



Business Continuity  
Institute

# EMERGENCY COMMUNICATIONS REPORT 2020



Correct as of January 2020

# F24

Contents

1

Executive Summary

PAGE 5

2

Main Report

PAGE 10

3

Annex

PAGE 52



Foreword  
BCI



The BCI’s Good Practice Guidelines 2018 Edition makes it clear that one of the key requirements for an effective response structure includes the ability to communicate effectively with internal and external interested parties. During 2019, this sound principle received practical demonstrations by many organizations involved in crises around the world when their ability to communicate clearly, quickly and effectively was shown to be a vital success factor.

Achieving this capability is easier said than done, and the challenge is made harder in an increasingly complex world, where organizations engage with far-flung audiences, accessed via multiple channels and devices. In response to this demanding reality, the option to use technology to assist with the emergency communications task is understandably being adopted by more and more organizations.

The 2020 BCI Emergency Communications Report concentrates on these challenges and provides valuable knowledge to reveal how organizations respond. These insights are relevant whether you are an existing user of Emergency Communications tools seeking to benchmark and enhance your capabilities, or a newcomer keen to learn from the experience of other professionals.

There is much to be gained by reading through the full report including a raft of statistical analysis, but as a taster, some of the notable findings from the 2020 survey reveal:

- **An evolving infrastructure.** The survey shows a clear preference for SaaS (Software As A Service) as the most popular solution compared to using on-premise installed software.
- **Reducing activation time.** In 2019, just over a fifth of organizations reported they could activate their emergency communications response within five minutes. By 2020, this figure has grown to nearly a third of organizations.
- **A move towards localisation.** Global organizations are taking a more local approach to their emergency communications response. Although the central Response Team still plays an important role, more of the communications response is delegated to individual countries which helps with language and cultural barriers and can improve response rates.
- **More areas considered to be high-risk.** Increasing tensions in multiple hotspots across the globe mean more countries are identified as high-risk areas, which further emphasises the value of an effective emergency communications capability to support staff in previously peaceful areas.

I would like to again express the BCI’s thanks to F24, our continuing partner in producing the *Emergency Communications Report* this year. My sincere thanks are also due to all the respondents who kindly shared their data and real-world experiences with the BCI, which enables us to produce this insightful and practical report.

**Tim Janes**  
Hon FBCI  
Chair of the BCI



## Foreword

### F24

What can you really rely on? This question might sound rather generic, but it is a crucial question when it comes to situations that are not part of “business as usual”. When a business faces the inevitable emergency and crisis situation, this is when you discover how well the best placed plans and processes run in practice and how well people actually work together when the situation gets serious.



With regards to people that you can rely on, it is obvious that the key to success is a good team, especially in crisis situations. A successful team doesn't just happen by itself. The team needs time to evolve through, planning, training and exercising to enable high performance collaboration. The same is true for technology: it is unable to work independently without some level of human interaction. It's also like teamwork in that needs time to evolve. For example, we started using smartphones a few years ago and now they are such an integral part of our lives used for so many things in both personal and business life. Therefore the better we understand technology, the better and more uses we can get from it.

When it comes to emergency communications and crisis management, technological solutions provide the only way to handle these situations in an efficient and professional way. This is reflected in the results of this year's survey: two-thirds (67%) of organizations now use a software/tool for emergency notifications or crisis management which is an increase on the 59% on last year's report. Using specialist solutions does not just enable a faster response, but also has additional benefits which can be invaluable in an emergency.

I remain convinced that professionals working together with sound, properly implemented technology can handle critical situations far better than without it. Even so, technology is often seen as a double-edged sword where the more we rely on it, the more we become dependent on it. This brings up several questions: Will it really work every time? What if the system fails or goes down at some point? These are all crucial questions which need answering before technology solutions are implemented.

The current global situation means these questions are becoming much more important. Availability and reliability of services are key, especially in the area of emergency communications and crisis management. This is true for the whole lifecycle: from planning, through to alerting, communicating and finally documenting. When it comes down to the crunch, people are only going to trust the technology if they can rely on it to support them effectively and at all times.

Furthermore, trust is best built on knowledge and experience. With F24, our technical knowledge ensures software always runs with a failsafe and redundant backup procedures, coupled with our experience of proven long-term high availability of critical communications. The knowledge of the BCI is also the reason why we at F24 are delighted to continue our partnership for the creation of this well-established Emergency Communications Report. We hope you will get a lot out of the data and analysis provided by this edition of the report. The most important aim of this research is to support you as professionals in your work, whether it is to optimise your processes, get inspiration or benchmark the current situation in your organization. Have a good read!

#### Christian Götz

Co-founder of F24 AG, Member of the Executive Board and responsible for Sales, Marketing and HR


# 1

## Executive Summary




Executive Summary

More organizations than ever before are using specialist tools or software within their emergency communications plans:

 **Two-thirds of organizations (67.0%)** are now employing specialist tools and/or software within their emergency communications plans. This compares to under half (**49.0%**) just two years ago.


Organizations are getting faster at activating their emergency communications plans:

 **Nearly a third (32.4%) of organizations** organizations can now activate their emergency communications plan within five minutes which compares to **21.3%** in last year's survey. The increase in activation speed can be primarily attributed to two reasons:

- 1 increased deployment of technology within plans;
- 2 an uptick in the amount of training and exercising of emergency communication plans.


**61.7%** of organizations now carry out regular exercising of emergency communications plans compared to **49.0%** only two years ago.

It is people, rather than technology, which is the primary cause for plans to fail:

 Gathering, validating and sharing accurate information was rated as the greatest challenge by respondents in 2019, with **58.4%** rating it as a key challenge.

The second highest-rated challenge was communicating with staff at **54.2%**. Given only **61.2%** of organizations regularly ensure employee contact details are kept up to date, it is hardly surprising that these two challenges are rated so highly.

Natural disasters and adverse weather are the most common reasons for activating emergency communications plans:

 Natural disasters/adverse weather accounted for over half (**50.2%**) of all activations of emergency communications plans in 2019, with IT/telecom outage just behind at **49.6%**.

Given the increasing reliance on technology in emergency communication plans, it is vital that organizations ensure procedures are in place to activate plans in the event of a technology or telecoms outage.

Tools and technology

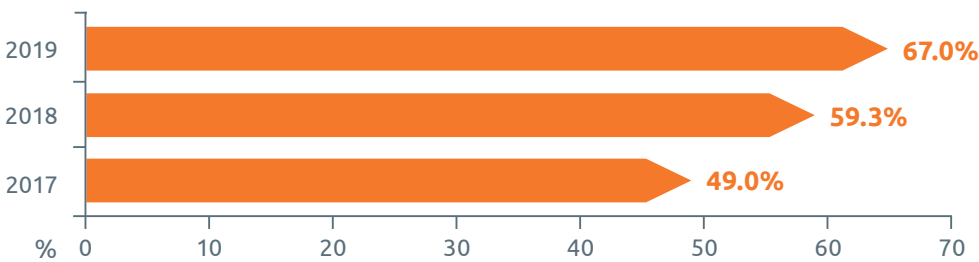
Mobile phones and computers are the primary devices used in emergency situations, although one-way communications still have their place

Percentage of organizations using devices in emergency situations



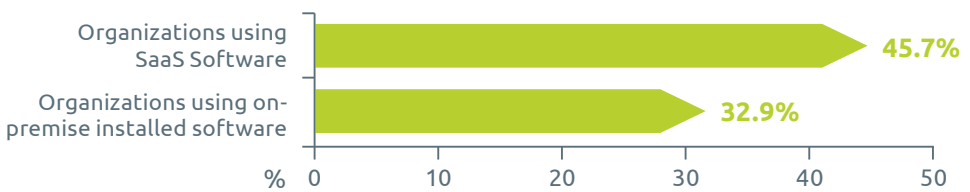
More organizations than ever are now using specialist emergency notification or crisis management tools and software

Percentage of organizations using specialist emergency notification/crisis management tools or software



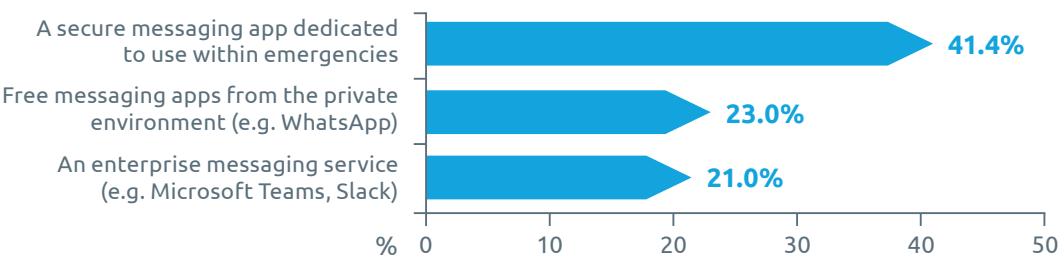
Organizations using software-as-a-service (SaaS) technologies can activate their emergency plans quicker than those using on-premise installed software

Percentage of organizations able to activate their emergency communications plans within five minutes



Nearly half of organizations are now using a secure messaging app dedicated to use within emergency situations, but use of free messaging apps is still high

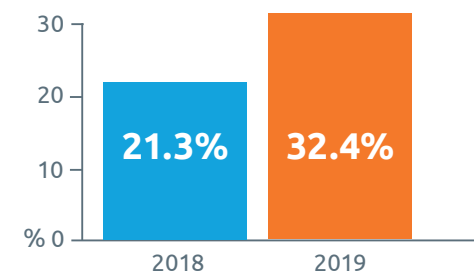
Types of messaging apps used to manage emergency notification processes



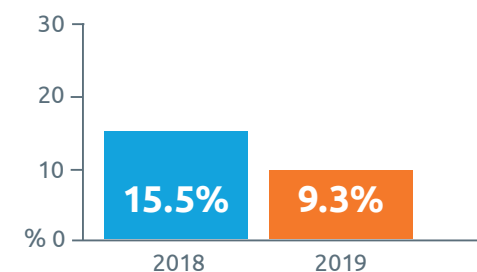
## Activation time

Organizations are getting faster at activating their emergency communications plans

Number of organizations who can activate emergency comms plan within five minutes



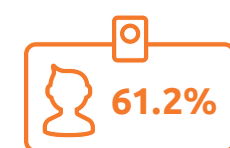
Number of organizations who take over an hour to activate their emergency communications plan



## Inhibitors to plans operating effectively

It is people, rather than technology, that are the greatest inhibitor to an emergency communications plan operating effectively

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

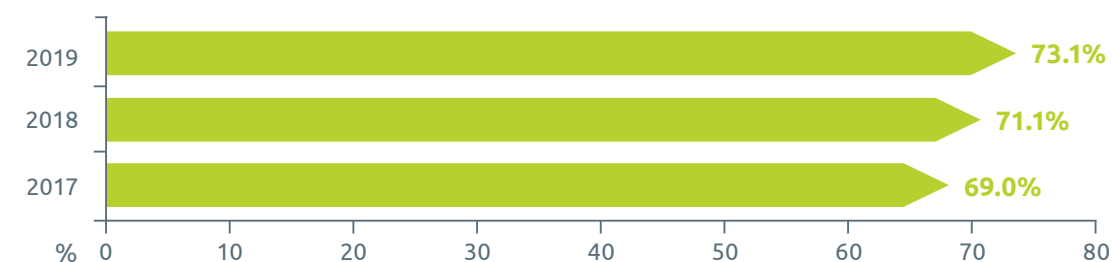


Despite accurate information being the primary cause for plans failing, less than two-thirds of organizations ensure employees' contact details are up-to-date

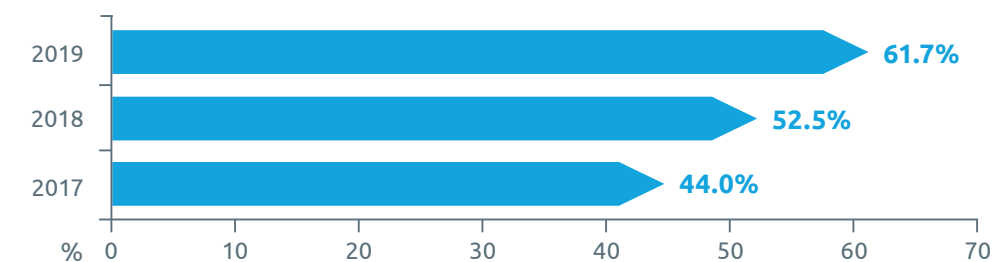
## Reaching response levels

Higher levels of training and exercising coupled with continued investment in communication technologies means more organizations than ever before are meeting their expected response levels

Percentage of organizations achieving their expected response levels

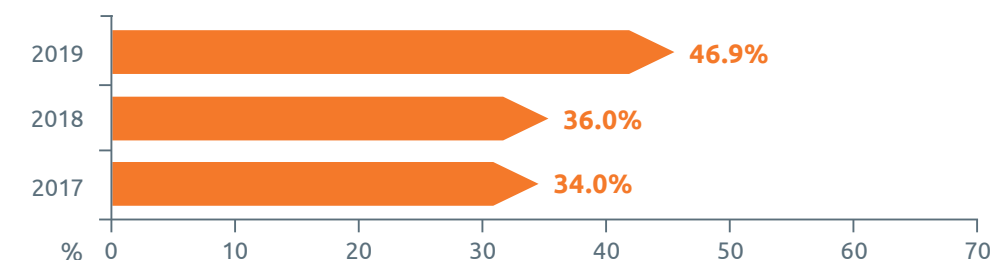


Nearly two-thirds of organizations are now carrying out regularly scheduled training programmes for emergency communications plans



## International travel

Nearly half of organizations have staff travelling to high risk countries



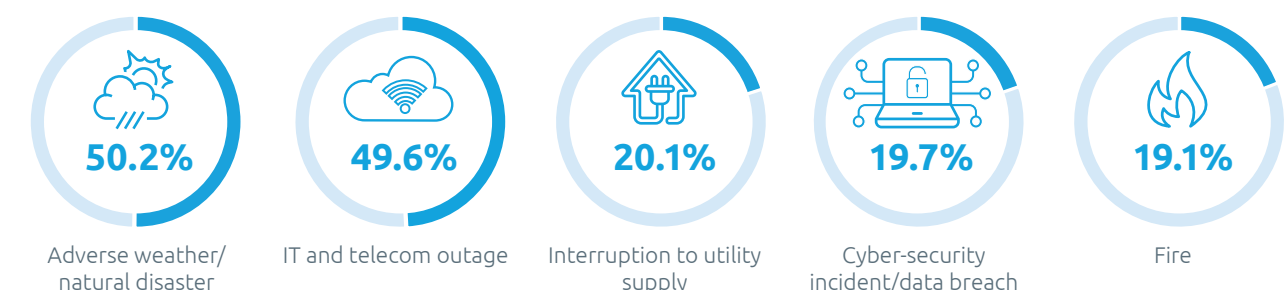
Despite an increasing number of staff travelling to high risk countries, preparations for staff travelling abroad is low

How does your organization ensure the safety of remote/travelling staff?



## Emergency communications plan triggers

Adverse weather and natural disasters account for over half of the triggers for implementing emergency communications plans





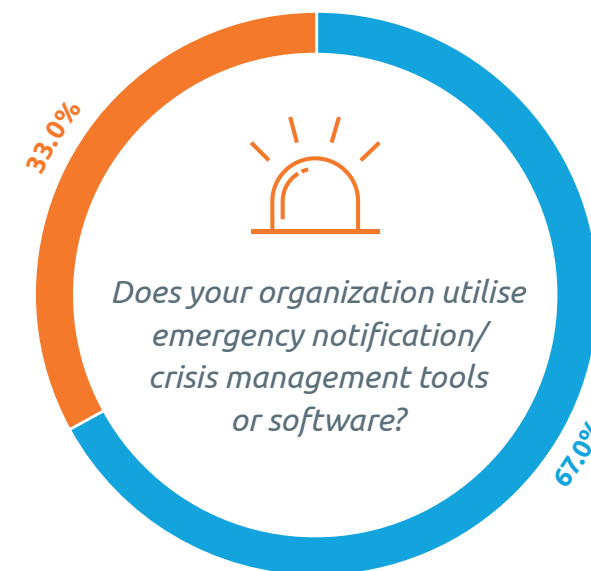
## 2

## Main report

## COMMUNICATION PROCESS

- Two-thirds of organizations are now using emergency notification or crisis management tools/software.
- Mobile telephones and laptops are the most frequently used devices in an emergency scenario, with one-way communication solutions (such as public address systems and pagers) still having their place.
- Lack of budget is the most cited reason for not using a tool, although increasing use of software-as-a-service (SaaS) tools is helping companies to better manage the cost of implementing cross-platform solutions.

The number of organizations using emergency notification and/or crisis management tools or software has increased for the third year running to 67.0% (2018: 59.3%). We noted in last year's report that nearly half (48.2%) of organizations felt that free apps such as WhatsApp were not fit for purpose within their organizations, and follow-up interviews confirmed this to be the case. This rise in popularity of using specialist emergency notification and crisis management platforms shows that many organizations have decided to switch to specialist tools rather than rely on the free options available ([discussed further under Tools and Solutions](#)).



