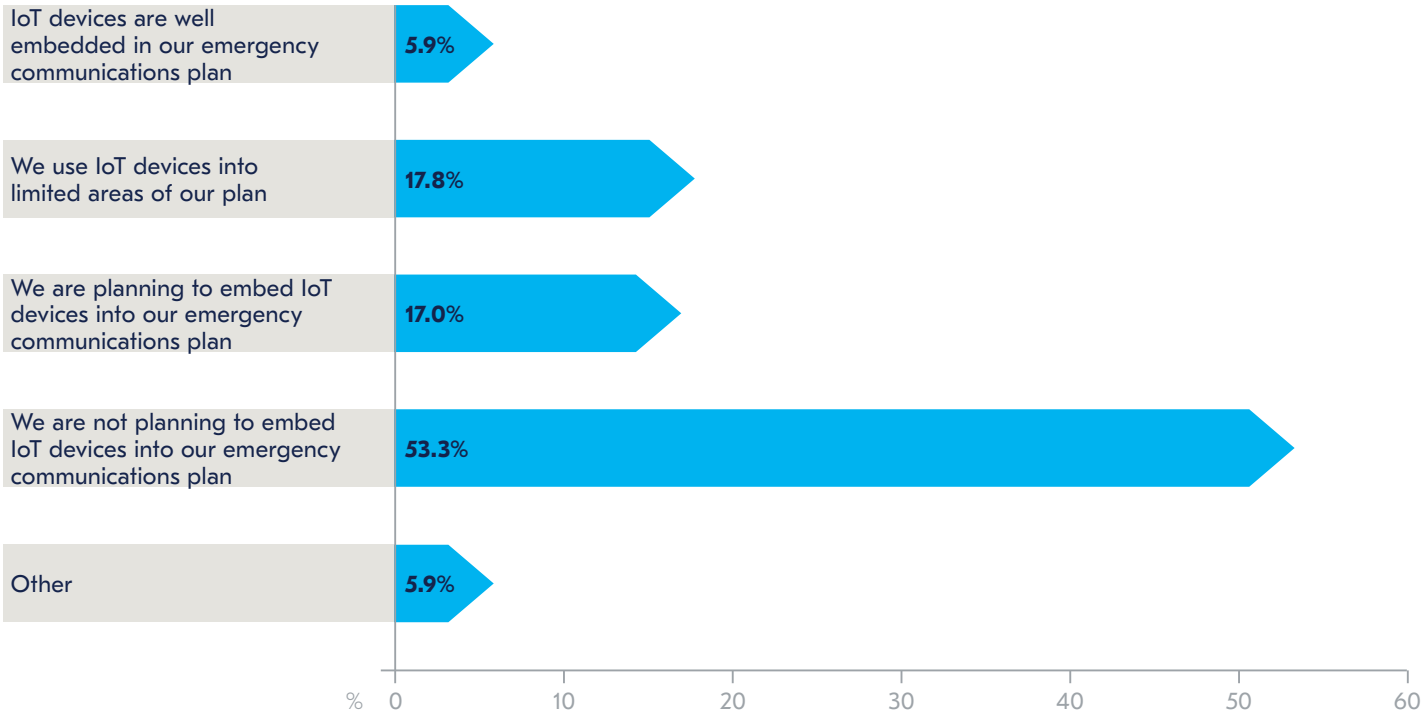
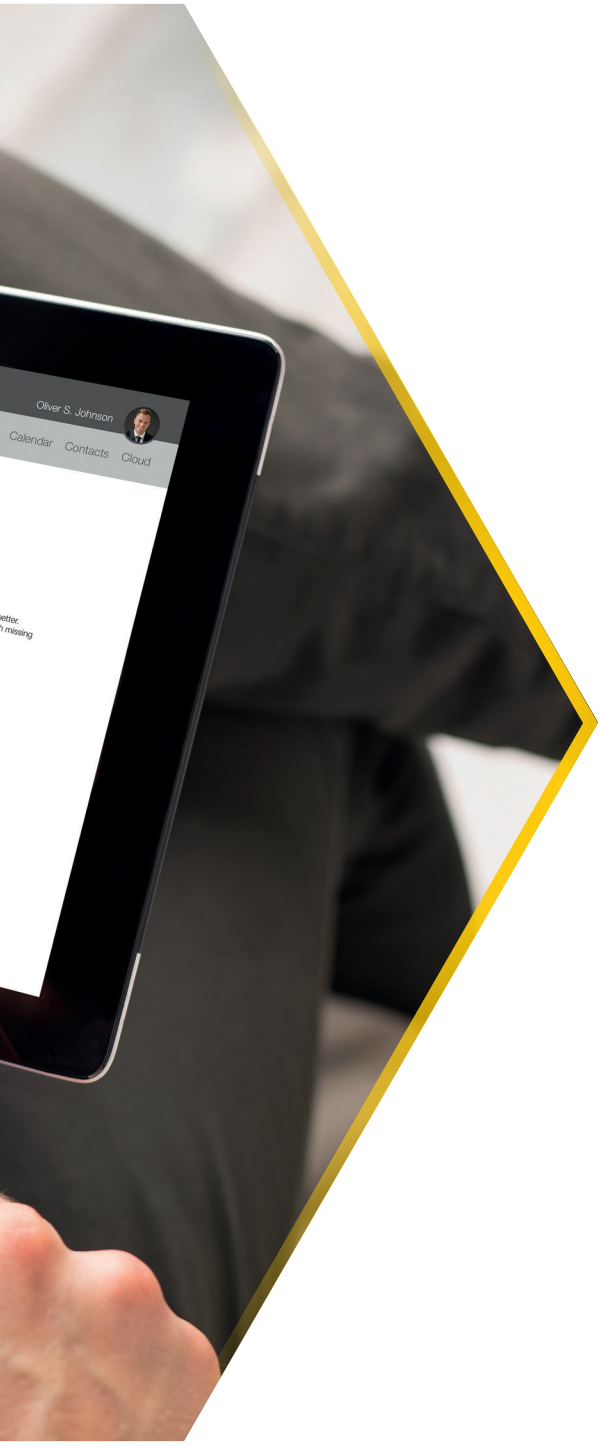