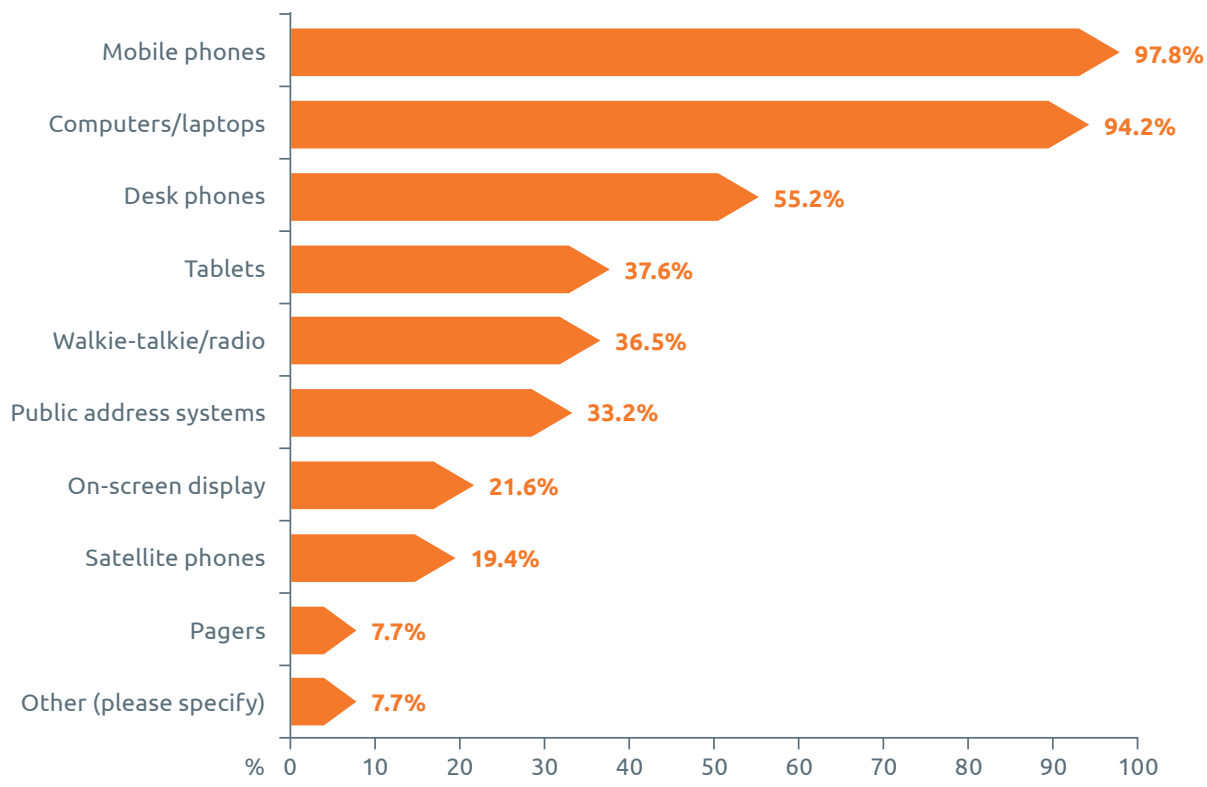
67.0%  
Yes

33.0%  
No

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

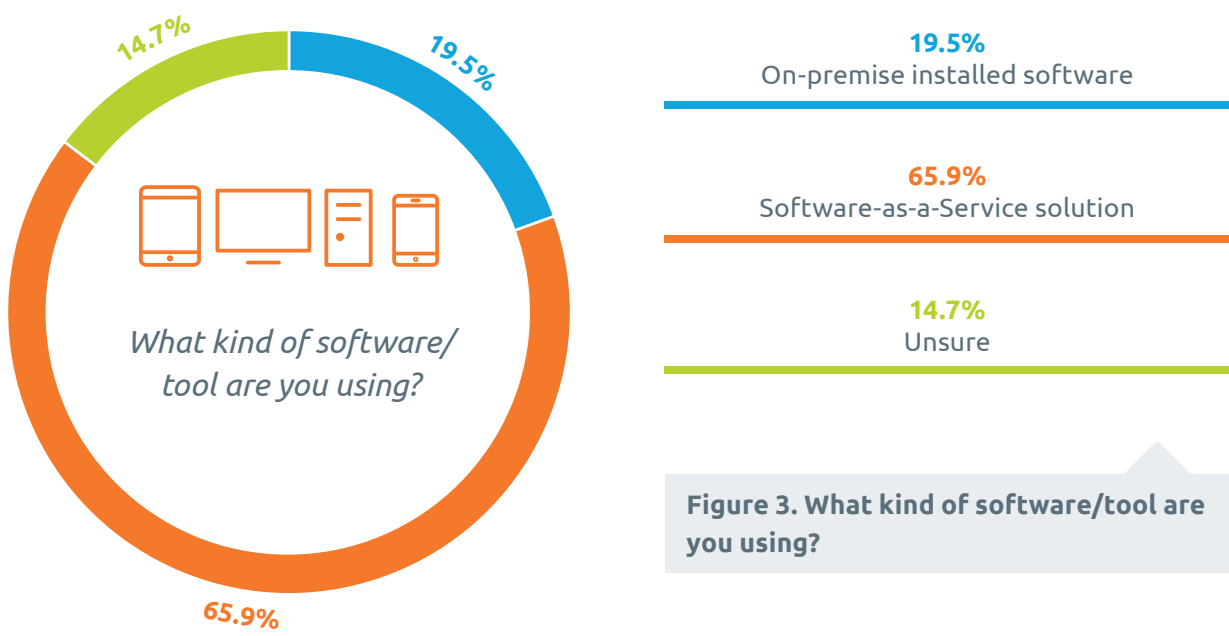
Of the tools used by organizations to manage emergency situations, mobile phones and computers/laptops are the most used tools, with 97.8% and 94.2% of respondents using these devices respectively. Just over a third of organizations are continuing to use radio communications/walkie talkies (36.5%), while 33.6% of organizations use public address systems demonstrating that one-way communications still have their place in an emergency. Pagers are, however, starting to see their popularity waning, with just 7.7% of organizations now using them.

Satellite phones, which can help to overcome mobile outages, are used by less than a fifth of organizations (19.4%). Given that 28.0% of organizations fail to reach their accepted response levels due to the unavailability of mobile networks, more widespread use of satellite phones could help to overcome the difficulties experienced with network unavailability. However, with satellite phones still being prohibited in some countries (such as India), it cannot be a universal solution for global organizations.



**Figure 2. What are the devices you are using to manage emergency situations?**  
Tick as many as applicable

With many organizations now using a variety of different devices in an emergency, an increasing number are preferring to use software-as-a-service (SaaS) solutions rather than on-premise software solutions. Nearly two-thirds of organizations (65.9%) are electing to use a SaaS solution, whilst under a fifth (19.5%) are using on-premise installed software. A SaaS solution can help to deliver a seamless emergency communications plan across multiple devices and can also help surpass the problem of adopting a new solution on legacy systems, an issue highlighted as a barrier to adoption by over half (51.2%) of respondents in the BCI 2019 *Disruptive Technologies Report*. However, many organizations would be advised to consider the benefits of employing SaaS solutions: 45.7% of organizations who use SaaS software report being able to activate their emergency communications plan within five minutes compared to just 32.9% who use installed software.



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







45.7%  
Organizations using SaaS software

32.9%  
Organizations using on-premise installed software

Figure 4. Percentage of organizations able to activate emergency communications plan within five minutes

Lack of budget is the most frequently cited reason for not employing an emergency communications tool, with over a third (36.4%) reporting they had no budget allocated to such tools. Just under a fifth (19.1%) felt their organization was too small for such a tool to be adopted. Interestingly, despite the lower levels of adoption of technology amongst organizations employing less than 1,000 people (58.8% use emergency notification and crisis management tools vs 67.0% for all organizations), the same percentage of organizations managed to achieve their expected response rate showing that the lack of a tool did not impact response levels. The reasons for this are twofold: 1) information transmission being easier within smaller organizations, particularly those who are located on one site with very few travelling staff; 2) smaller organizations having different definitions for response levels and have differing requirements from larger organizations.

TIMING

- Emergency communications plans are being activated faster this year: just under a third can activate their plan within five minutes, compared to a fifth in 2018.
- Incidents occurring out-of-hours where staff availability is low are more likely to see a delayed response.
- The increased levels of remote working are having no impact in the time it takes for top management to be provided with initial information: over three-quarters are alerted within an hour, compared to two-thirds in 2018.

Organizations have become much faster at activating their emergency communications plans in the past year. This year, 32.4% of respondents claimed their organization was able to activate its emergency communications plan within five minutes, up from just over a fifth (21.3%) in 2018. Furthermore, a small but significant minority (1.6%) claimed activation took zero time due to an automated response based on an IT event/rule. Only 1.0% of organizations reported that it took over 12 hours to activate their emergency communications plan, down from 2.4% in 2018. Furthermore, just 2.6% of organizations reported not having an emergency communications plan (2018: 3.9%).

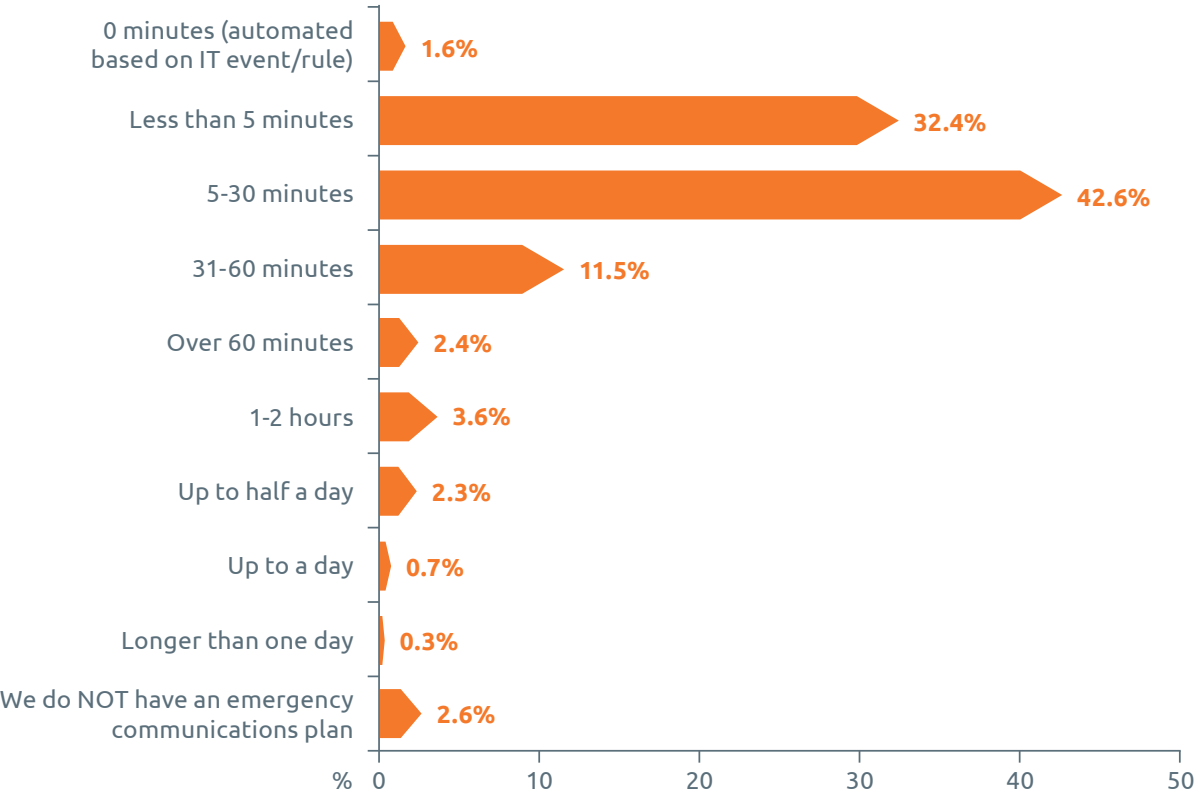


Figure 5. On average how long does it take to activate your emergency communications plan?





It is important to understand that an event can escalate and de-escalate slowly or in a matter of seconds. It is therefore good practice to activate emergency communications plans earlier rather than later as they can be managed in a more co-ordinated manner and may reduce complications when trying to activate later.

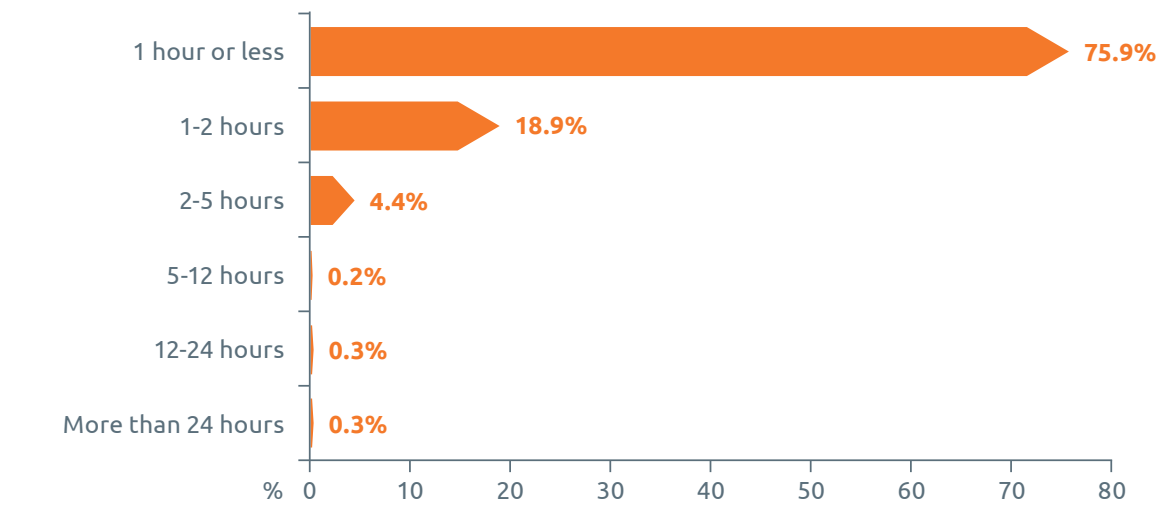
*[Response times] depend on the availability of the persons. I don't know why, but in the two days we have off during the week, more incidents happen. I would say 40% happen during the weekend. Ideally, we would ask that staff be more available, but this is always a problem. Some are more available; 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 now to the holiday season, this can be where the failures happen."*

**Security Manager, Professional Services Organization, Switzerland**

Some organizations also find they fail to meet their emergency communications plan response levels due to incidents occurring at times when staff are away from the office which can cause activation to be delayed significantly. Tracking such situations can help organizations to better plan for out-of-hours incidences occurring and put plans in place to ensure a faster response time can be achieved in future.

Another encouraging result from this year's survey is the decrease in time taken 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 information to top management within an hour. This year, over three-quarters (75.9%) reported the same. Furthermore, just 0.7% claimed it would take longer than 12 hours compared to 2.1% in 2018. Such an increase is exceptional given the increasing trend for staff to work remotely which could potentially lead to difficulties in contacting top management: Global Workforce Analytics produced research this year which showed that the number of people who are able to work remotely has grown by 173% since 2005<sup>1</sup>.



**Figure 6. On average, how long does it take you to provide initial information on a crisis to top management?**

The speed at which plans can be activated also correlates closely with whether an organization uses emergency communications software. 42.2% of organizations that use emergency communications software can activate their plans within five minutes, compared to 34.0% who do not use software. Furthermore, 80.2% who use specialist software can provide top management with information within an hour compared to 75.9% who do not.

	Organizations using emergency communications software	Organizations <b>not</b> using emergency communications software	% difference for those using software vs those who do not
Percentage activating plans within 5 minutes	42.2%	34.0%	+8.1%
Percentage providing top management with information within an hour	80.2%	75.9%	+4.3%

**Figure 7. Percentage of organizations able to activate their emergency communications plans within five minutes and reporting information to top management within an hour**

With the increasing adoption of advanced warning tools, escalation to management can now be made automatically based on an IT event/rule without the need for staff intervention. Whilst this can obviously increase the speed at which information is relayed to top management, many organizations are likely to be reluctant to employ such tools, believing information dissemination should be made by humans: just 4.0% of those surveyed for the BCI 2019 *Disruptive Technologies Report* were completely comfortable with machines making decisions in the place of humans; the figure rising to 36.8% if decisions were shared immediately with humans for review. Furthermore, management may want information fully corroborated before it is passed to them.

Nevertheless, the trend for speed of information transmission is clearly increasing which is a positive step in terms of the effectiveness of emergency communications plans.



<sup>1</sup> Global Workforce Analytics 2019, Latest Telecommuting/Mobile Work/Remote Work Statistics, Global Workforce Analytics, Last viewed 12 December 2019, <https://globalworkplaceanalytics.com/telecommuting-statistics>

# KEY COMMUNICATION CHALLENGES DURING AN EMERGENCY

- It is people, rather than technology, which is the primary challenge for ensuring effective execution of an emergency communications plan.
- Gathering, validating and sharing accurate information is the greatest challenge to organizations during an emergency response, with communicating with staff at second place.
- Whilst technology does have its place in ensuring an effective response, it can also lead to reputation issues if communications are not controlled during a crisis; a major concern for a third of respondents.

Gathering, validating and sharing accurate information was rated as the greatest challenge by respondents this year when asked what their key challenges were during an emergency incident. Over half (58.4%) considered this to be their greatest challenge. The greatest challenge in 2018, communicating with staff, has subsequently dropped to second place this year after 54.2% of respondents rated it as one of their key challenges. Despite the two options changing places at the top of the table, both saw significant drops compared to 2018: communicating with staff was selected by 77.4% of respondents in 2018, and gathering, validating and sharing accurate information by 69.4%.



Figure 8. What are your top three key challenges during emergency notification/crisis management?



As with last year however, it is clear it is people, rather than technology, which is the greatest inhibitor to emergency communications plans running effectively: the lack of reliable and accurate information is the primary issue for organizations in an emergency and keeping records up-to-date and ensuring staff are contacted via a medium they are familiar with is vital. Regular exercising can help to expose where information and communication gaps lie and, whilst many organizations are following good practice and regularly exercising, there are a significant proportion who do not. The section *Exercising Emergency Communications Plan* provides further detail around organizations' training and exercising programmes.

*"One of the main things I would be concerned about is making sure that the database of contact information in the emergency notification system is regularly updated. Specifically, whenever an employee joins the company, leaves the company, or changes his or her role within the organization the notification system database should be updated and refreshed as soon as possible. That way, at any given moment, the emergency notification system has an accurate database of contact information for all employees."*

**Independent Business Continuity Consultant, United States**



*"I exercise the call trees quarterly which pulls a report out of the system that shows every bad cell phone number. Furthermore, in financial services, a lot of my guys are contractors and the HR systems usually will not send over the contractor information. I've encountered this across basically every system over my career, and I've been doing this for years. A priority therefore is chasing all the contracted staff to make sure their numbers are up to date. Another issue is with Senior Execs, because they have all their numbers blocked as they don't want anyone to know their numbers. In my role, I therefore have to manually do it in the system. The manual upkeep of it is therefore a big challenge. Also, with a lot of the rules on the privacy, it's really tough."*

**IT Director, Insurance Organization, United States**

*"To me, without some sort of an organized and documented process for doing that, there's a real risk of employees and other stakeholders in the organization not knowing what's going on, not knowing how the organization is responding to an emergency, what they're actively doing, what kind of recovery activities they're doing, or what people are doing because people are the lifeblood of any organization. It's essential to have a documented and frequently exercised process for emergency communications. Even if it's something as simple as the emergency system sending out a message to everybody's mobile phone once a month, for example, that should be sufficient."*

**Independent Business Continuity Consultant, United States**

*"Even in our text messages to staff we've got built-in reminders that official communications will come out, and don't tweet stuff. It's actually built into the standard announcements that we use to remind people."*

**IT Director, Insurance Organization, United States**

*"The reaction to social media is very fast. If the fake news becomes widespread then this may lead to a very big disaster for us, especially nowadays in Hong Kong."*

**Security Consultant, Hong Kong**

Many organizations rely on HR to provide accurate contact information which can provide another point of failure, particularly for contract staff. Furthermore, some senior executives are reluctant to provide personal contact details to global systems, and GDPR regulations also mean it is much more difficult for organizations to share employee information, even internally.

A further example of the human factor causing a challenge during an emergency is getting staff to follow planned procedures: nearly half (49.1%) saw this has one of their key challenges during an emergency. Again, rehearsing a plan and exercising frequently is the most effective way of ensuring this happens, but those who were interviewed for this report also cited the importance of having an organized and documented process in place, as well as frequent messaging to staff to raise the awareness of an emergency communications plan.

A final issue which is of increasing priority is around external communications: in an era of fake news and social media, a message on social media from a misinformed member of staff regarding an emergency situation can quickly escalate into a major news story which can potentially lead to loss of customers and have a detrimental impact on a company's balance sheet. Indeed, nearly a third (32.0%) of those surveyed considered controlling external communications to be a key challenge during an emergency, with communicating with customers and other stakeholders being a challenge selected by 38.1% of respondents. Ensuring staff are briefed about social media best practice as part of an emergency communications plan is vital to ensure external messaging is controlled effectively.

## TOOLS AND SOLUTIONS

- **Nearly half of organizations (41.4%) now have a secure messaging app integrated into their emergency communications plan.**
- **Free messaging apps are still used by nearly a quarter of organizations, but over half of these know they are not the optimal solution. However, in some scenarios, applications such as WhatsApp are still being used with positive effect.**
- **The ability to collaborate and exchange information with an emergency communications tool is valued as more important than the ability to effectively transmit one-way communication.**

Close to half of organizations (41.4%) are now using a secure messaging app dedicated for use within an emergency as part of their emergency communications plan.. 12.7% find that an enterprise messaging service (e.g. Skype, Teams, Slack) suffices for their emergency communication needs, whereas 8.3% of respondents using such messaging services feel it is not effectively integrated into an emergency communications plan. A significant minority (10.7%) are continuing to use free messaging apps from the private environment (e.g. WhatsApp, WeChat) and believe it suffices for their needs, with a further 12.3% using these apps but realising they have limitations within an emergency situation.