Figure 31. How do you see the implementation of Internet of Things devices within emergency communications? (e.g. fire sensors sending out alerts)

Communication Preferences by Scenario



Communication Preferences by Scenario

- Email remains the preferred method of information transmission and is favoured across most scenario types.
- The only exception is for external communications for a natural disaster: a website announcement or social media is more likely to be used. This is likely to be because a natural disaster has less potential for causing a reputation impact than, for example, a cyber-attack where communications will need to be carefully crafted.
- Social media leaks from staff during an incident are a major concern for organizations: some cite it as their primary concern during an incident.

External Stakeholders

Communicating with external stakeholders during and immediately following an incident requires different techniques to communicating with internal stakeholders or staff. In an era where news travels fast, a mismanaged or badly written communication can not only lead to stakeholders being misinformed, but can ultimately result in lost contracts, customer attrition, falls in revenues and a drop in an organization's share price. Legal issues could also arise if, for example, a critical customer's contract states that they must be informed if an incident occurs and they hear of it first via third party sources.

Communicating with external stakeholders is very different to communicating with internal stakeholders as staff require additional information on what they should be doing during an incident e.g. where they should be going, how they should continue to work (if possible) and how they can ensure their own safety. Information transfer needs to be both quick and informative whereas communicating with external stakeholders typically requires more measured communications which are crafted to the audience they serve.

For external communications, email is the preferred method of communication for cyber security/data breach and disease outbreaks with 59.1% and 56.1% of respondents respectively selecting this as their method of communication. Website announcements and public announcements (typically a press release) are the second and third options for both incident types. The most striking difference between the two incident types is the use of social media: just 27.3% of respondents would use social media to communicate the news of a cyber security/data breach to external stakeholders, whereas 35.6% would use it during a disease outbreak. The difference here is likely to be due to reputational impact: a cyber breach is something which can readily be blamed as a failure of an organization's processes, whereas a disease outbreak is something which an organization has somewhat less control over.

Such a theory is further exemplified for the third incident type: natural disaster. Notifying external stakeholders by email is in third place here (51.5%) but one-way methods of mass communication take the first two spots: website announcement (59.1%) and social media (53.0%). A natural disaster, whilst an incident which external partners do need to be informed about, is one which has less potential to cause reputational damage and producing blanket communications are less of an issue.

Which processes would you use to communicate to external stakeholders (e.g. customers, media) during each of the following scenarios?