Whilst free tools can have their place within an emergency scenario (e.g. providing staff with a tool where they can contact colleagues for support in the aftermath, or keeping in touch if staff are displaced after an emergency), the use of such a tool during an emergency can be limiting: a lack of audit trail means it cannot be determined whether staff have viewed a message and its reliance on a functioning data network means such a system may become redundant in the event of a network outage. Security concerns about using free applications coupled with concerns about data privacy can be additional deterrents to universal adoption by an organization. Furthermore, the availability and functionality of free tools may be impacted at times when usage is high (such as New Year's Eve or during a major news event).

A surprisingly high 8.1% of respondents reported they did not use messaging apps as felt they were not helpful, and the percentage answering this was similar across all company sizes. This demonstrates that even in some of the world's largest organizations, messaging apps are still failing to be implemented effectively or, in some cases, the benefits of using an application have failed to be realised.

*"Within this company, I doubt [they'll be using WhatsApp]. Being in the financial services sector, the security concerns mean they're not likely to do it. In this organization, they are very much against using Shareware or freebies of any type. The concern is that as an organization with deep pockets, you're going to be targeted by attacks."*

**IT Director, Insurance Organization, United States**

*"within an organization, there may be a growing reliance on various apps nestling within devices allowing access to everyone from their devices. They could be at risk for poor mass communications."*

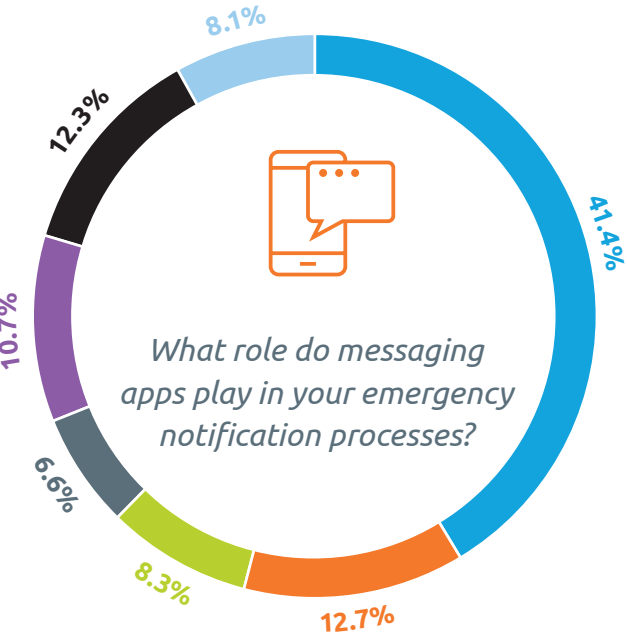
**Resilience Professional, Education Sector, Australasia**

*"We cannot count on WhatsApp as certain global regions cannot be trusted for reliability due to high risk levels and therefore need to use our own formal tools."*

**Security Manager, Professional Services Organization, Switzerland**

**41.4%**  
We're using a secure messaging app dedicated for the use within critical situations and integrated into our emergency communications solution.

**12.7%**  
We're using our enterprise messenger (e.g. Teams, Slack, Skype) and we are happy with it.



**8.3%**  
We're using our enterprise messenger (e.g. Teams, Slack, Skype) but feel it needs better integration with the alerting scenarios.

**6.6%**  
We would like to use messaging apps but there are no fitting solutions compliant with data protection requirements etc.

**10.7%**  
We're using free messaging apps from private environment (e.g. WhatsApp, WeChat) and we are happy with it.

**12.3%**  
We're using free messaging apps from the private environment (e.g. WhatsApp, WeChat) but we realise that's not the optimal solution

**8.1%**  
We don't use messaging apps as we don't think they are helpful

**Figure 9. What role do messaging apps play in your emergency notification processes?**

When considering the importance of certain aspects in the functionality of an emergency communications tool, collaboration was the mostly highly valued asset by professionals. 79.8% of those surveyed rated the ability of a tool to “enable expert teams to collaborate easily and in real time” as “extremely” or “very” important, whilst “constant exchange of information to enable decision making” was rated “extremely” or “very” important by 77.4% of respondents. As a contrast, one-way communication (via tannoy systems or pagers) was given the same rating by only 58.0% of respondents.

Collaboration in an emergency can help to achieve a more holistic response, as well as ensuring designated people across the organization are both kept informed of the situation and can help to input on a departmental or geographical level. The BCI 2019 *Organizational Resilience Report* discussed how delegating control in an emergency scenario can lead to a quicker and more effective response, and it is encouraging to see that professionals are considering this in their emergency communications technology.

Furthermore, we are now seeing professionals valuing some of the more contemporary aspects of emergency communications tools and software: location-based services, for example, are seen as “extremely important” by nearly a fifth (18.4%) of respondents whereas the ability to personalise functionality for different groups of people is seen as “extremely important” by nearly a third (29.9%).

*“Sometimes managers recommend to travellers when they’re going to remote areas or high-risk countries, to enable the geofencing feature in case of emergency. This means we can help them quickly and we can know where they are. This is something that we wanted to have on our emergency communications tool. For example, we regularly hold events in big cities such as Tokyo, London, New York or Boston; there are around 20 to 40 cities at any one time that have more than 1,000 travelling staff there, not including the local staff. So, if we have an emergency situation, we will have to reach out to those 1,000 travelling staff as well as the 12-15,000 local staff. These high numbers cannot be supported by all of these different kinds of free apps or systems and geofencing would really help.”*

**Security Manager, Professional Services Organization, Switzerland**

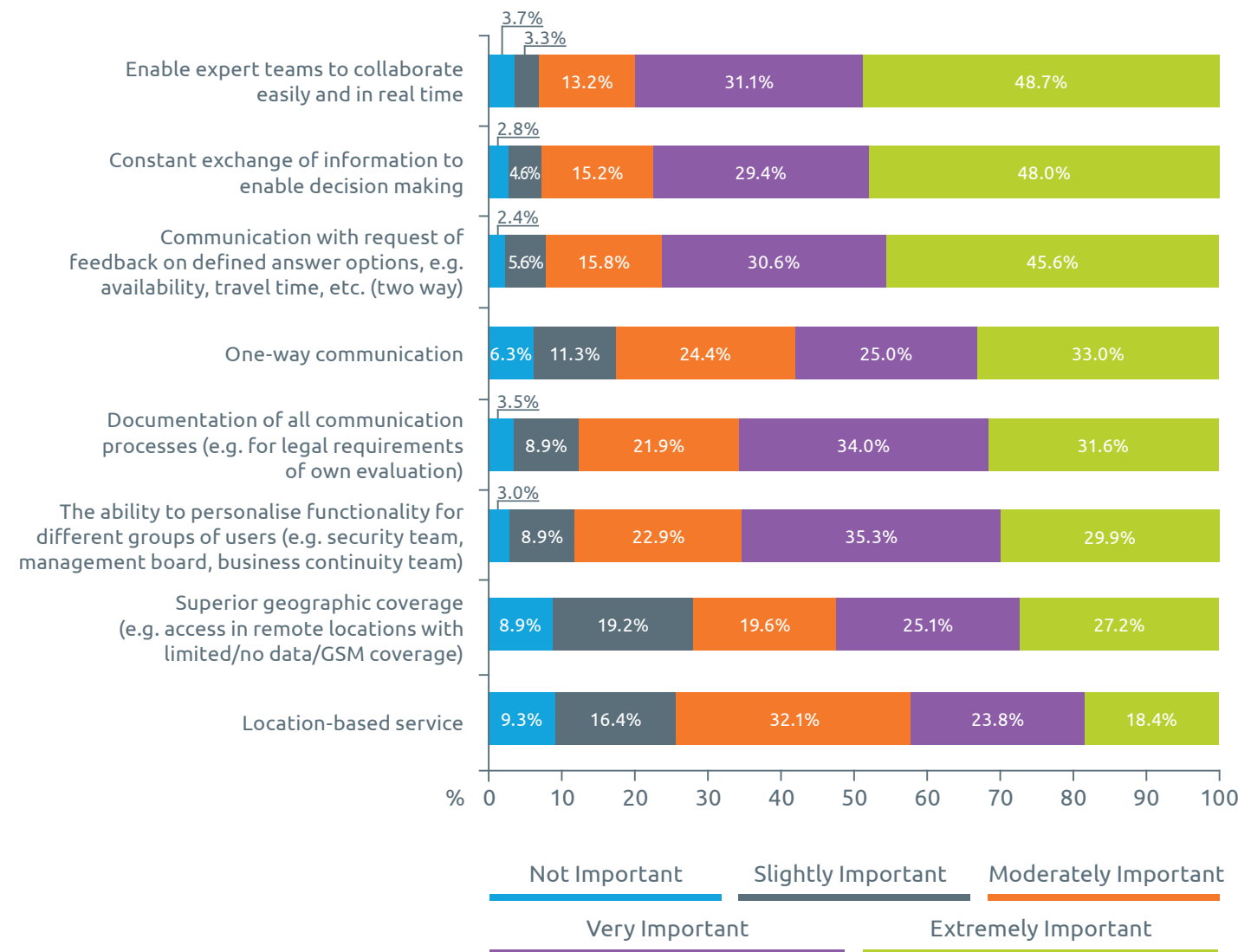
*“For this kind of [emergency message], more than 75% are using [the Chinese version of] WhatsApp. It also works with specific customers, particularly in China. We have a group for them too.”*

**Security Consultant, Hong Kong**

Although dedicated messaging apps help to provide comprehensive solutions to managing emergency communication requirements, there are some situations where free apps have their place. A Hong Kong-based communications professional interviewed for this report claimed that free chat tools had such universal use in China, their use as a communications tool was particularly effective. Elsewhere, interviewees discussed how it could be used as a fall back if other communications failed.





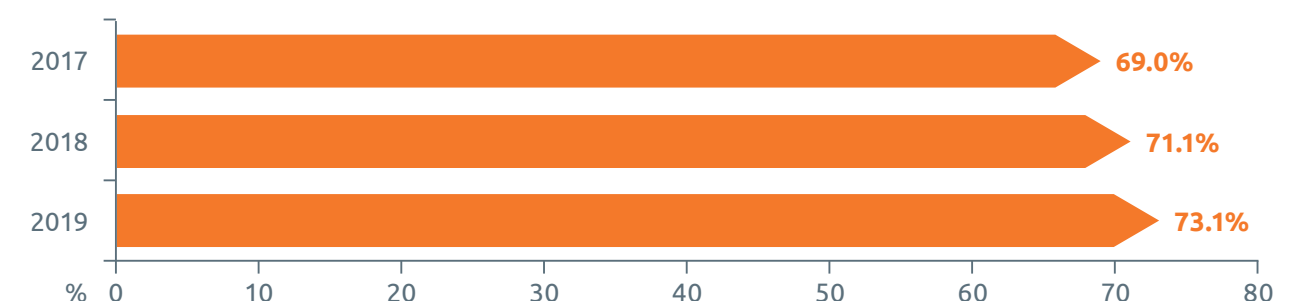


**Figure 10. How important are the following aspects for your alerting and emergency communications? Please rate on a scale where 1=not important and 5=extremely important**

## INCIDENT PREPAREDNESS

- **More organizations than ever (73.1%) are achieving their expected response levels due to higher levels of investment in technology and increased dedication to training and exercising.**
- **Human error is again the primary cause for plan failure, with lack of accurate staff information and lack of understanding the top causes for failure.**
- **More organizations are carrying out regularly scheduled training programmes for staff, and fewer than a quarter of organizations (24.8%) are now only carrying out training in an ad-hoc manner (2018: 36.0%).**

73.1% of organizations reported they achieved their expected response levels in 2019 which demonstrates a continuing level of improvement: in 2018, 71.1% achieved their expected levels, and 69.0% in 2017. Continued investment in emergency communication technologies coupled with an increased dedication to training and exercising are having a tangible impact on the effectiveness of emergency communication plans.

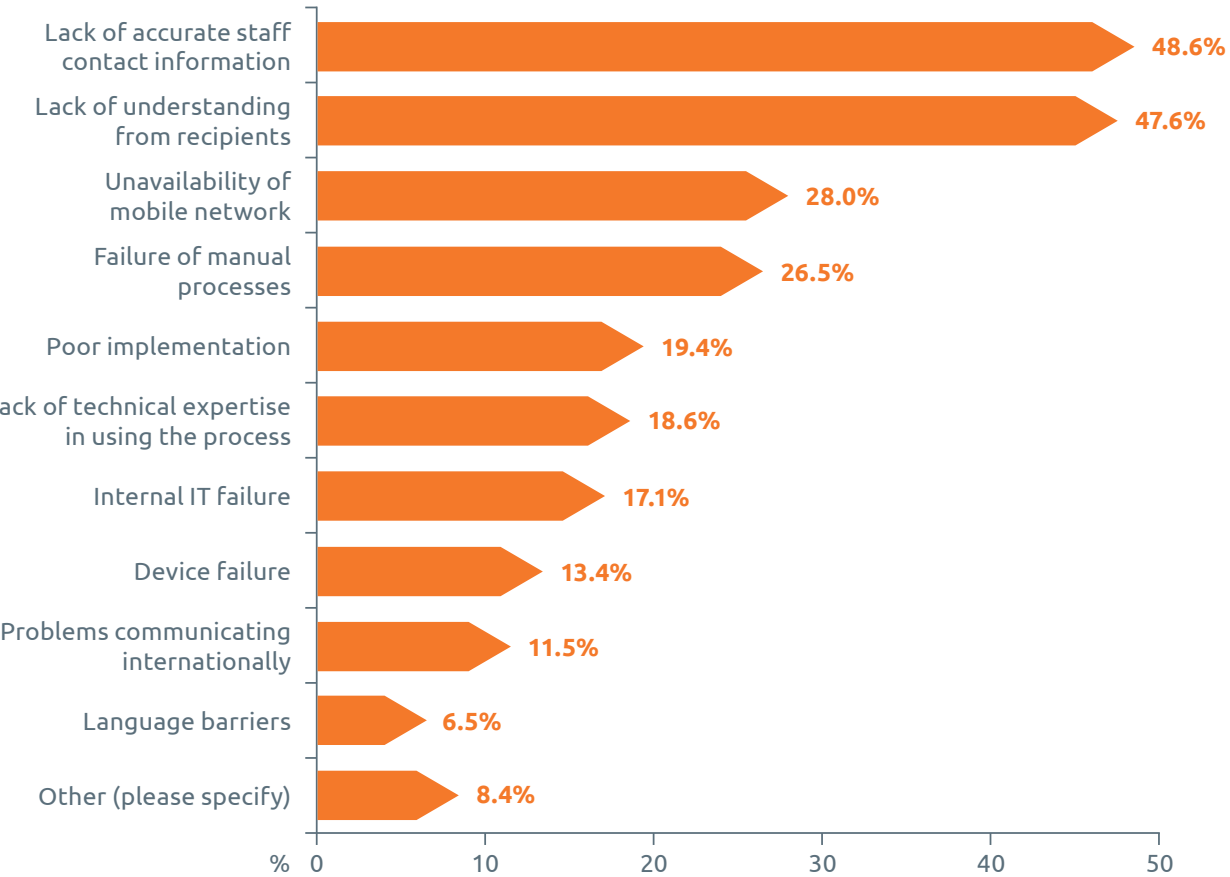


**Figure 11. How often have you achieved your expected response levels?**

Once again, however, it is human error which is the primary cause of plan failure rather than technology failure: 48.6% responded that lack of accurate staff contact information was the main cause for failing to achieved accepted response levels closely followed by lack of understanding from recipients (47.6%). The same two choices led the table in 2018, although lack of accurate staff contact information fell slightly (2018: 49.2%).

*"It depends on the systems and organization, but sometimes there is a lack or a gap of accuracy of the data that is being fed, especially with large organizations. We have 300,000 employees, so to maintain and have an accurate data feed is really, really hard. But at the same time, it's critical."*

**Security Manager, Professional Services Organization, Switzerland**



**Figure 12. If you failed to achieve your accepted response levels, what caused the failure? Tick as many as applicable**

Failure of manual processes fell to fourth position this year from third place in 2018, with 26.5% of respondents citing it as the cause for failure vs 33.4% in 2018. With a discernible uptick in training and exercising this year, it appears that some organizations are beginning to reap the benefits of this increased attention. Unavailability of mobile networks has replaced failure of manual processes in third place, indicating that this is still a major problem for organizations. Dual sims in telephones and dedicated emergency communications software can help to mitigate against such failures, and some organizations are still resorting to satellite phones to ensure a network drop can be bridged.

Interestingly, problems communicating internationally and language barriers were at the bottom of the list of reasons why expected responses levels were not achieved at 11.5% and 6.5% respectively. Whilst there is a visible move towards managing emergency communications on a central, globalised level, most organizations choose to delegate control of response to country teams as it enables a more effective response. A university employee explained how a communication was far better adhered to in an emergency if it came from a student’s department.

Some organizations have become adept at managing emergency situations by ensuring that individual countries are given the autonomy to manage emergency situations within their own geography, but global support is available if the incident escalates or needs additional support (such as PR support) within their individual country.

*“If the internet is not available for some amazing reason, then it is likely that the telecoms carriers will be having difficulty as well. So, after that, using satellite phones is a possibility. They’re fairly expensive but they don’t rely on local infrastructure. They essentially just connect to a satellite or a galaxy of satellites orbiting the earth. That’s one way of getting around a mobile network outage.”*

**Independent Business Continuity Consultant, United States**

*“We know from our experiences that students respond best to things that are more relevant for them so for us, that means coming from the school faculty that they’re particularly engaged in. For example, if an accounting student in the business faculty gets a communication from the department team, they’re more likely to respond to that than a general corporate message.”*

**Resilience Professional, Education Sector, Australasia**

*“The global operations will always be informed, even if it is a local incident. It is important that we don’t hear from the media first about an incident occurring in one of our territories or we get people asking our global CEO what’s happening in a country and they are unaware. It’s therefore very important that we are all aligned on an incident that happened on a local level, even if it’s being managed at the lowest bronze level. We need to be prepared to provide media statements and support to the local company if needed.*

*In some cases, the incident may have a wider impact and this would be managed on a regional or global level; on what we call a silver or gold level. The global operations routinely deliver training to local companies to ensure they are all aligned on how to use emergency communications systems.”*

**Resilience Professional, Telecommunications, United Kingdom**

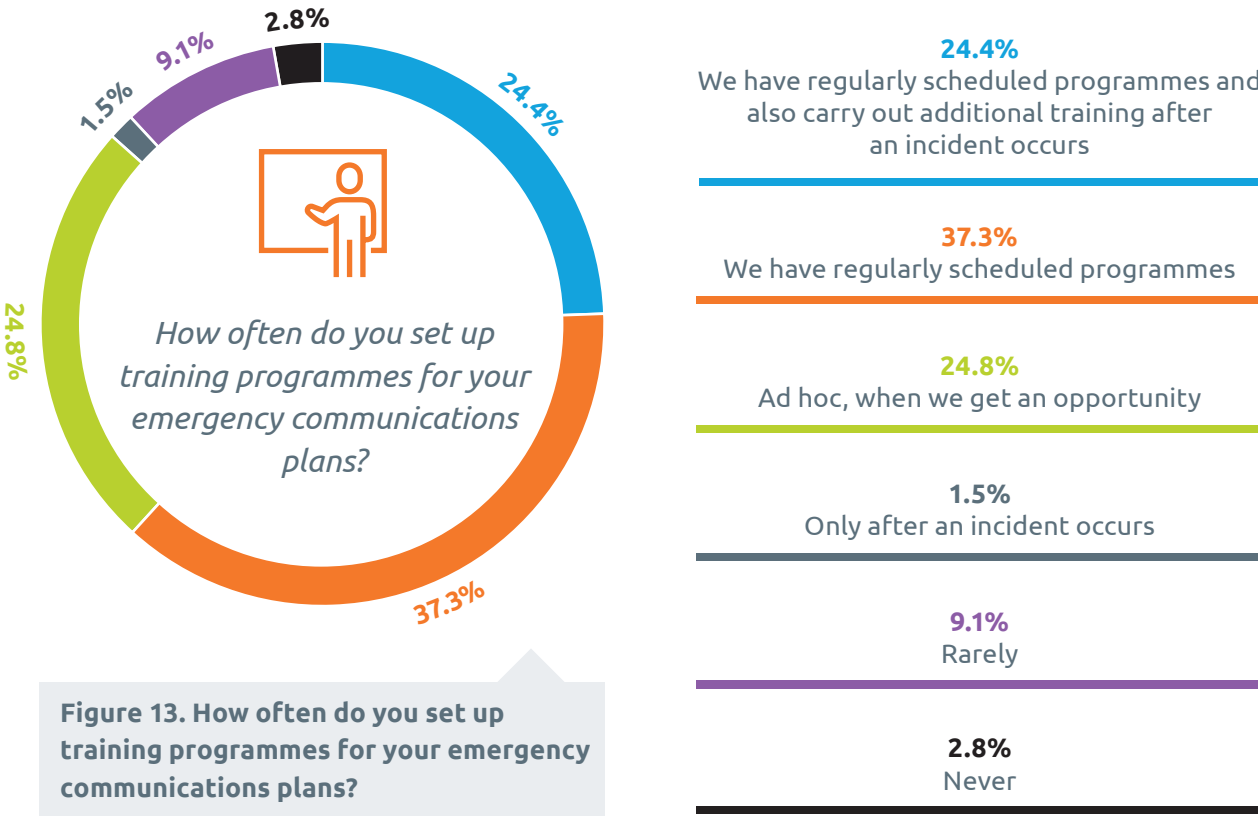




EXERCISING EMERGENCY COMMUNICATIONS PLANS

- The number of organizations who are carrying out regular training and exercising of their emergency communications plans has increased this year: nearly two-thirds have regularly scheduled training programmes.
- Over half (53.2%) are now exercising plans at least once a year and the number of never exercise has dropped by over half to 3.6%.
- The number of organizations who have had to activate their emergency communications plans over the past year has risen marginally to 71.6% (2018: 71.0%) and organizations are increasingly using these real-life activations to improve process and procedure.

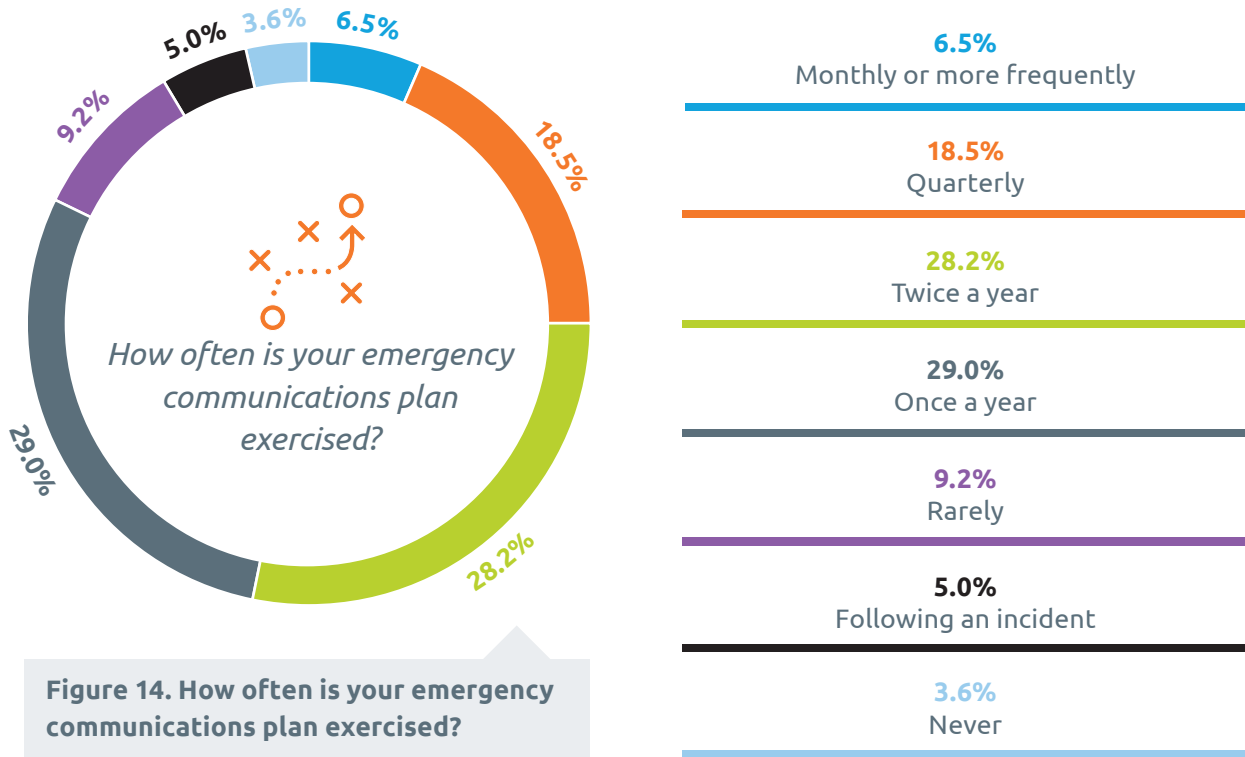
This year, there was an improvement in the effectiveness of emergency communications which can be partly attributed to increased attention to training and exercising. The survey backs this up: 37.3% of respondents claim to have regularly scheduled programmes whereas 24.4% have regularly scheduled programmes and carry out additional training after an incident occurs. This is a positive response: it is advisable to carry out regularly scheduled programmes in addition to carrying out further training after an incident. This helps all those involved to be aware and gain a level of knowledge and confidence to carry out the emergency communications process of the organization. Such post-event training will not only provide a learning tool for staff but can serve the dual purpose of identifying areas for improvements in processes or procedures. There is still room for improvement, however: 24.8% responded that they only set-up training programmes in an ad-hoc manner which, although concerning, still represents a fall from 36.0% in 2018.



The same elevated interest in training is also exemplified when considering the number of times organizations carried out exercises: 38.6% of those surveyed in 2018 carried out exercises more than once a year. This year, the figure was 53.2%. Furthermore, 7.3% of respondents in 2018 claimed to “never” exercise their emergency communications plan and the figure halved this year to 3.6%. Emergency Preparedness guidelines by the UK Government say that emergency communications plans should be carried out a minimum of twice a year as staff contact details change, staff leave, or new staff join<sup>2</sup> and the US Department of Health and Human Services advises similar<sup>3</sup>. Many global associations echo government advice and advise comparable strategies: the International Air Transport Association (IATA), for example, recommends exercising every six months<sup>4</sup>. Some organizations fail to carry out exercising as they have yet to encounter an incident where they need to initiate their emergency communications plan. Therefore, it is not until they must exercise a plan for a real incident and uncover the gaps in it that they realise the importance of it. For other organizations, a lack of trained staff can be the primary issue in ensuring plans are regularly rehearsed and, crucially, the results analysed.

*“It is important to have a sufficient number of employees trained to use the emergency notification system to initiate and send out messages, and then analyze the results after the messages have been sent. I’d also recommend that organizations provide awareness and refresher training on emergency notification systems periodically.”*

**Independent Business Continuity Consultant, United States**



2 Cabinet Office 2011, Chapter 5 (Emergency Planning) Revision to Emergency Preparedness, Cabinet Office, viewed 12 December 2019, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/61028/Emergency\\_Preparedness\\_chapter5\\_amends\\_21112011.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61028/Emergency_Preparedness_chapter5_amends_21112011.pdf)

3 Office of the Assistant Secretary for Preparedness and Response 2017, 2017-2022 Hospital Preparedness Program; Performance Measures Implementation Guidance, Assistant Secretary for Preparedness and Response, viewed 12 December 2019, <https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/hpp-pmi-guidance-2017.pdf>

4 IATA 2018, Guidance Document. Crisis Communication and Reputation Management in the Digital Age: A Guide to Best Practice for the Aviation Industry, IATA, viewed 12 December 2019, <https://www.iata.org/publications/Documents/social-media-crisis-communications-guidelines.pdf>

“Personally, I would exercise the plan at least quarterly or even as much as six times a year just to make sure that people know what they’re supposed to do and how they should perform in an emergency.”

Independent Business Continuity Consultant,  
United States

“All staff are getting test messages quarterly that they have to acknowledge and respond to. If you don’t get a high enough response rate in your organization, you have got to repeat it until you do. So we’ll build that into our programme.”

IT Director, Insurance Organization, United States

“Every post-incident review highlights issues [with our plan] at varying degrees. We have a new director who is bringing some energy to this and, is getting buy-in from other executives. We’re rethinking what our incident team structure should look like. Part of that rethink was that while we technically have that power to delegate authority to make communications, we’re going to do two things to make improvements: we’re going to get a whole set of pre-approved communications and flesh out the plan through exercising and through discussion with senior leadership.”

Resilience Professional, Education Sector,  
Australasia

71.6% of organizations had to initiate their emergency communications plan outside of an exercise scenario at least once in 2019. This was a marginal increase on the 71.0% reported in 2018. The number that had to initiate their plan more than ten times over the course of the year increased more notably from 4.6% in 2018 to 7.1% in 2019. The increased volume of incidents may also be a reason why organizations are able to reach their targeted response rates more effectively: more incidents means more opportunities for plans to be rehearsed, problems with plans identified and steps made to improve the process for the next occurrence. The interviews conducted for this report uncovered multiple incidences of organizations actively learning from incidents to improve their processes for future emergencies:

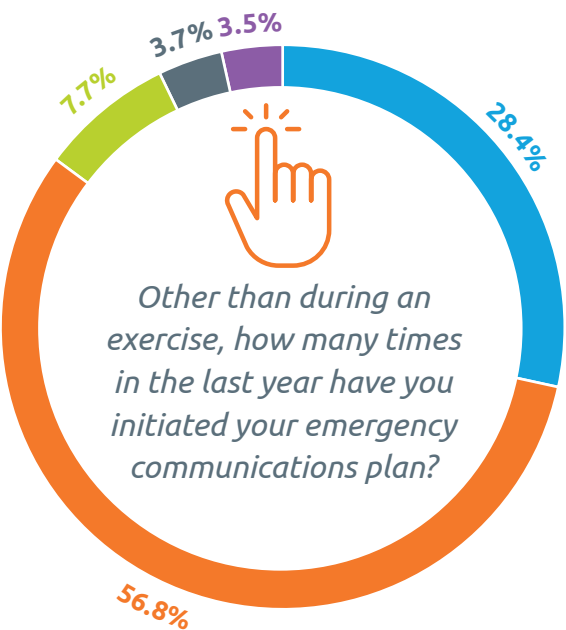


Figure 15. Other than during an exercise, how many times in the last year have you initiated your emergency communications plan?

INTERNATIONAL TRAVEL

- Organizations have more staff travelling to high risk destinations than ever before, with nearly half (46.9%) reporting employee travel to such destinations.
- Localization of an emergency communications strategy helps to action an effective response within a specific destination, with many organizations using tools such as geofencing or dual-sim cards within phones to ensure an effective response.
- Despite increased international travel, preparations for staff travelling abroad is surprisingly low: only just over a third (39.7%) have a comprehensive travel risk management plan in place and under half (48.2%) ensure reliable contact information is collected for staff travelling abroad.

The number of respondents who work for an organization which only operates within a single country has remained on a par with 2018 (2019: 42.8%; 2018: 43.0%). The more global an organization, the more complex the emergency communications plan. Furthermore, many organizations that only operate within a single domestic market still have staff who travel internationally so emergency communications plans should include plans for travelling staff in order to be effective.

Qualitative research undertaken for this report reveals that many global organizations centrally manage emergency communications plans but have localised response teams who are better placed to deal with the scenarios occurring within their local territories. Other organizations have a global team which looks after travelling staff, whilst domestic teams are responsible for staff within their own location.

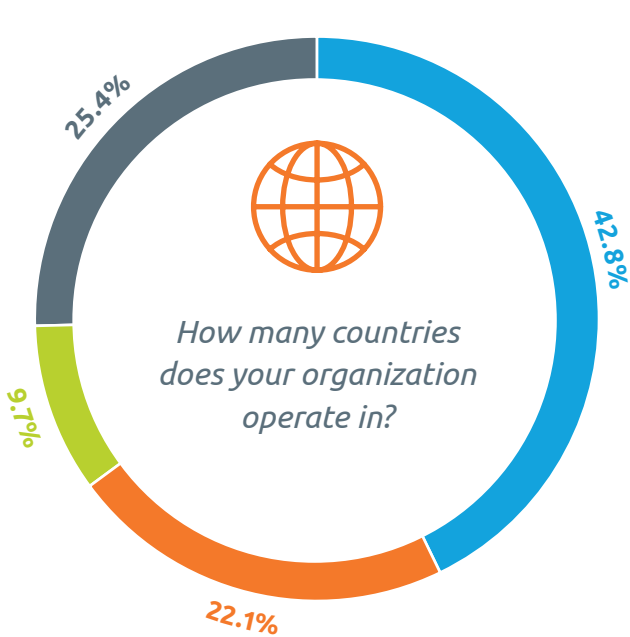


Figure 16. How many countries does your organization operate in?



There is a marked increase this year in the number of organizations who consider staff travel to areas of high risk: just under half (46.9%) reported that staff travelled to high risk areas, compared to just over a third (36.0%) in 2018. Whilst it is unlikely that the countries staff are visiting has dramatically changed over the course of a year, organizations may have an elevated perception of risk this year due to high profile incidents occurring: the crisis in Venezuela, for example, has escalated in the second half of 2019, whilst the Hong Kong protests are impacting business travellers in the region. Lone shooter incidents in North America and isolated terrorist incidents throughout Europe are all adding to traveller anxiety.

*"We will do a little bit more for our employees than others when it comes to incidents which are happening outside of work. Many companies would view someone on leave as "they're on vacation, they're fine" but we respect everybody and we would like to be able to at least reduce the possibility of the number of staff who are being affected because of an incident at the Eiffel Tower, for example."*

**Security Manager, Professional Services Organization, Switzerland**

Although the probability of a single member of staff being affected by an incident whilst travelling is low, for global organizations with upwards of 100,000 staff, the chances of some staff being affected by an incident is high. Some organizations go a step further and seek to help employees even when they are on leave and not on work business:

Many organizations are realising the benefits of tools within their emergency communications applications to help locate staff abroad: geofencing, for example (as discussed under Tools and Solutions), can be an invaluable tool for contacting travelling staff.



**Figure 17. Does your organization consider some or all of the countries your staff travel to as high risk?**

Despite many organizations exhibiting exemplary procedures for contacting staff abroad by ensuring contact details are up to date when staff are travelling abroad, ensuring travel risk plans are in place and using tools such as geofencing, the number of organizations who do not ensure plans are in place for remote staff is surprisingly low. Worryingly, under half of respondents (48.2%) said their organization seeks reliable contact information for employees when they are abroad. This suggests many organizations are relying on being able to contact staff through standard means of communication (such as by email or by mobile phone) and are perhaps not considering difficulties such as poor or no mobile signal or network outages. Perhaps of even more concern is that less than half of organizations (43.9%) said that their organization believes travellers and remote-based employees need to fulfil their duty of care obligations. This is a significantly lower percentage than in 2018 when 57.7% of respondents answered positively to this question.

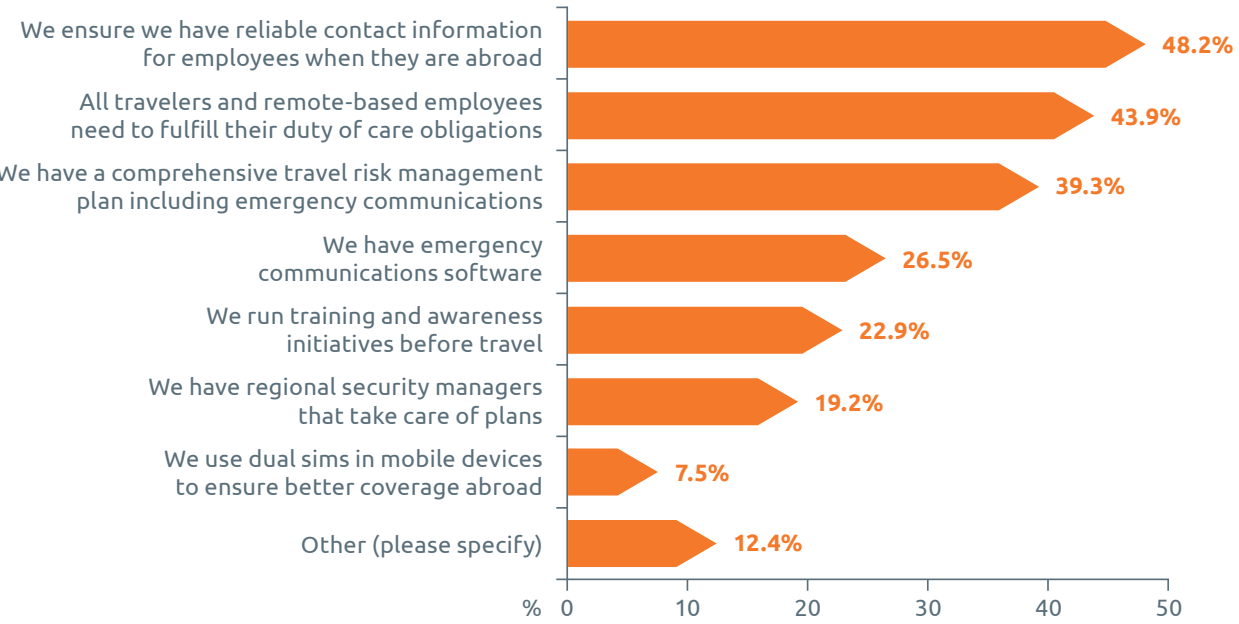
The number of organizations who have a comprehensive travel risk management plan in place has also fallen to 39.3% in 2019, down from 42.5% in 2018. Larger organizations tend to be better placed than small organizations in terms of having comprehensive travel risk management plans in place: nearly two-thirds (60.0%) of respondents from organizations employing over 100,000 said their organization had a travel risk management plan in place.

The benefits of training and exercising to ensure effective delivery of emergency communications plans have already been discussed, but when it comes to sending staff abroad for work, only 22.9% of organizations run training and awareness initiatives for employees travelling abroad (2018: 27.2%). Training and awareness programmes can help staff to be prepared for incidents as they occur abroad and provide an opportunity for staff to ask questions about potential technology issues. However encouragingly, a significant minority (7.5%) use dual sims in mobile devices to ensure better coverage abroad showing a proactive approach to solving the issue of poor mobile coverage abroad, and nearly one in five (19.2%) have regional security managers who are charged to take responsibility for the safety of travelling staff.