Cyber security incident or data breach

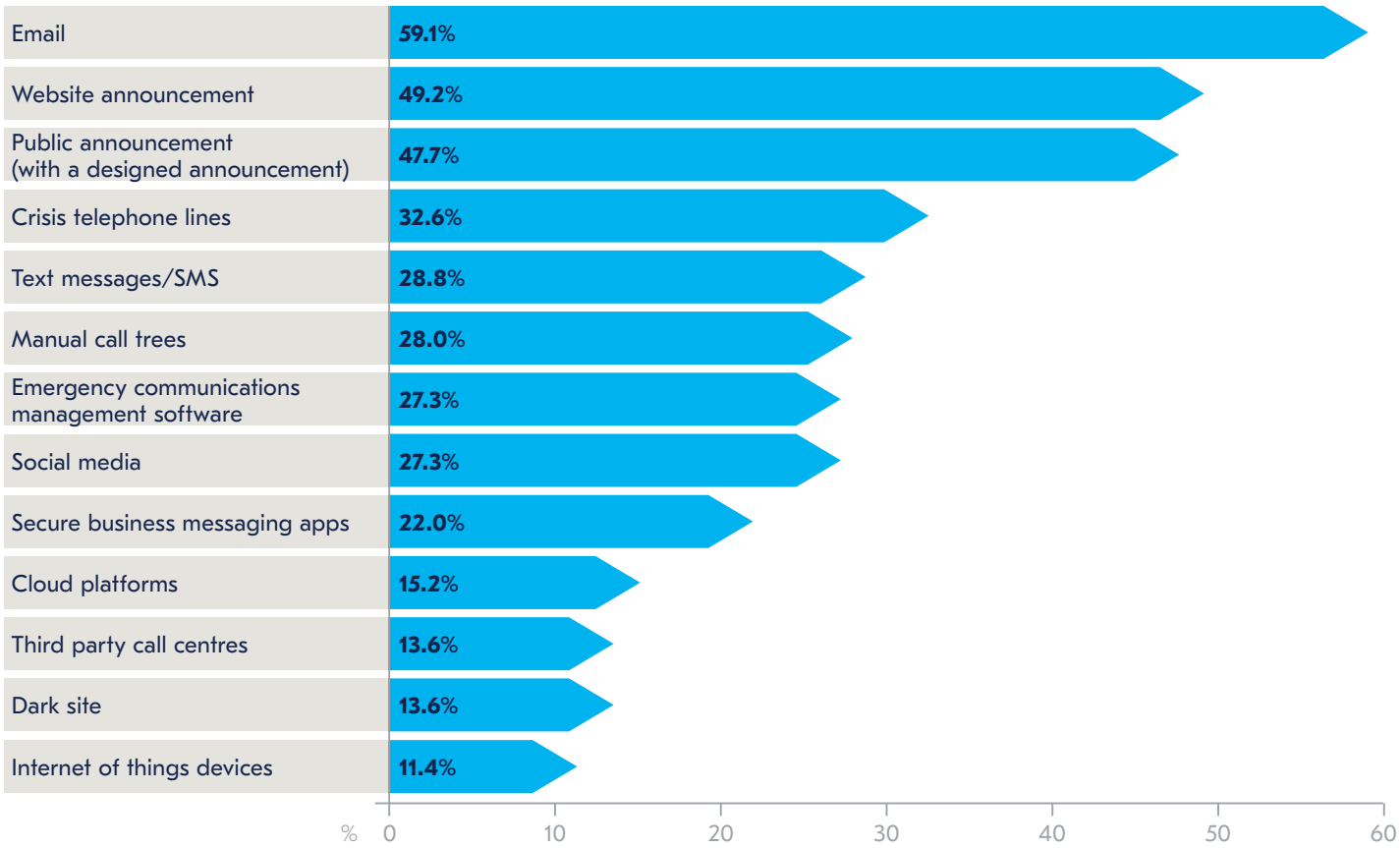


Figure 32. Which processes would you use to communicate to external stakeholders (e.g. customers, media) during each of the following scenarios?