*"Even with our own organization, we see that some countries, some parts of the world, will do a little bit more for their employees than others, especially when it comes to things that are happening when individuals are off work. Nowadays it is challenging ensuring staff safety as people do not like to be tracked, especially European communities due to the Big Brother concept. An article in the US said they have actually given up, 9/11 being one of the triggers, and not wanting to give up their basic amendments; the right to life and the right to privacy."*

**Security Manager, Professional Services Organization, Switzerland**





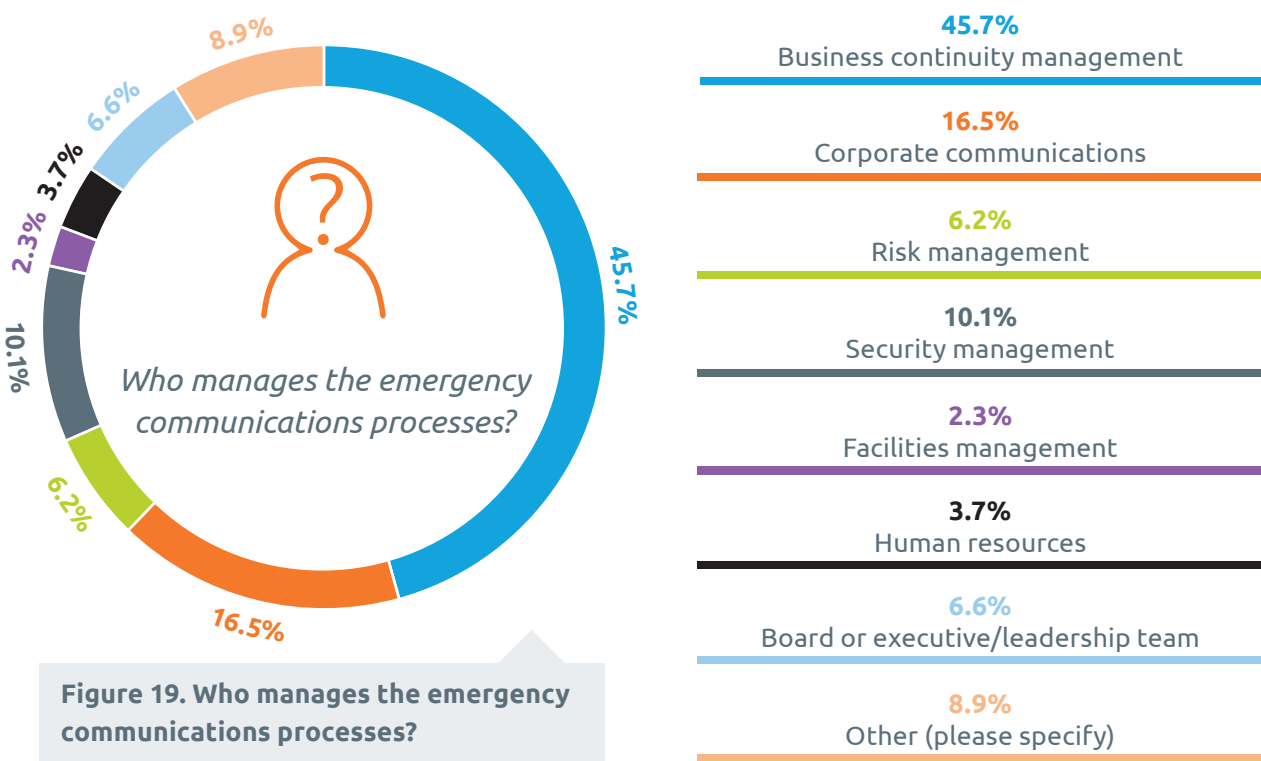
**Figure 18.** How does your organization ensure the implementation of effective emergency communications plans for travelling or remote-based staff? (please tick all those that apply).

COLLABORATIVE APPROACH

- Nearly half (45.7%) of organizations report that the business continuity department is responsible for managing the emergency communications process, but the most effective plans require close collaboration between departments.
- The importance of the external communications/PR department is crucial to the effectiveness of an emergency communications plan, particularly for larger organizations who could see significant customer or share price impact if incorrect or false news is spread.

Nearly half (45.7%) of organizations reported that the business continuity department is responsible for managing the emergency communications process. For 16.5% of organizations, responsibility lies within the corporate communications team, for 10.1% it is within security management and a significant minority of 6.6% said that responsibility lies within the board or executive team. Whilst it would be expected that responsibility for emergency communications would be managed by one team, it is important that the team works closely with other functions in order for plans to be effective: HR, for example, might take responsibility for keeping staff records up-to-date, the IT department could be responsible for ensuring that emergency communications software and hardware is installed and maintained to a high level, and security staff could be responsible for physical assistance during an emergency.

Furthermore, many departments may need to interact in order to give advice to staff on how to react in an emergency. For example, some staff may not appreciate the importance of responding to an email or text alert to report they are accounted for during an emergency whereas others may assume their mobile phone will function as normal when they are travelling to a developing country. Organizations that rely on WhatsApp for communications, for example, might need additional assistance from IT on how to overcome communication barriers when travelling to countries where its use is banned, such as in China or the UAE.



**Figure 19.** Who manages the emergency communications processes?





*"With an ineffective communication process, or a team that does not effectively understand or manage incident communications to their target audience, the entire continuity or recovery process can be hindered"*

**Resilience Professional, Education Sector, Australasia**

communications/PR was the third most popular response after security and human resources. Given nearly a third (32.0%) of respondents saw co-ordinating the external message as a key challenge during a crisis, the importance of working closely with the external communications or PR department will be crucial for many organizations.

In addition to managing the internal communications process, many organizations consider the importance of external communications as core to an effective emergency communication programme. When respondents were asked which other departments took a key role in emergency communications processes, external

TRIGGERS FOR ACTIVATING EMERGENCY COMMUNICATIONS PLANS

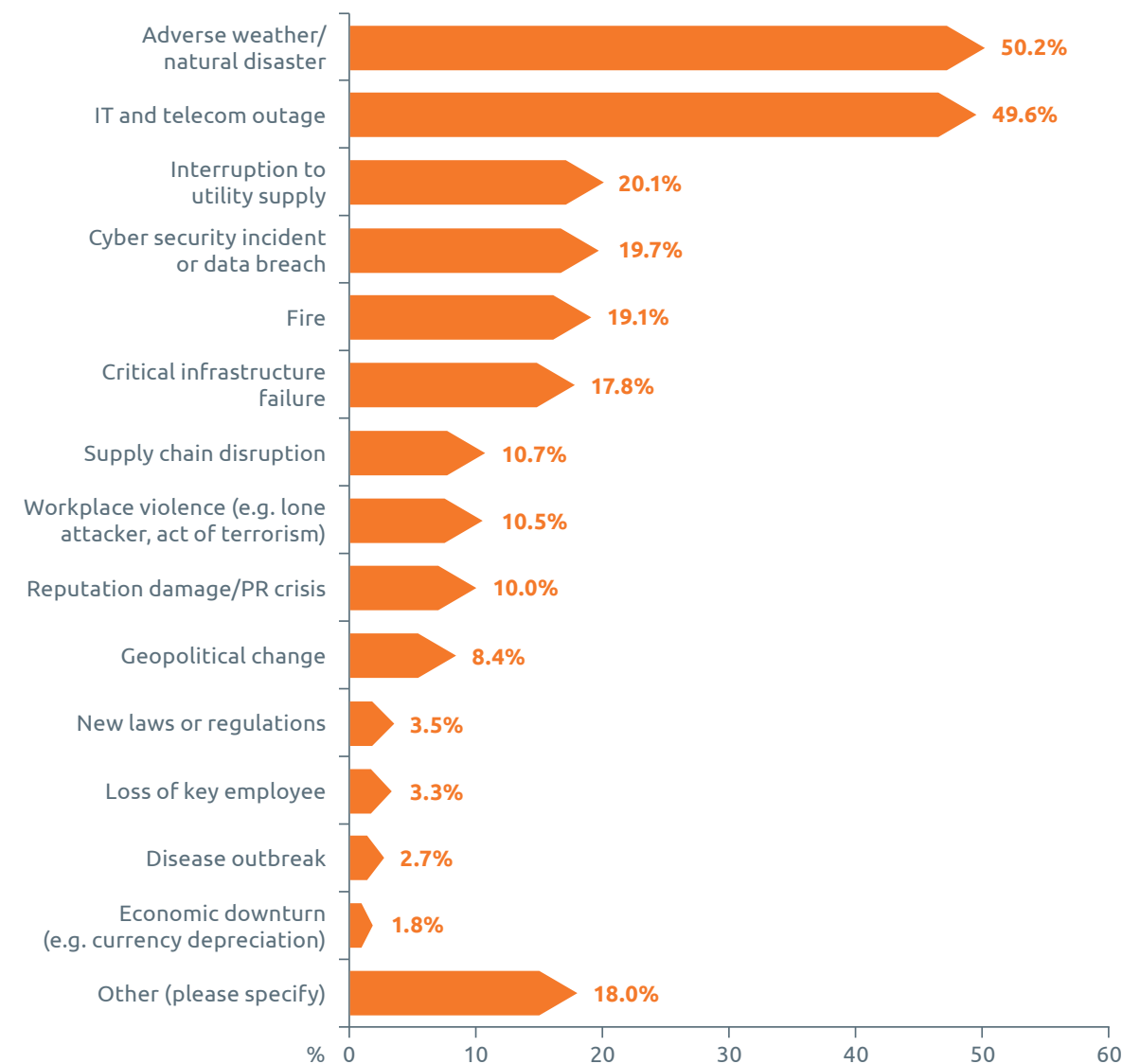
- **Adverse weather/natural disaster and IT/telecoms outage are the most frequent reasons for emergency communications plans being activated in the past year.**
- **With email a favoured method of communication in a crisis but IT/telecoms outages and cyber-attacks the frequent cause for triggering an emergency communications plan, other forms of communication should be considered in the case of a system outage.**
- **Terror attacks/lone attacker incidents account for one in ten incidences of emergency communications plans being activated demonstrating the importance of having a plan in place even for incidents which are perceived as being unlikely to happen.**

Adverse weather/natural disaster and IT/telecom outage were the most frequent reasons for emergency communication plans being activated in 2019 at 50.2% and 49.6% respectively. Last year, adverse weather/natural disaster topped the list for triggering emergency communications plans, with 61.8% of incidences being attributed this. This mirrors findings in the 2019 BCI *Horizon Scan* report where organizations reported a drop in the number of incidences caused by adverse weather or natural disasters.

With IT/telecom outage being the cause of nearly half of all emergency communication plan triggers and cyber security incident/data breach accounting for a fifth (19.7%) of triggers, it is vital that a plan can be activated even if employees have lost IT or telecoms connectivity. Furthermore, this year’s survey revealed that 72.2% of organizations would notify staff about a cyber security incident or data breach by email. In the event of a system being hacked, would this method of communication be reliable?

Interruption to utility supply, fire and critical infrastructure failure accounted for around a fifth of triggers, whilst supply chain disruption and workplace violence (e.g. lone attacker, act of terrorism) accounted for over one in ten triggers. This demonstrates that incidences which many may consider to be unlikely still need to be considered as part of an emergency communications plan.





**Figure 20. Which of the following triggered your emergency communications plan in the past twelve months? Tick all those applicable.**

## RELIABILITY OF INFORMATION

- **Under two-thirds of organizations (61.7%) seek to ensure that employees' contact information is kept up to date. Given over half of organizations (54.2%) cite communicating with staff as a key challenge during an emergency, this is cause for concern.**
- **Collaboration is key in a crisis, yet only half of organizations collaborate with emergency services or government agencies during an emergency to ensure accurate information is received, and just over a third exchange information with other organizations in the local area.**
- **Despite many organizations still failing to update contact information regularly, other organizations are improving their processes by using technology: automatic interfaces with HR systems are now being used by nearly half of organizations, and a further fifth run automated requests to update contact information.**

Ensuring reliability of information is crucial to the success of an emergency communications plan: failing to use reliable information sources during an emergency can at best lead to confusion amongst staff due to mixed messaging or, at worst, result in loss of life.

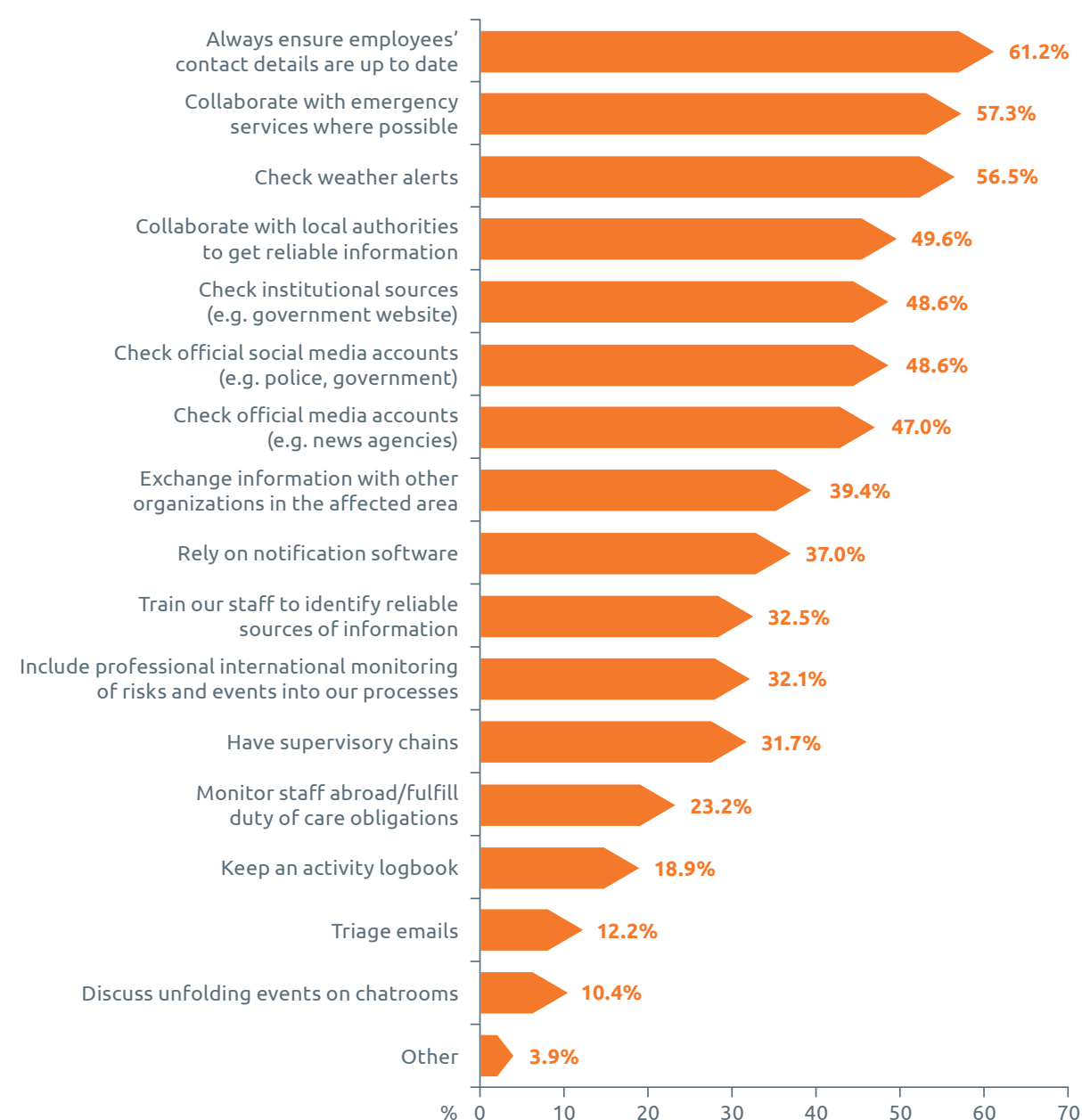
There are several ways organizations can ensure that information sources are reliable. The most highly rated choice by respondents was ensuring employees' contact details are up to date with 61.7% claiming to do this. However, given such information is crucial during an emergency scenario, the fact that more than a third of organizations are failing to do this is a cause for concern and goes some way to explaining why over half (54.2%) of respondents saw communicating with staff as one of their key challenges during an emergency.

Collaboration with external parties during an emergency can be a way of ensuring an accurate source of information and can also enable an organization to work with other businesses in the local area to ensure a cohesive response in an emergency. However, the number of organizations who do seek to collaborate is still fairly low: just over half (57.3%) collaborate with emergency services where possible in order to ensure the acquisition of accurate information relating to an emergency or crisis, under half (49.6%) collaborate with local authorities or government agencies and only 39.4% exchange information with other organizations in the local area.

Given severe weather remains one of the most frequent causes for activating an emergency communications plan, the checking of weather alerts is an inexpensive method of being prepared. 56.5% of organizations check weather alerts either via websites, downloaded apps or, for some organizations, direct feeds from government and/or private weather forecasters. Hyper-local forecasting (e.g. DarkSky) is also now becoming more accurate and can provide organizations with richer information about how a weather event will directly affect business locations.

Checking official media accounts is carried out by 47.0% of organizations, a low percentage given the rich information that can be obtained from official news sources and institutional and government resources. 37.0% of organizations rely on notification software to inform them of updates during an emergency. Whilst this is a more time efficient way of scanning for information, it can also lead to information being missed if alerts a) do not contain enough information sources; b) are not updated regularly or c) provide too much information meaning important alerts are lost.





**Figure 21. How do you ensure the acquisition of relevant sources of information in the context of managing an emergency case/crisis scenario? Please tick all that apply.**

As already discussed, it is crucial that contact data of staff (both permanent, contract and temporary) is kept up to date to ensure a timely response and recovery from both domestic and international incidents. Whilst only 44.0% of organizations are communicating with HR in order to get the data, a significant proportion are now automating processes which ensures data is regularly updated: 43.0% have a system which regularly interfaces with HR systems for automatic updates and 20.4% of organizations send out regular automated requests to update contact information via emergency notification systems. However, although this is a reliable way of updating information, it does rely on HR systems, data being correct for the former, and contact information being correct on the emergency notification system which sends out the updates for the latter. Many organizations hold accurate information for permanent staff, but contract and temporary staff information can cause issues.

42.6% of respondents still use manual lists which are kept in a database or spreadsheet such as Excel. Whilst Excel is a tool which is readily used across all functions and updates can be easily made, there are issues with version control and lists should be regularly reviewed to ensure the data is the same as is held on the HR system. Relying on data being stored on Excel also can be an issue during a system outage and it is vital a back-up document, updated as regularly as the master document, is safely stored somewhere where it can be accessed in such an outage but also adheres to GDPR and data protection guidelines. Nearly a quarter of organizations (24.2%) run regular test alarms to ensure messaging is received by all staff and then perform corrective actions afterwards if data is found to be missing.

*"The big challenge is the manual upkeep of [staff contact information]. We continually have to remind the contractors that they're required to give us a contact number for emergencies. We have to do a lot of chasing."*

**IT Director, Insurance Organization, United States**



*"Back up resources such as a generator should be available in the event of a power outage. There should also be a call tree activated to notify internal and external stakeholders if access to online documents or telecoms are unavailable to notify internal and external stakeholders. This should be well practiced to a level that staff can implement and carry out the necessary plan. It is important that the process is embedded into the organization's culture: senior management should be seeing the systems on a regular basis and staff receiving a text message, probably every quarter, that they have to respond to."*

**IT Director, Insurance Organization, United States**



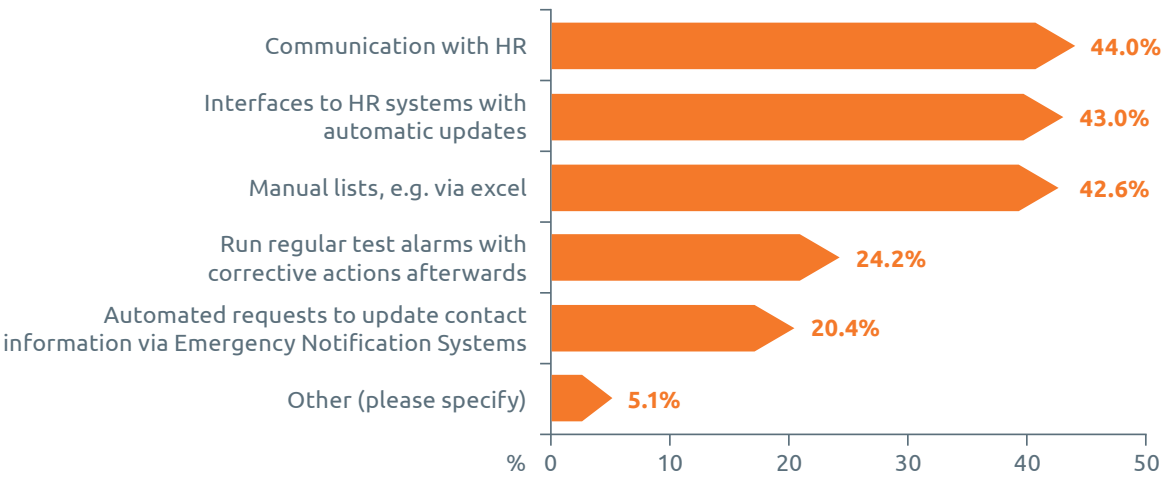


Figure 22. How do you ensure contact data of employees, experts, etc. is up to date?

INTERNET OF THINGS (IOT) AND EMERGENCY COMMUNICATIONS

- IoT devices are currently being used by less than a quarter of organizations, with over a half not having any plans to implement them.
- Devices have a wide variety of uses within an emergency communications setting: they can provide early warning of emergencies (such as fire) to emergency services, automatically cut off utility supplies or automatically update public display boards with evacuation information.

The BCI *Disruptive Technologies Report 2019* and the BCI *Supply Chain Resilience Report 2019* both pointed to an uptick in the number of organizations who are using IoT within their organization and throughout the supply chain to help improve processes and ultimately increase the resilience of an organization. Despite the benefits that IoT technology can bring to an organization (such as providing advanced warning of danger to emergency services, automatically cutting off power or utility supplies or providing automated alerts to display on public address systems), uptake specifically for emergency communications purposes has been less marked. 56.3% of organizations either have no plans to embed IoT devices into their emergency communications plan or do not see how they could improve their plan, a lower figure than in 2018 (59.4%) but still shows just how few organizations will be benefitting from the technology.

10.9% of organizations report that IoT devices are now well embedded into their plans, 12.8% say they are used in limited areas and a further 14.6% claim to be planning to use IoT devices. The lack of uptake is attributable to several reasons: a lack of understanding of the benefits IoT can bring to an organization, concerns about system failures causing disruptions and outages, worries about the cyber-security of devices and budgetary reasons. However, despite the barriers to uptake, the number of organizations who are employing IoT technology or plan to do so has risen by 5% this year to 38.3% (2018: 33.0%).

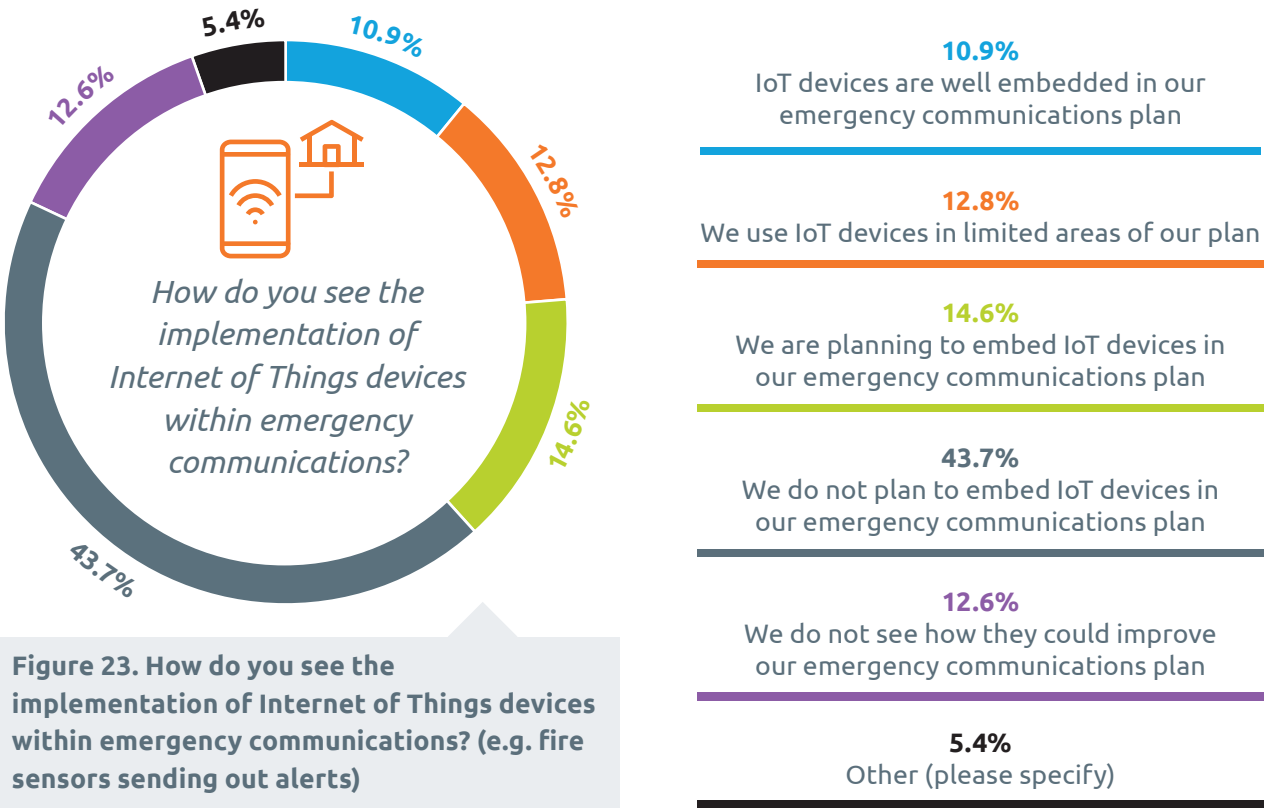


Figure 23. How do you see the implementation of Internet of Things devices within emergency communications? (e.g. fire sensors sending out alerts)



# COMMUNICATION OF INFORMATION IN DIFFERENT SCENARIOS

- **Communicating information relating to an emergency requires different communication tools for internal and external communications.**
- **Email remains the preferred method of communication for all scenarios, whether internal or external. However, an alternative means of information should be considered for some scenarios in case of an email or system outage.**
- **When communicating more sensitive information, SMS or text message is often not appropriate as more information needs to be given to employees (e.g. counselling services or succession plan information).**

The methods of informing external stakeholders following an incident is very different from the processes used to inform staff of an incident. In an era where news spreads fast, the way an issue is communicated to external stakeholders is hugely important to many organizations, particularly for incidents where customers will be directly affected which could lead to lost customers, falling revenues and, for listed organizations, a fall in share price. Legal issues could also arise if contracts state that a stakeholder needs to be informed of an incident.

Email remains the preferred means of contact for all incidents, although there are minor differences in the way different incidences are treated. News of a cyber-attack, for example, which has the potential to create significant damage to customer confidence is communicated through formal channels: 45.0% of organizations would announce the incident on their website, with a public announcement (i.e. press release) the third rated option at 40.0%. Social media would only be used by 26.8% of respondents. The loss of a key employee uses similar channels of communication for external stakeholders.

For adverse weather or a natural disaster, organizations are much more comfortable with using social media as an external communications tool. After email, it is the second most used tool for this kind of scenario at 53.3%. Such incidents do not have the same negative PR consequences of a cyber-attack or phishing incident, and social media can help to inform multiple stakeholders very quickly.

Cyber security incident or data breach

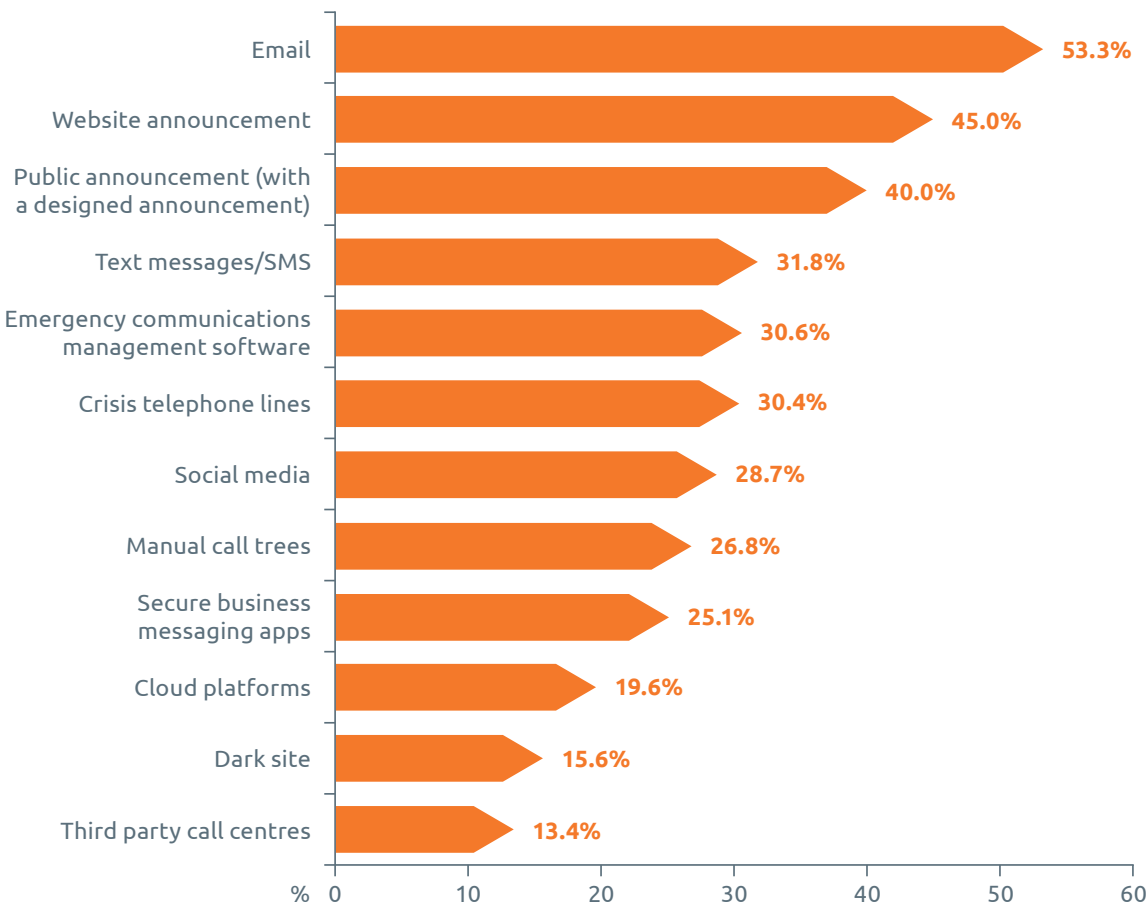
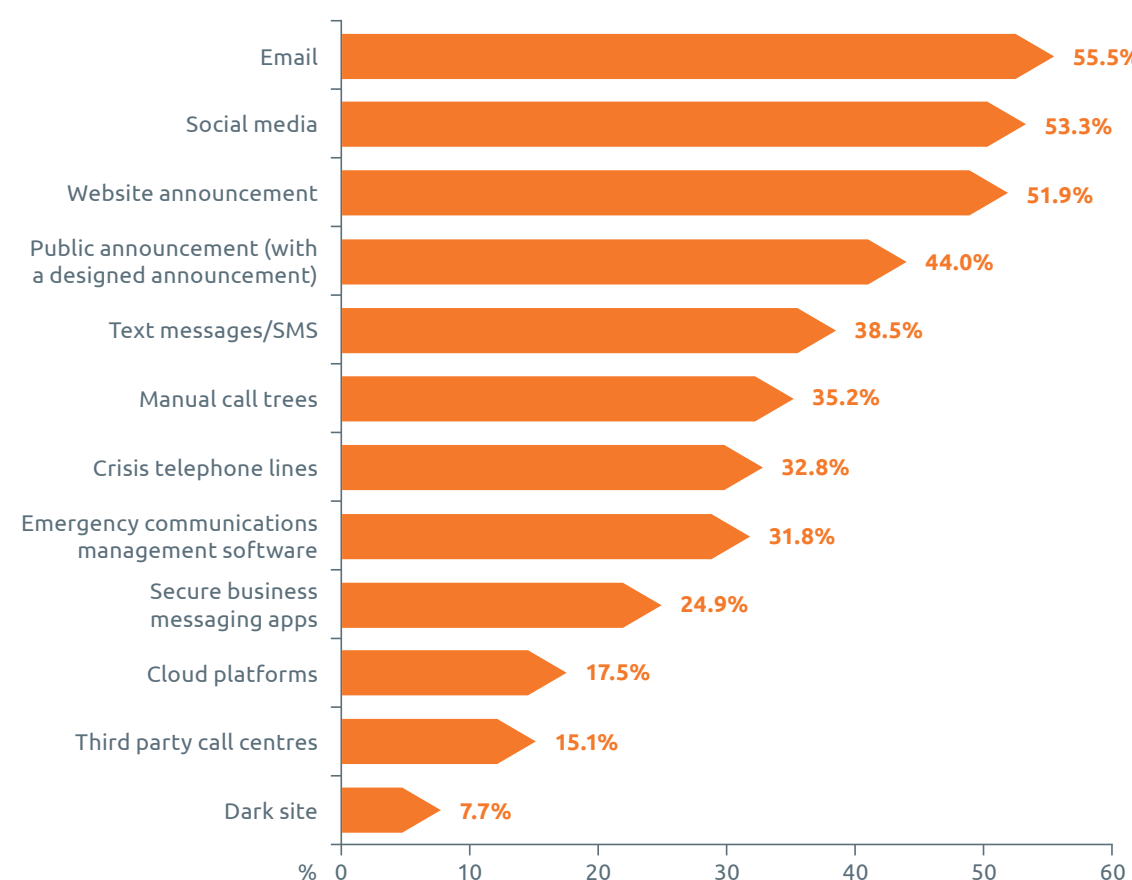


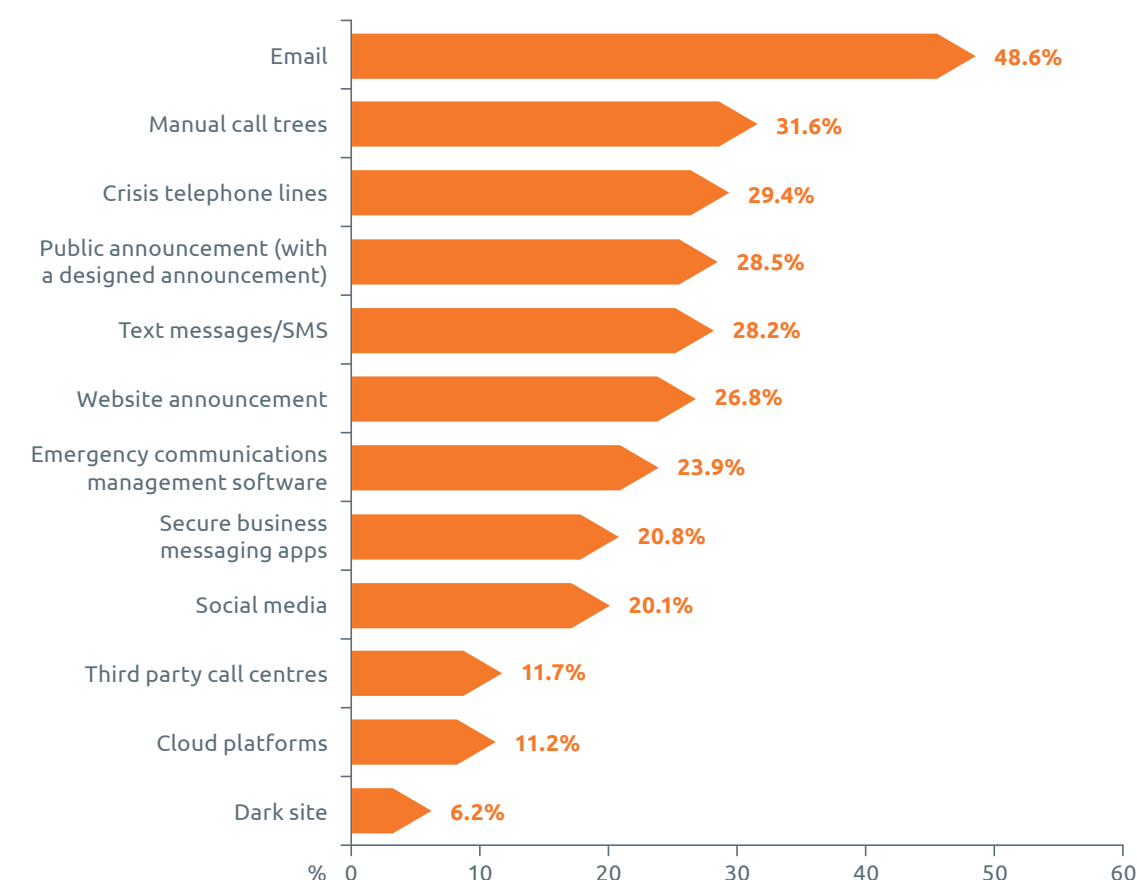
Figure 24. Which processes would you use to communicate to external stakeholders (e.g. customers, media) during each of the following scenarios?