Disease outbreak

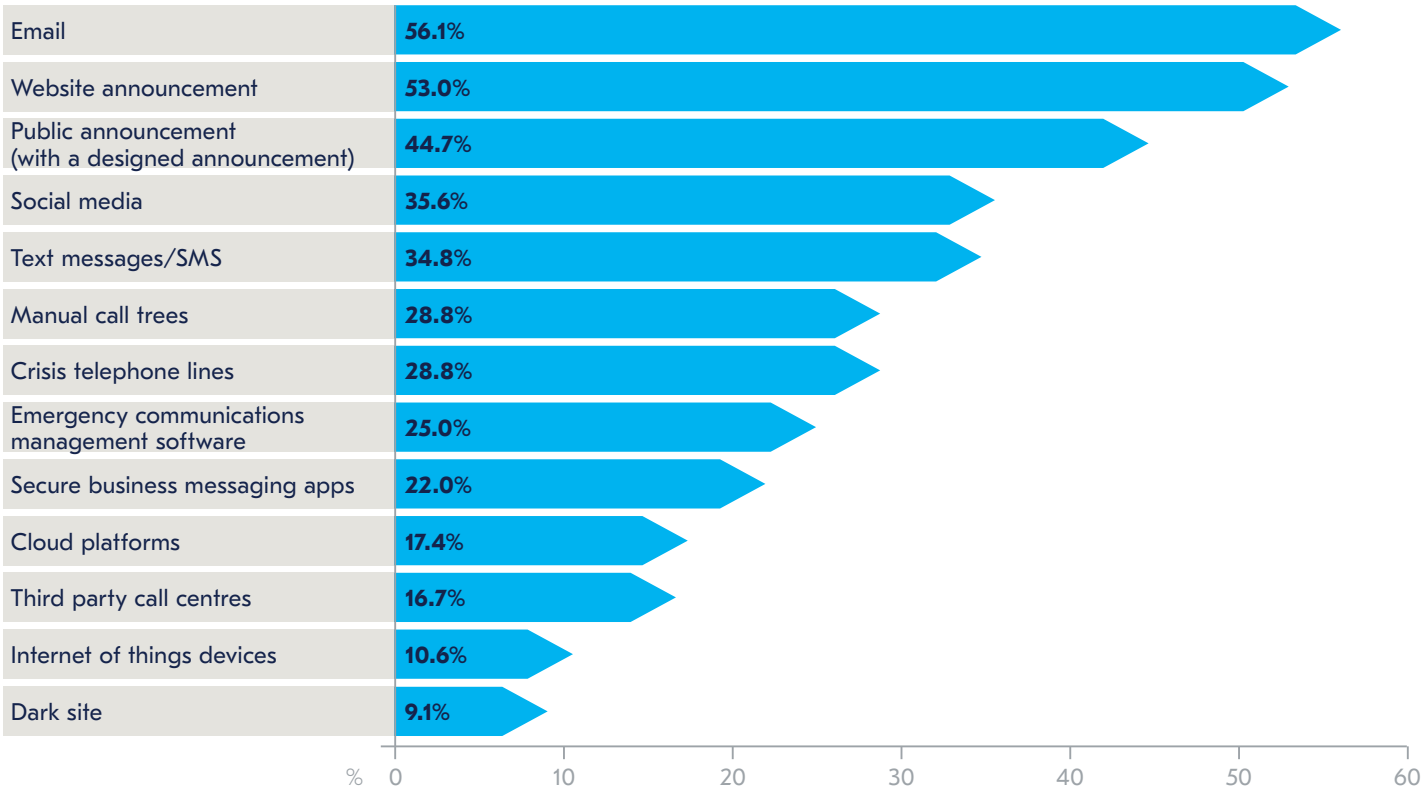


Figure 32. Which processes would you use to communicate to external stakeholders (e.g. customers, media) during each of the following scenarios?

Natural disaster

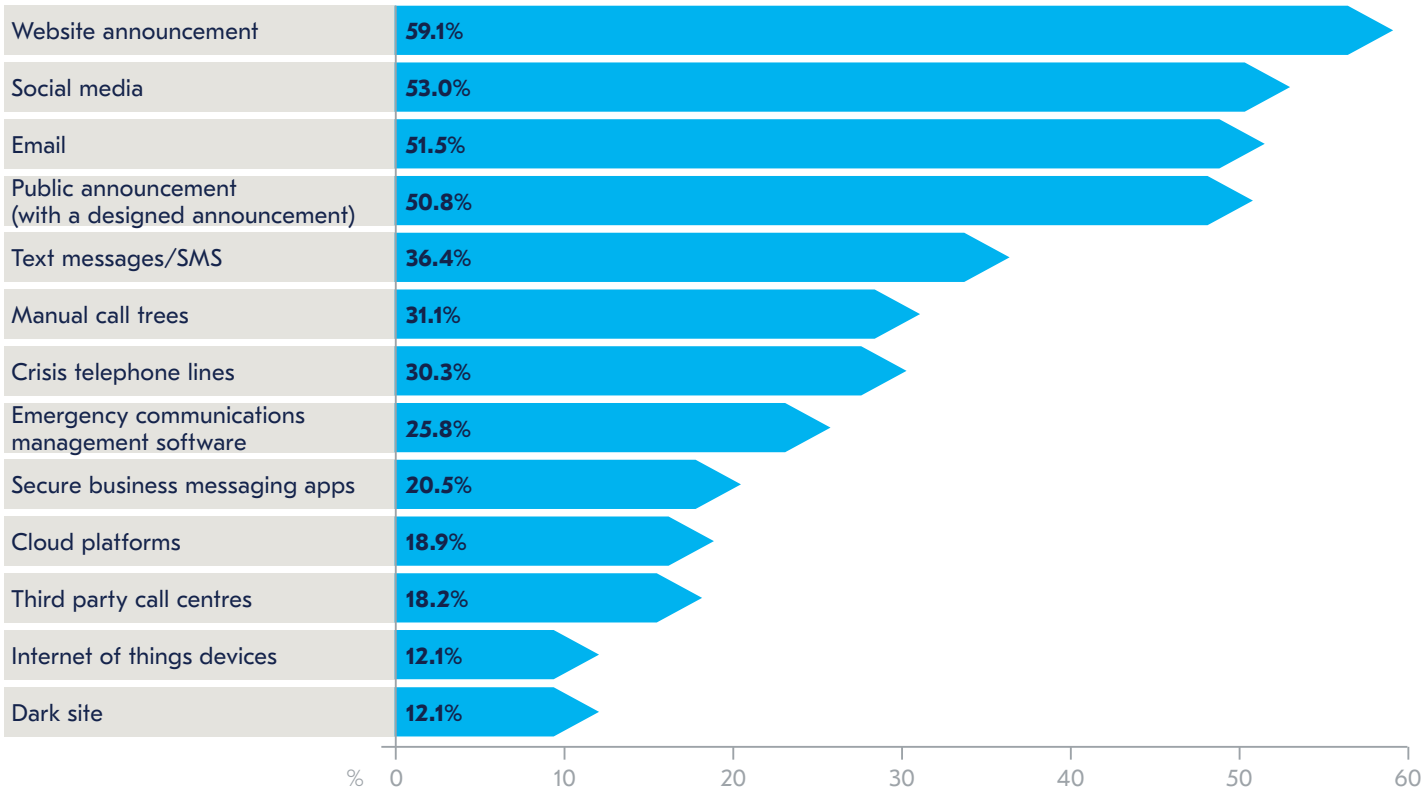


Figure 32. Which processes would you use to communicate to external stakeholders (e.g. customers, media) during each of the following scenarios?

Internal Stakeholders

For internal communications, email is by far the preferred method of communication for all incident types: cyber security incident/data breach (77.4%), disease outbreak (82.0%) and natural disaster (81.2%). As noted in the 2019 report, the applicability of using email to communicate news of a cyber security incident/data breach is questionable when systems may have been compromised and are inaccessible. However, it does appear that some organizations are aware of this: manual call trees (a method of communicating without the need for IT systems) is the third most popular method for communication of a cyber security incident/data breach, with 39.1% using it during such an incident.