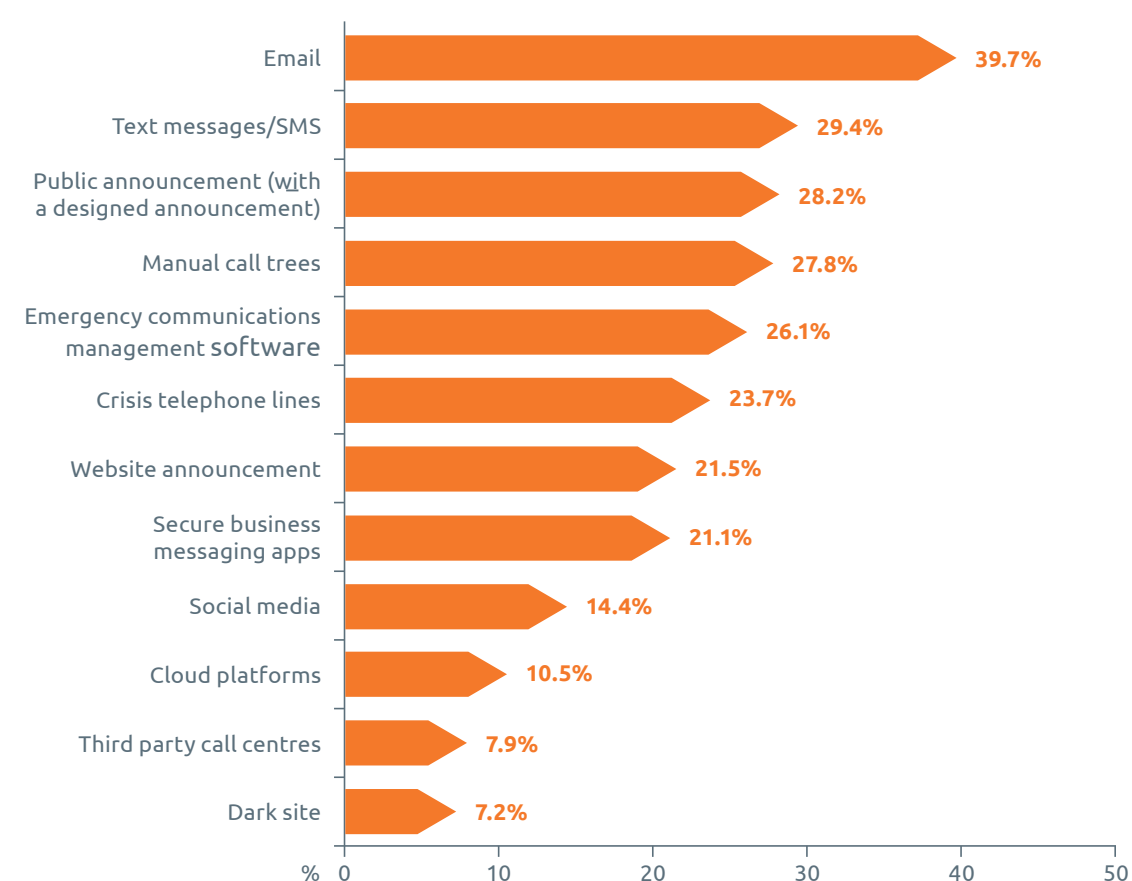
### Adverse weather/natural disaster



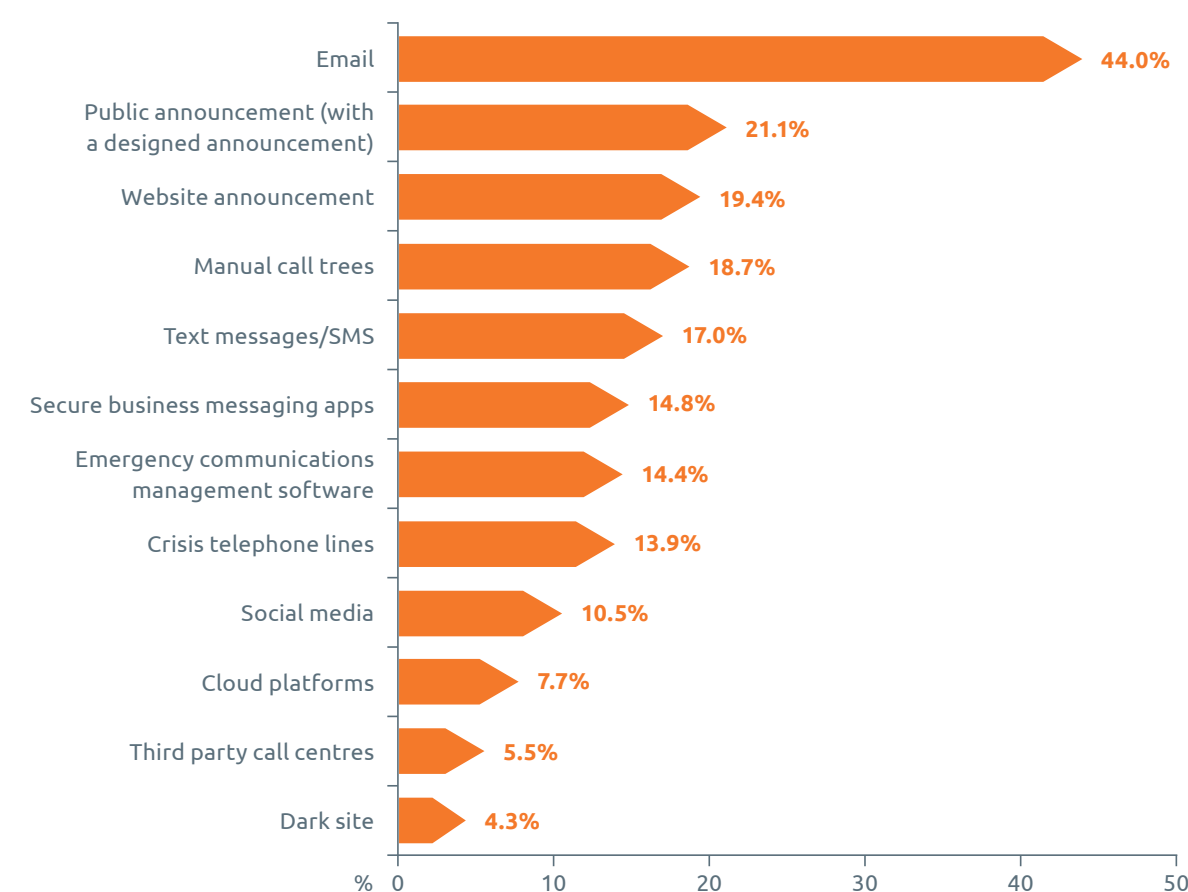
### Health and safety incident



### Workplace violence (e.g. lone attacker)



### Loss of key employee





For internal communications, email is once again the top-rated method of communication for all incidents. Indeed, it appears to be the default tool to use in an emergency scenario. However, it should be questioned whether it is the right tool in some circumstances: 72.2% of respondents claimed they would use internal email to communicate about a cyber security incident or data breach. If the incident had caused a system outage, the email system may not be functional, and an alternative means of communication should be used.

For a lone attacker or workplace violence related issue, two-thirds of respondents (64.9%) selected email as their preferred method of communication. In such an incident, particularly where there is a threat to life, communication via multiple means should be considered in the first instance. Emergency communications software can help to reach users on multiple platforms, yet only just over a third (37.1%) would use it in this scenario.

*“When somebody senior passed away recently, the CEO did not use the mass communication tool as he thought it wasn’t appropriate, and he used something else. He recorded a message and sent it to all the employees.”*

**Security Manager, Professional Services Organization, Switzerland**

When an organization is communicating the loss of a key employee, less impersonal methods of communication are used. The use of manual call trees is the second highest rated option for transmission of information in this scenario, with just under a quarter (23.9%) electing to use this method. Such sensitive information is better communicated without

the boundaries of character limitations in a text message, particularly when information such as support lines must be communicated.

Cyber security incident or data breach

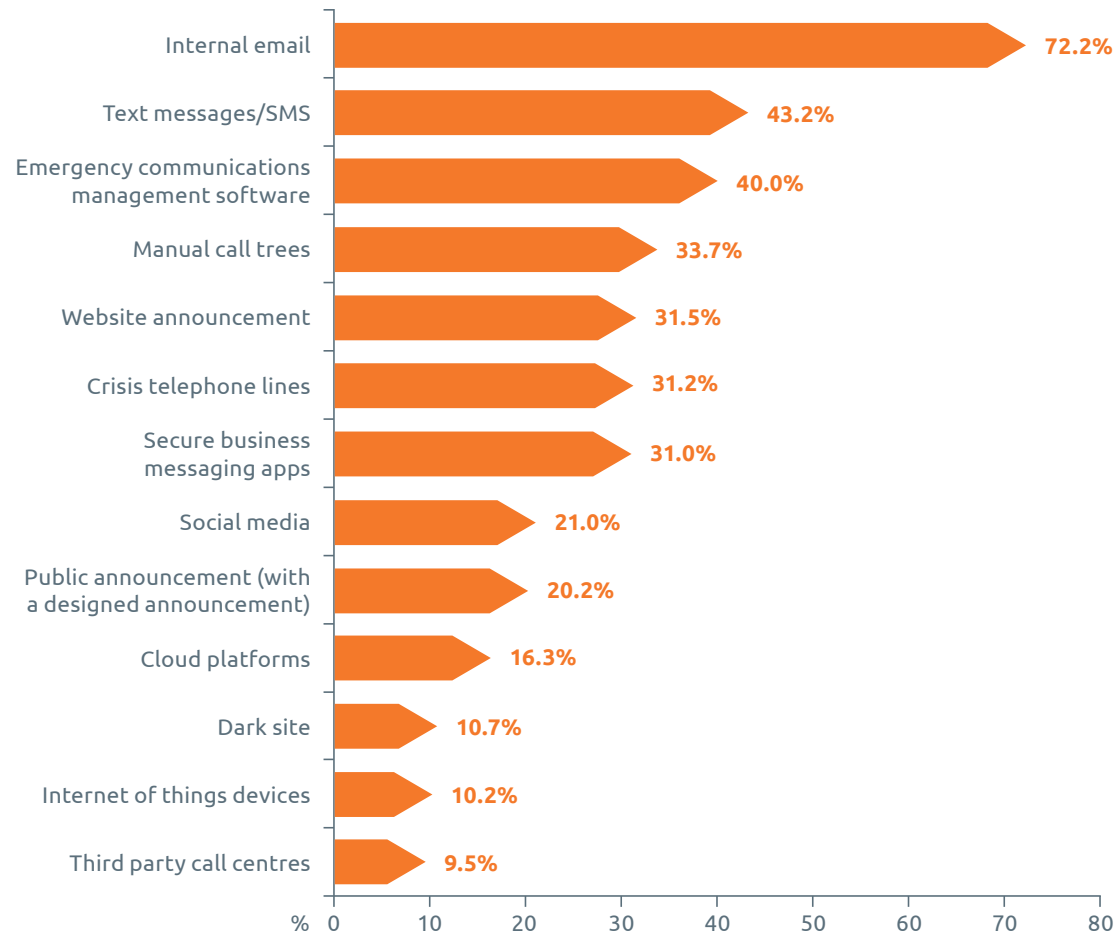
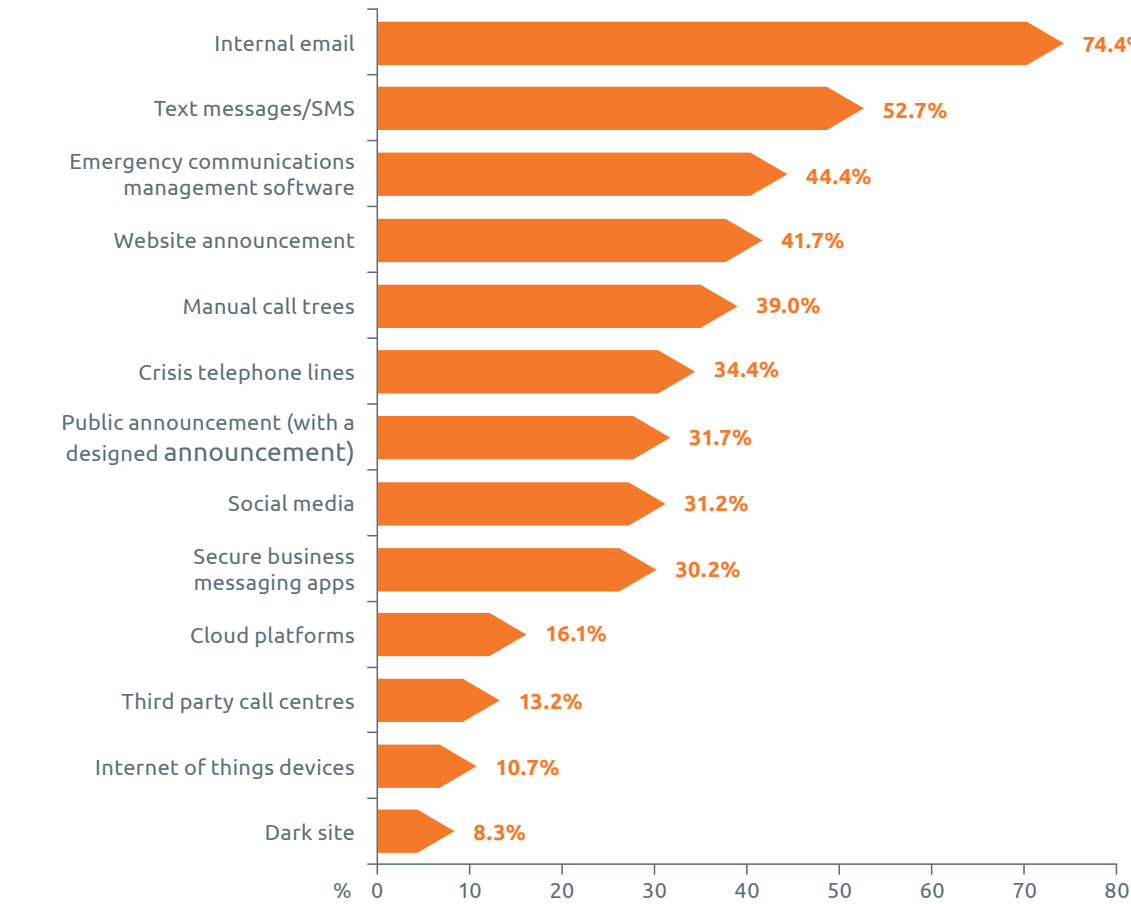


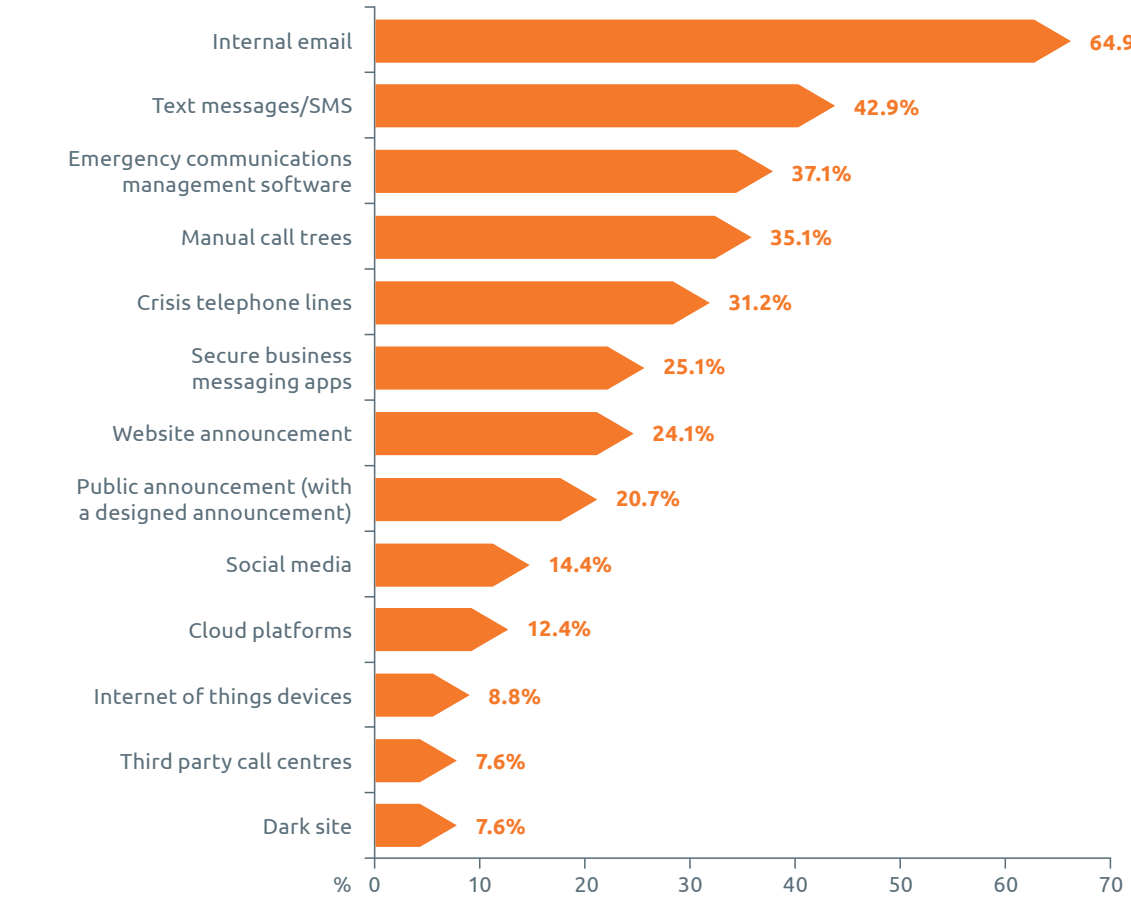
Figure 25. Which processes would you use to communicate to internal stakeholders (e.g. employees, contractors) during each of the following scenarios?



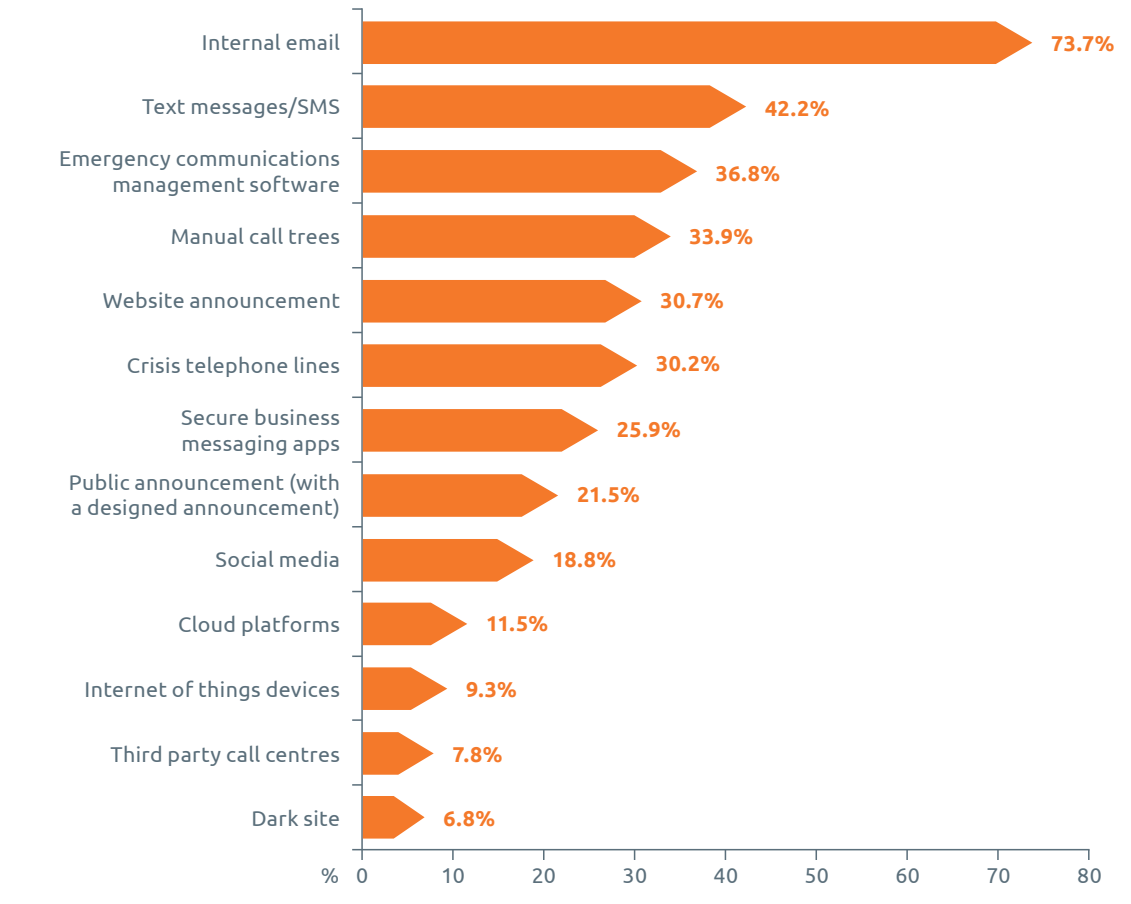
Adverse weather/natural disaster



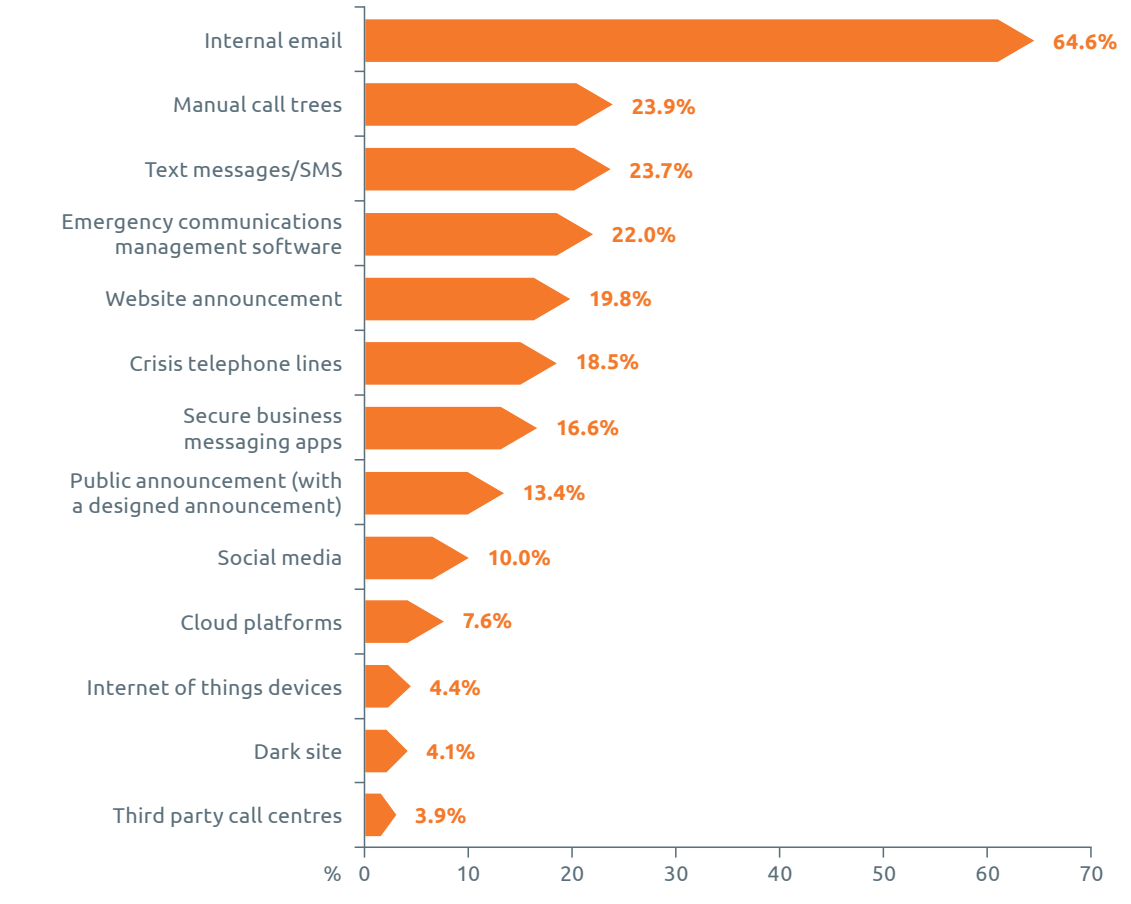
Workplace violence (e.g. lone attacker)