A further issue with email is speed of information delivery. Some organizations can take a significant amount of time to craft an email to employees which can, in turn, inhibit organizations' ability for a timely response. An interviewee in one organization explained how he tasked himself to quickly curate an email and then get it checked rather than a group of people cumulatively writing one. His method meant emails could be sent out in a timelier manner.

> **"There is often a meeting which starts with 'well, what are we going to say to people?'. I think that process takes a little bit longer than it should do. One of my strengths is writing emails quickly, so I do quite a lot of that for the company. I'm quite prepared sometimes just to sit down and write down some thoughts and then get people to comment on it, rather than wait for other people to bat the ideas around. It's better that someone's got something to look at and critique rather than take time just discussing it!"**
>
> Group Business Continuity Manager, Financial Services, United Kingdom

Which processes would you use to communicate to internal stakeholders (e.g. customers, media) during each of the following scenarios?

Cyber security incident or data breach

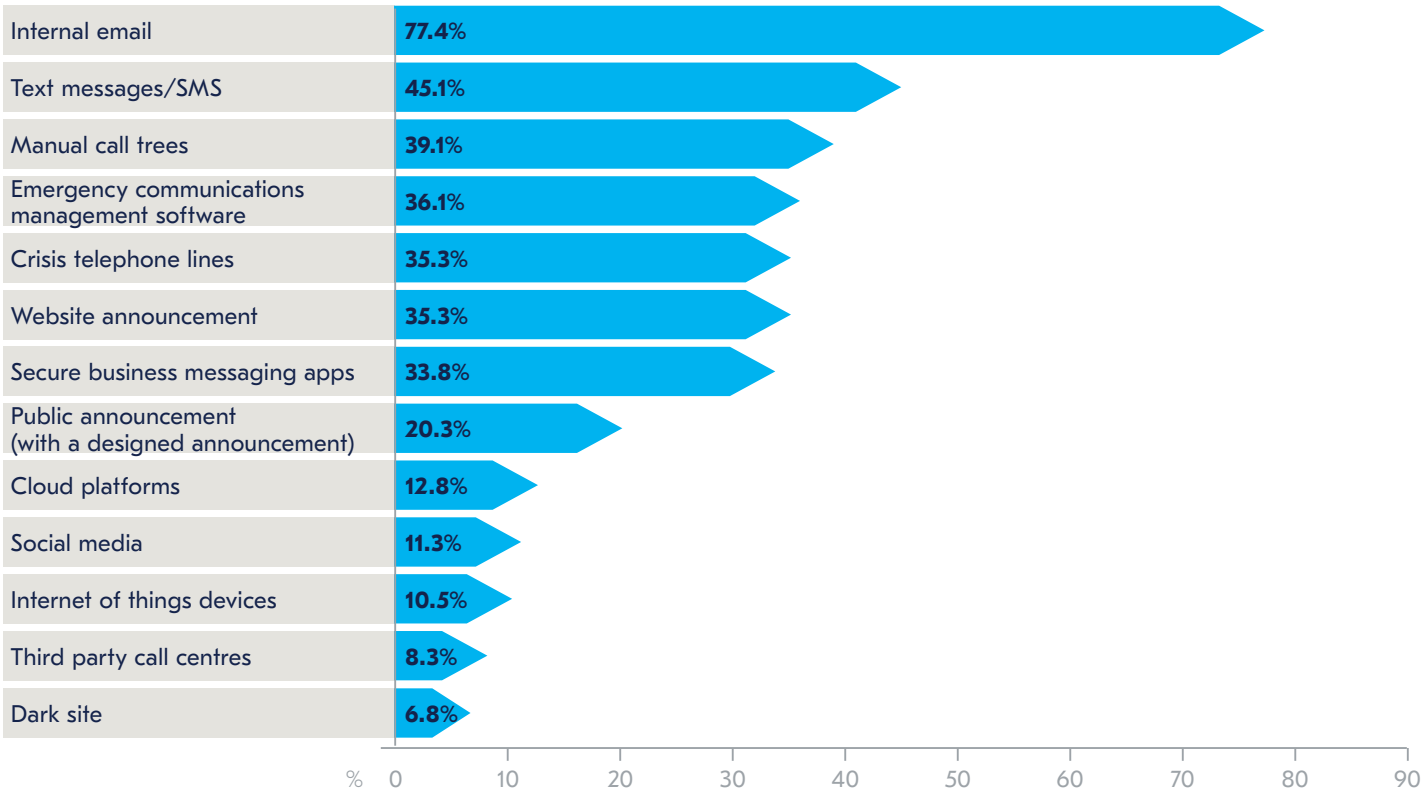


Figure 33. Which processes would you use to communicate to Internal stakeholders (e.g. customers, media) during each of the following scenarios?

Disease outbreak

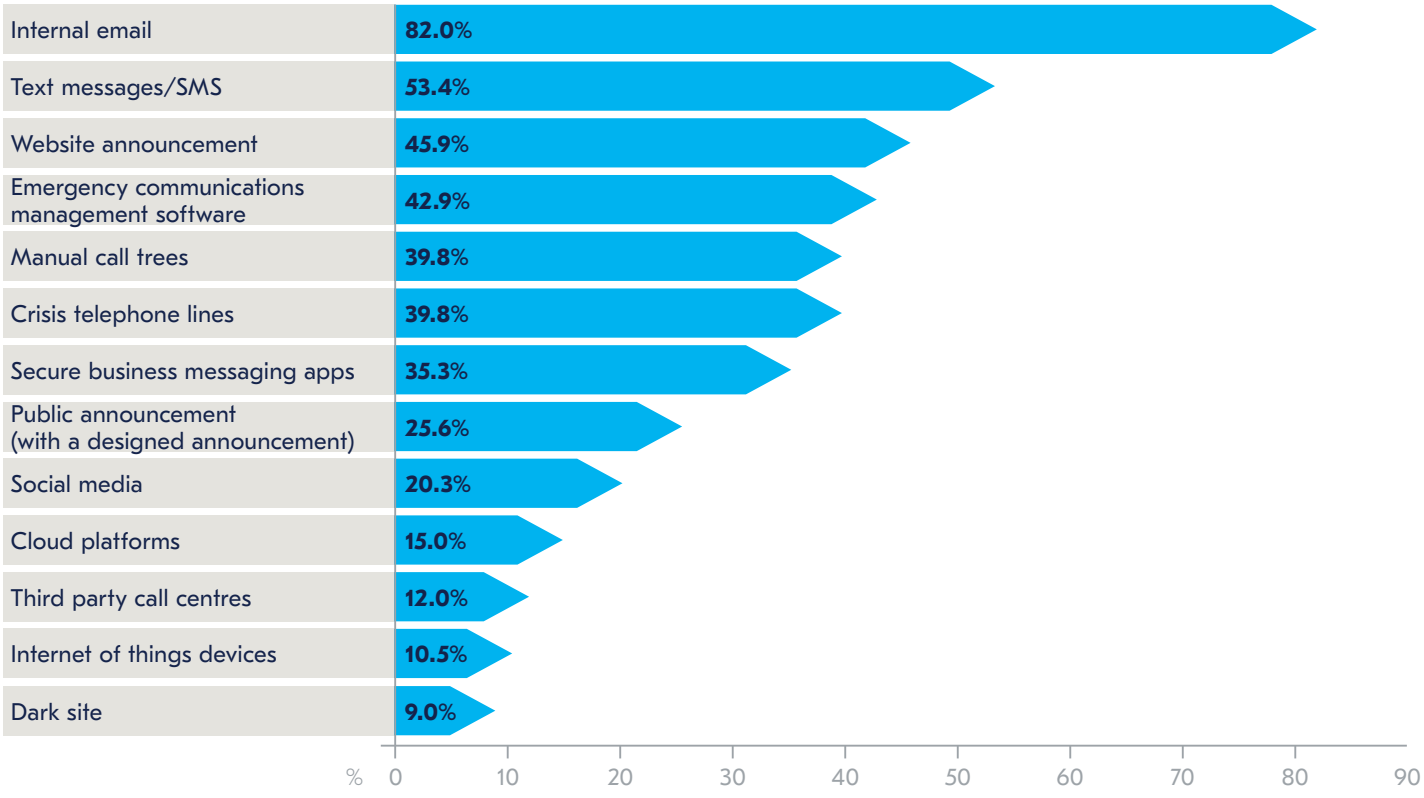


Figure 33. Which processes would you use to communicate to Internal stakeholders (e.g. customers, media) during each of the following scenarios?