Health and safety incident



Loss of key employee





# 3 Annex



Annex

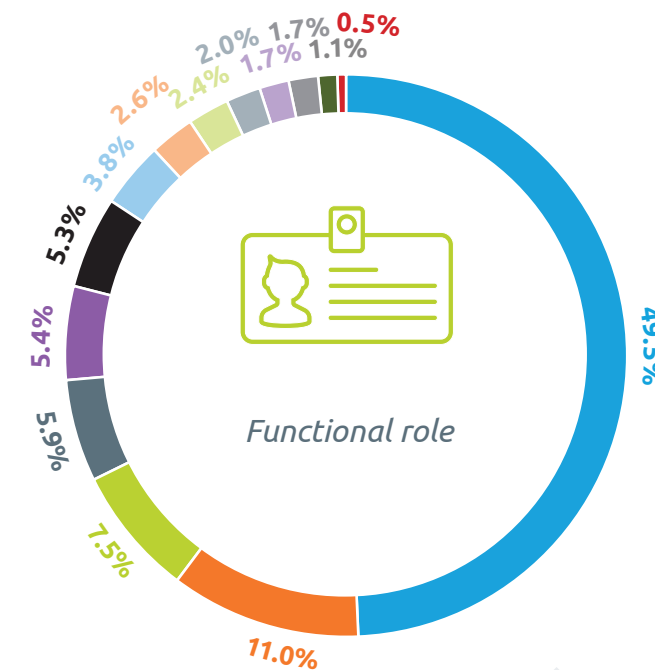


Figure 26. Which of the following best describes your functional role?

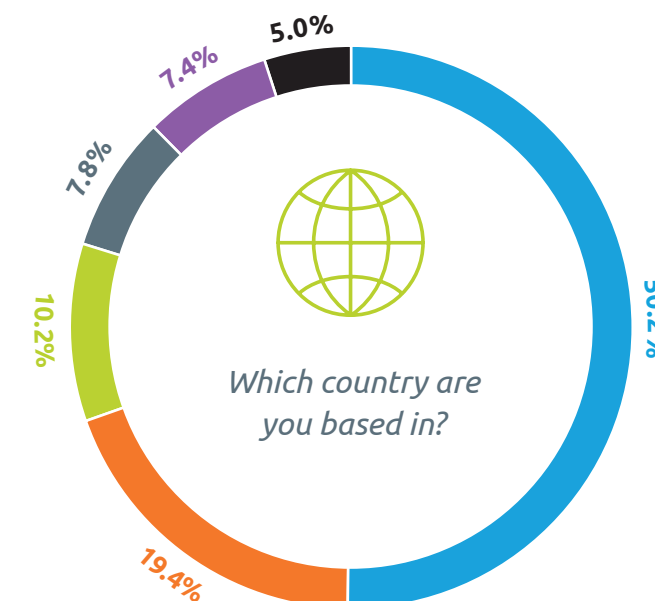
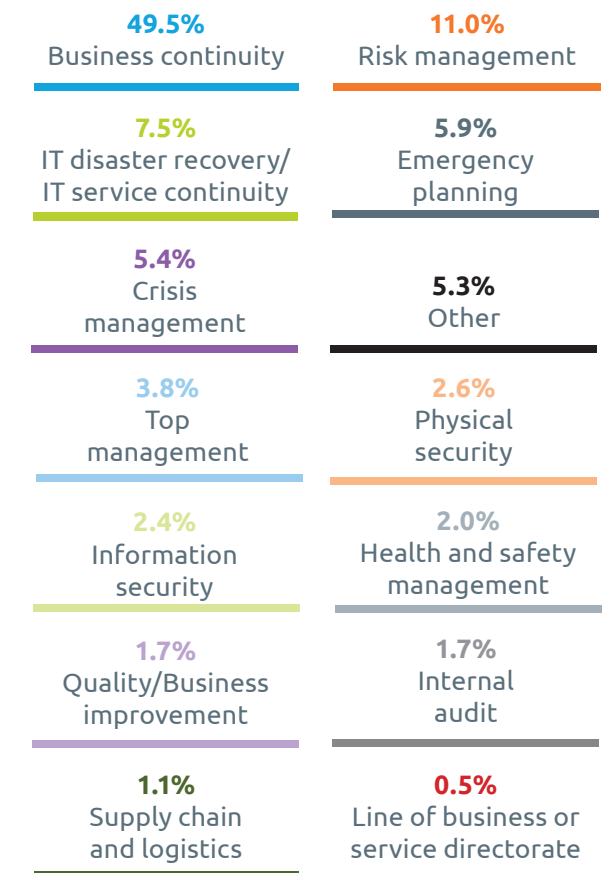
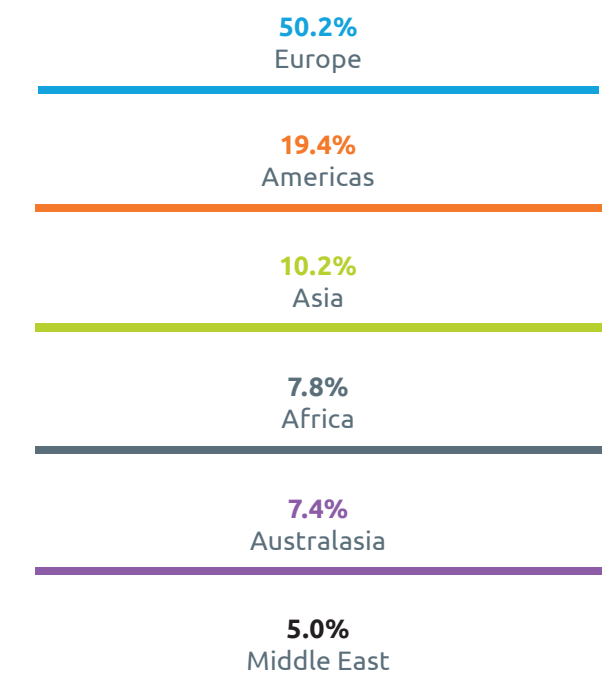


Figure 27. Which country are you based in?



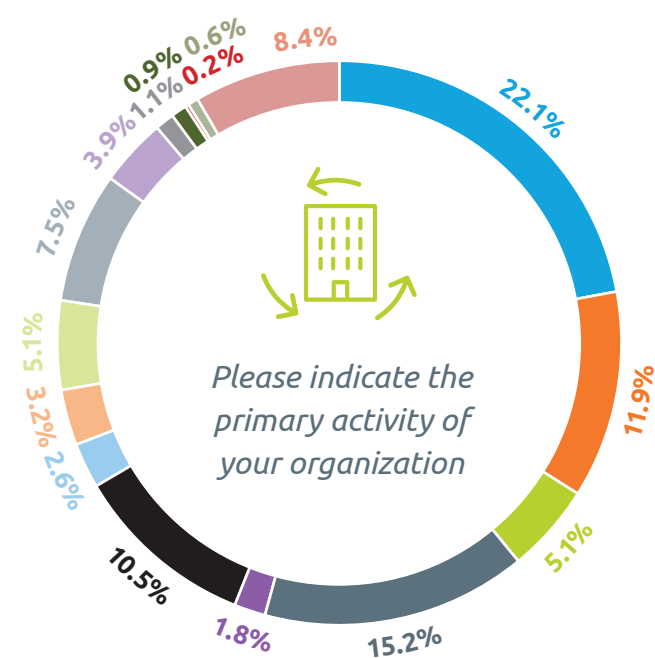


Figure 28. Please indicate the primary activity of your organization using the SIC 2007 categories given below. (For example, a management consultancy would mark “Professional Services” only and not the sectors in which its clients operate.)

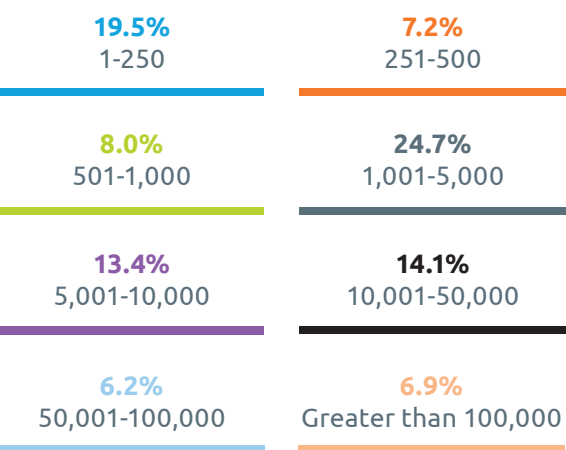
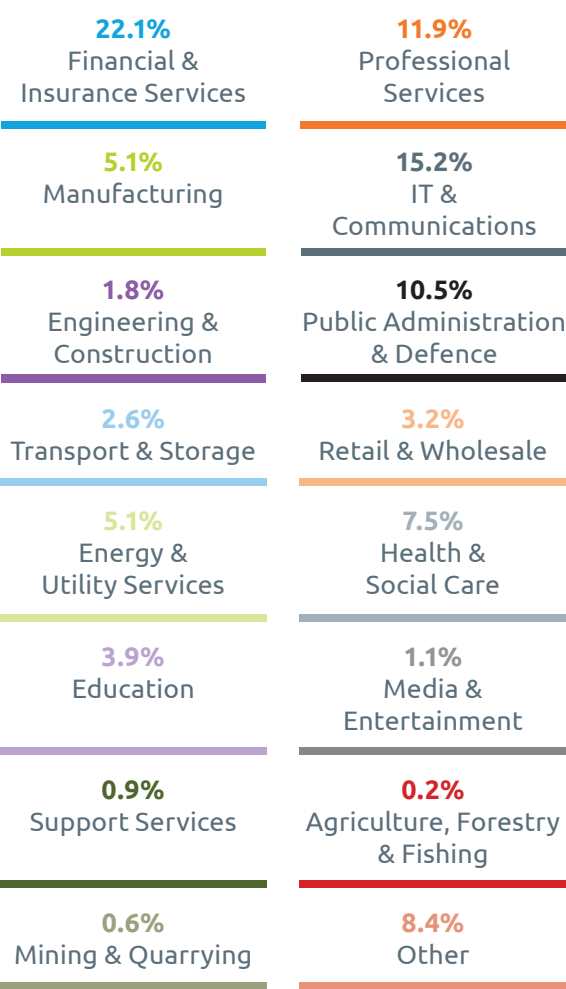


Figure 29. Approximately how many employees work at your organization?

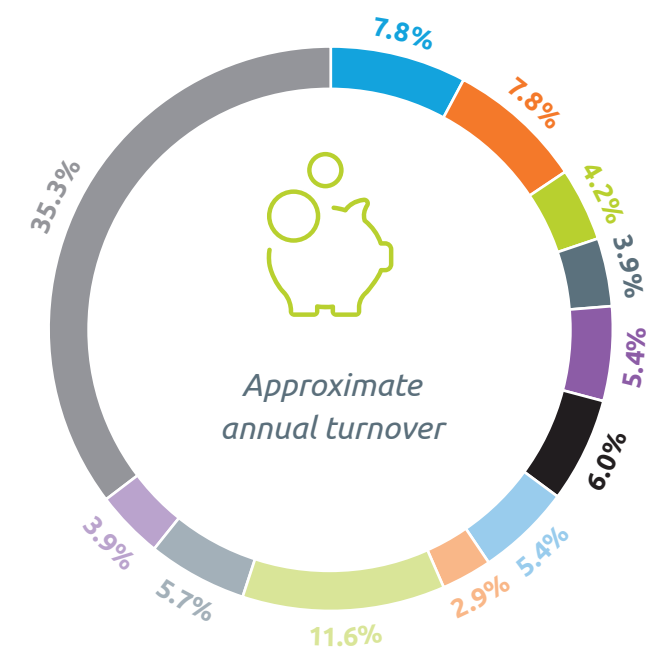
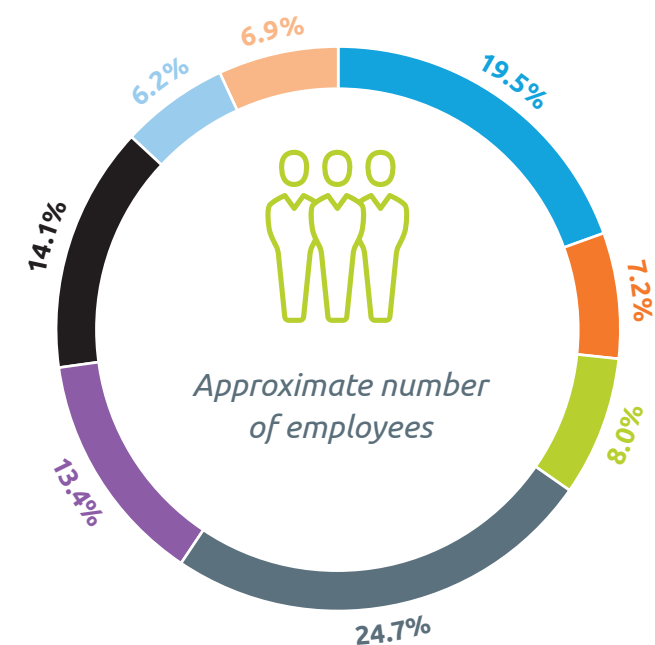
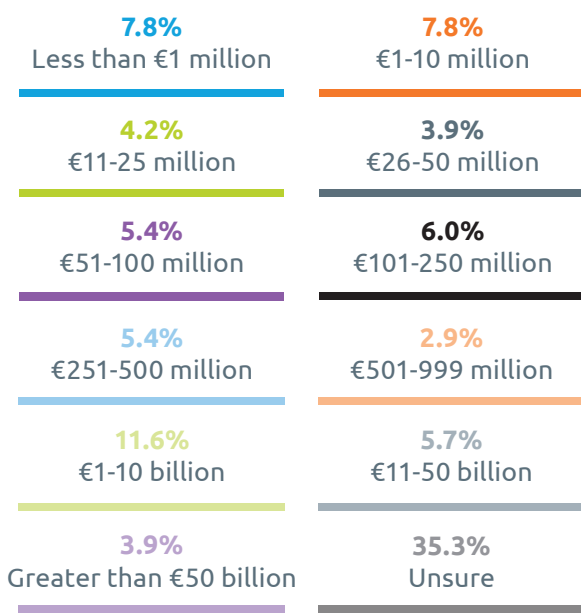


Figure 30. What is the approximate annual turnover of your organization?





About the Authors

Rachael Elliott (Head of Thought Leadership)

Rachael has twenty years’ experience leading commercial research within organizations such as HSBC, BDO LLP, 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](mailto:rachael.elliott@thebci.org)

Catherine Thomas MBCI (Research and Insight Manager)

Catherine comes from a resilience background in central and local government with a particular focus in public health and community incident response. She holds a Masters degree in Forensic Investigation from Cranfield University and a BSc in Forensic Investigation from Canterbury Christ Church University. She has a background in research from an analytical and qualitative perspective and has a particular interest in delving into the qualitative detail behind our surveys through investigative research



She can be contacted at [catherine.thomas@thebci.org](mailto:catherine.thomas@thebci.org)

Kamal Muhammad (Research and Insight Analyst)

Kamal has more than five years’ experience as a researcher in economics, working on economic growth and development. He previously worked as a Research Fellow/Economist at the United Nations, where he was attached to the Macroeconomic Policy Division and was responsible for conducting policy analysis and providing technical assistance to Member States. He holds a PhD in Economics (University of Hull) and a Masters in Development Economics and Policy (University of Manchester).



He can be contacted at [kamal.muhammad@thebci.org](mailto:kamal.muhammad@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](http://www.thebci.org).**

Contact the BCI

**+44 118 947 8215 | [bci@thebci.org](mailto:bci@thebci.org)**

10-11 Southview Park, Marsack Street, Caversham, RG4 5AF, United Kingdom.

Acknowledgements

The BCI would like to thank F24 for their support with this report.



## ABOUT F24

F24 is the leading software-as-a-service (SaaS) provider for alerting and crisis management for sensitive and critical communications in Europe.

With FACT24, F24 is able to offer a highly innovative solution and help customers all over the world to successfully and efficiently manage incidents, emergencies and critical situations.

In addition, the eCall platform offers solutions for the high-volume communication of critical to confidential information in the business environment.

### **12 locations and more than 2,500 customers**

Founded in 2000, F24 AG is headquartered in Munich, Germany, and supports companies and organisations in more than 100 countries around the globe with its subsidiaries in Zurich, London, Trondheim, Paris, Luxembourg-City, Madrid and Munich along with its branches in Mexico City, Santiago de Chile, Brussels, Vienna and Dubai. F24's customers come from the following sectors: energy, industry, trade, banks & insurance, healthcare & pharmaceuticals, tourism, aviation, logistics & transport, IT & telecommunication and public organisations.

Around 2,500 customers around the world rely on the solutions of F24 to manage their communication requirements as part of the daily communication of critical and confidential information or in the event of a crisis.

### **Recommended by Gartner and multiple ISO-certified**

F24 AG is the only non-US company listed in the current Gartner report for emergency/mass notification services (EMNS). Listing in the Gartner report makes F24 one of the most prestigious providers of EMNS and as the first European-based company, meets the institute's stringent requirements. The Board of Directors of F24 AG consists of Christian Götz, who founded the company with Ralf Meister, Dr. Joerg Rahmer and Jochen Schütte.

F24 is the first company in the world to be certified by 'The British Standards Institution' (BSI) for its integrated information security (ISMS) and business continuity (BCMS) management systems. In addition to annual checks carried out by an independent, accredited institution, successful re-certification as per ISO/IEC 27001:2013 and ISO 22301:2012 standards was achieved in 2013, 2016 and 2019.

## Contact F24

**+49 89 2323638 81** | **[www.f24.com](http://www.f24.com)** | **[patrick.eller@f24.com](mailto:patrick.eller@f24.com)**

Ridlerstraße 57, 80339 Munich, Germany





Business Continuity  
Institute

## Business Continuity Institute

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

[bci@thebci.org](mailto:bci@thebci.org)  
[www.thebci.org](http://www.thebci.org)

Correct as of January 2020

# F24