Natural disaster

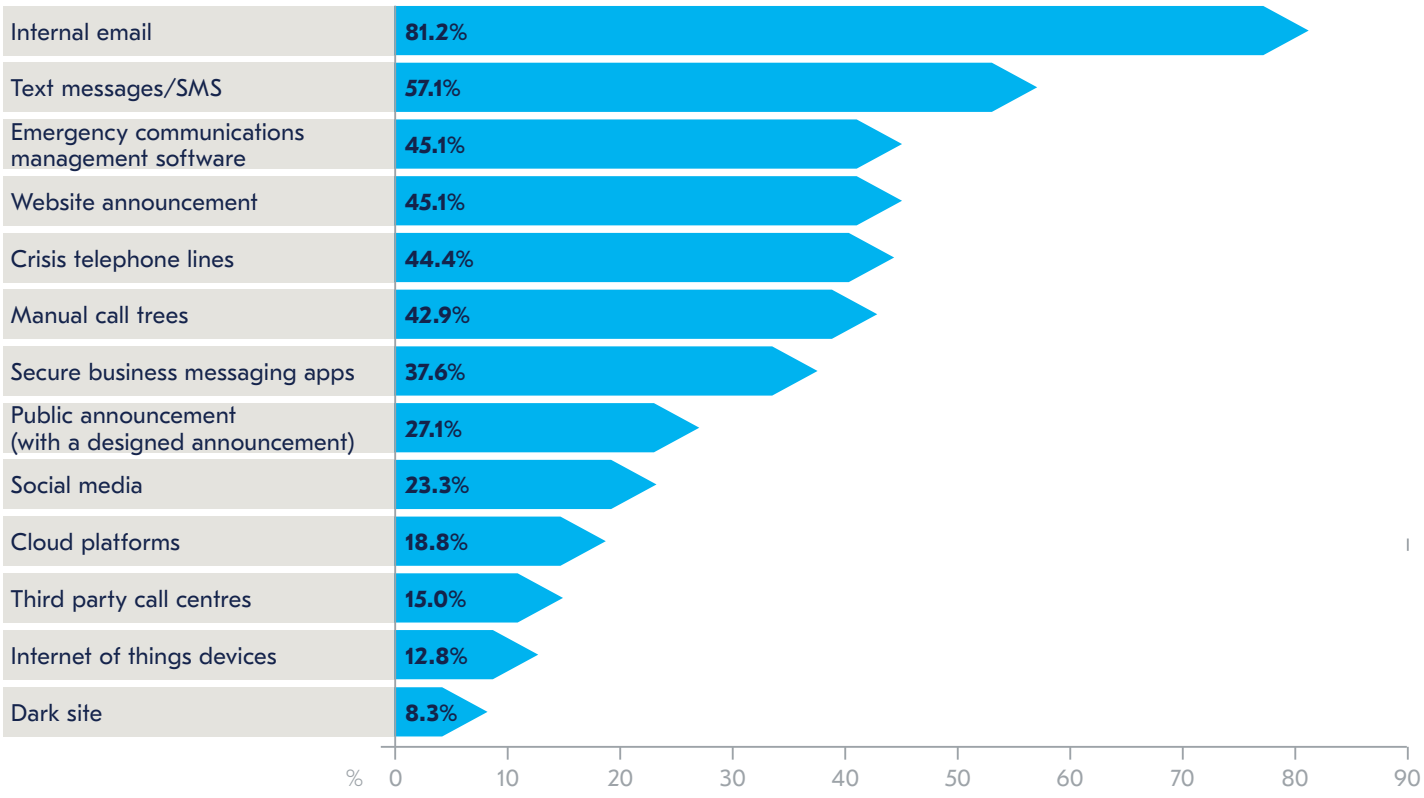


Figure 33. Which processes would you use to communicate to Internal stakeholders (e.g. customers, media) during each of the following scenarios?

The use of emergency communications management software is also fairly high for internal incidents, particularly for natural disasters where it would be used in 45.1% of incidents. During a major incident when buildings are destroyed and communications severed, emergency communications software can help to ensure staff get relevant messaging across multiple channels.

Whilst keeping staff informed is crucial during an emergency, staff also need to be aware of the critical importance of keeping company-sensitive information away from social media — however tempting it may be. According to a 2017 survey, 34% of organizations have reprimanded or fired an employee due to posts on social media[19], and even the CFO of Twitter was not immune to causing damage through inappropriate use of social media when he accidentally posted a direct (private) message on his public feed[20]. Leaking information on social media and not using the correct communication channels could cause a devastating impact on an organization's reputation and ultimately affect its chances of survival.

Many organizations, particularly those with many younger people on site, have issues ensuring that confidential information is not dispersed via unofficial channels. Universities, for example, frequently cite leaked information on social media as the most difficult issue during a crisis.

"You could say that the communications are not up to date with modern technology and modern practice; it's impossible to control the Facebook postings and tweets. We have an agreement between our emergency management team and the students' union that they should be at one for communications, particularly if there's a person's life involved. But that's only for the students' union, and many students are not members of it."

Risk Manager, Education, Ireland

Although staff should always be discouraged from posting information to personal social media accounts, some organizations curate communications carefully so staff have enough information to be able to inform those questioning but are very limited in the information they receive. Initial communications would normally inform that an incident is "occurring" but that it was being investigated and they would be informed in due course what the next stages are.

"In most cases, the first message is always an initial advice to staff along the lines of 'There's an issue, we're looking into it, we'll let you know what to do next'. We'll let you know what the next steps are."' We don't go into chapter and verse in the first instance. I think staff like to be informed of the situation, know that the right people are addressing it and what the likely impact is. So, we are really balancing the amount of information people get against the speed of communication; just to let them know so that they're aware. If the incident could impact the way that the company operates or on its reputation then, obviously, they need to be aware in case they're questioned by other people and don't have at least some of the story."

Group Business Continuity Manager, Financial Services, United Kingdom

19. Nauen, R (2017). Number of Employers Using Social Media to Screen Candidates at All-Time High, Finds Latest CareerBuilder Study. Career Builder [online]. Available at: http://press.careerbuilder.com/2017-06-15-Number-of-Employers-Using-Social-Media-to-Screen-Candidates-at-All-Time-High-Finds-Latest-CareerBuilder-Study [last accessed 15 January 2021].
20. Kleinman, A (2014). Twitter Exec. Accidentally Tweets Private Direct Message. Huffington Post [online]. Available at: https://www.huffingtonpost.co.uk/entry/twitter-cfo-direct-message_n_6218488?ri18n=true&guccounter=1 [last accessed 15 January 2021].

Annex

232

Respondents

51

Countries

14

Sectors

9

Respondent Interviews

46.1% Business Continuity

7.4% Crisis management

4.8% Emergency planning

3.5% Physical security

2.2% Communications

1.3% Information security

0.9% Line of business or service directorate

7.4% Real estate and construction

10.9% Risk management

6.1% IT disaster recovery/ IT service continuity

3.5% Health and safety management

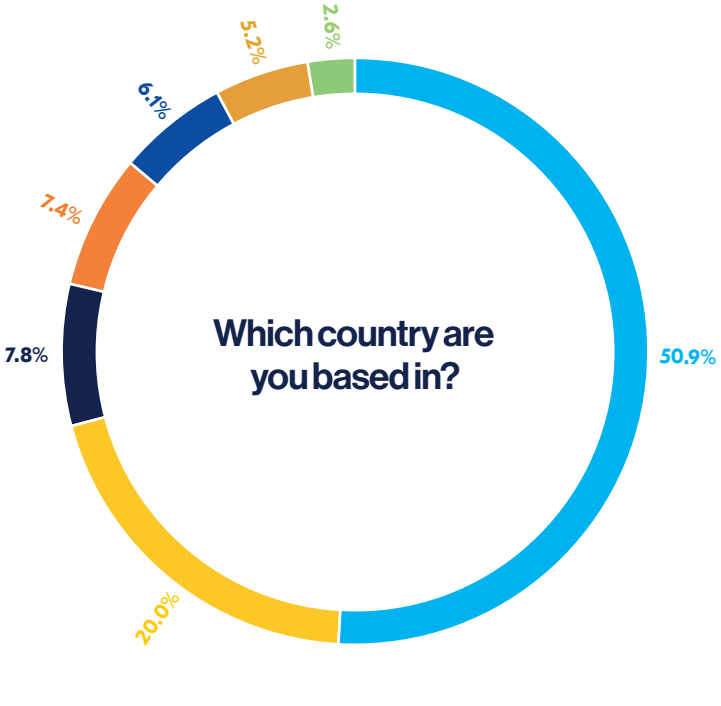
3.0% Top management

1.3% Quality/Business improvement

1.3% Internal audit

0.4% Supply chain and logistics

Figure 34. Which of the following best describes your functional role?



50.9% Europe

20.0% North America

7.8% Africa

7.4% Australasia

6.1% Asia

5.2% Latin America

2.6% Middle East

Figure 35. Which country are you based in?

25.2% Financial & Insurance Services
13.9% Professional Services
13.0% IT & Communications
9.1% Public Administration & Defence
6.1% Health & Social Care
4.8% Manufacturing
3.9% Transport & Storage
3.5% Education
3.0% Energy & Utility Services
2.2% Retail & Wholesale
1.7% Media & Entertainment
1.3% Engineering & Construction
0.9% Support Services
11.3% Other

Figure 36. Please indicate the primary activity of your organization using the categories below.

12.7% 1-10
2.2% 11-20
3.1% 21-50
2.2% 51-100
4.8% 101-250
7.0% 251 - 500
5.7% 501 - 1,000
29.3% 1,001 - 5,000
11.4% 5,001 - 10,000
7.4% 10,001 - 50,000
7.9% 50,001 - 100,000
6.6% More than 100,000

Figure 37. Approximately how many employees work at your organization?

About the Author

Rachael Elliott (Head of Thought Leadership)

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

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

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.

F24

About F24

F24 is Europe's leading Software-as-a-Service (SaaS) provider for incident and crisis management, emergency notification, as well as business messaging.

With FACT24 we offer a highly innovative solution that supports clients worldwide in the efficient and successful management of incidents, emergencies, and crises.

In addition, the eCall platform offers solutions for high-volume confidential communication within the corporate environment.

13 locations and more than 3,000 customers

Since being founded in 2000, the company has been based in Munich. From here F24 provides support through our subsidiaries in Zurich, London, Trondheim, Paris, Luxembourg City, Madrid, Belgium and Munich as well as our offices in Mexico City, Santiago de Chile, Vienna, Dubai and Auckland. F24 supports companies and organizations in over 100 countries around the world.

More than 3,000 clients worldwide rely on our SaaS solutions to meet their needs for crisis management or the daily communication of critical or confidential information. F24 clients operate in virtually every sector ranging from energy, healthcare, industry, finance, IT, Tourism and Aviation, through to a wide variety of public organizations. More than 20 years of experience have made F24 international experts on incident and crisis management as well as confidential communications.

Recommended by Gartner and ISO-certified

F24 is the first and only European company to be listed in the Gartner Report for Emergency/Mass Notification Services (EMNS). This listing in the Gartner Report means F24 is the first company based in Europe to meet the stringent requirements of this prestigious institute and this makes F24 one of the most relevant providers of EMNS worldwide.

In 2010, F24 became the first company worldwide to have the Integrated Management System for Information Security (ISMS) and Business Continuity (BCMS) certified by "The British Standards Institution" (BSI). Since then, F24 AG and the majority of its subsidiaries have been certified up to ISO/IEC 27001 and ISO 22301 standards.

In addition to annual audits by an independent accredited institution, successful re-certifications according to the international standards ISO/IEC 27001:2013 and ISO 22301:2012 took place in 2013, 2016 and 2019.

Contact F24

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

Ridlerstraße 57, 80339 Munich, Germany

Correct as of January 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