Business Continuity Institute

EMERGENCY COMMUNICATIONS REPORT 2019

Correct as of January 2019

F24

Foreword
BCI

When business continuity and emergency management professionals talk about effective response capability, they often mention the "Golden Hour". This is the earliest time period following a catastrophic event when those in charge of the immediate response aim to establish stability and control – to understand the situation, assemble resources, notify key stakeholders, anticipate issues and begin to consider response options. Optimal use of the "Golden Hour" is a crucial foundation for an effective, robust response; it provides a window of opportunity to "catch up" with the crisis and get ahead of the deluge of problems and demands that is just about to arrive.

An organization's ability to react quickly and maximise this brief opportunity is greatly affected by its level of preparedness, the quality of information to hand and the quality of the support tools available. The 2019 Emergency Communications Report provides some indispensable insights that reveal how organizations are preparing for these challenges.

When reading the report, I was encouraged that 84% of respondents confirmed they could activate their response plans within an hour. It is also reassuring to see that the ability to activate plans and teams within this short timeframe has a powerfully positive association with training and exercising. Effective exercising aids a rapid response.

The report also confirms my personal experience; that in an emergency many organizations struggle to communicate effectively, in the face of inaccurate contact information and the continuous challenge of efficiently gathering and sharing reliable information.

Emergency alert and communications software can help to address these challenges. A well-designed solution can provide structured, time-saving support to gather incident updates and efficiently distribute communications to diverse stakeholder groups. Of course, they are not a cure-all and still rely on good quality data combined with proficient users.

If you are grappling with these and other emergency communications challenges, this report will provide you with some useful intelligence. It may help to verify that you are on the right track or save you from repeating the mistakes of other organizations. It may simply confirm that you are not alone in confronting these issues and that there are solutions available.

I would like to express the BCI's thanks to F24, our partner in producing the Emergency Communications Report. Most importantly, the report rests on the contributions of 650 respondents. Without their participation and willingness to share their real-world experiences we would be unable to benefit from the insights contained in the following pages.

Tim Janes
Hon FBCI
Chair of the BCI

Foreword
F24

F24 is delighted to partner with the Business Continuity Institute for the established Emergency Communication Report which has resulted in many changes not least this being the first time for F24 to contribute to this report. The Emergency Communications Report provides valuable insights for our profession. This year's report format has been adapted to reflect the changes in our world in order for our profession to evolve with the continuous changes and demands that today's fast paced world presents.

As our world is highly interconnected and globalised, the requirements for communication are now higher than ever before. Time has become even more critical, where even seconds can make a huge difference in business continuity. Information overload makes it more difficult to aggregate reliable information efficiently and additionally with GDPR, data security has rightly gained significant new importance. To be able to achieve these requirements, technology plays a crucial role and becomes even more important. There are many facets, such as tools for emergency notification as well as the role of connected devices / internet of things (IoT), and the change of usage from desktop to mobile. All these examples have great influences on day-to-day work within Emergency Communications and Crisis Management and therefore this needs to be considered carefully when planning and implementing such solutions.

I am pleased to see that six out of ten companies are now using software for emergency notification. This is an improvement compared with 2017 (from 49% to 59%), however there is still more that can be done, especially within critical situations where technology can be used very profitably: The numbers within the report show that organizations, who employ IoT technology, have significantly faster response times when informing their target groups than those who don't (see Table 4, page 22).

Of course, technology cannot take over the responsibility of these complex situations as typically they can only be handled by humans. But this does not mean that technology cannot be used to add value, in order to improve our processes and quality. Saving time by having automated notifications through "sensors" gains more flexibility and redundancy which are two obvious advantages.

There are many more extremely interesting results within this report, so before you dive into the following pages in greater depth, I want to thank all 650 participants of this year's report – which by the way is the highest number ever reached – as thus underling the importance of emergency communications and the important insight that this report provides.

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

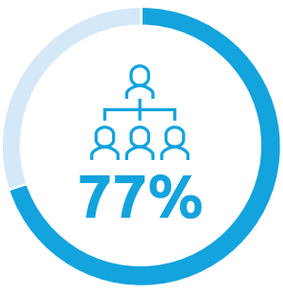
Contents

1 Executive Summary

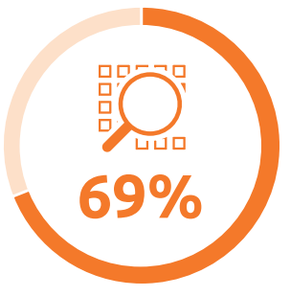
Executive Summary

This report aims to provide guidelines on how to build an effective emergency communications plan and raise awareness on best practice. The executive summary advises on how to build and implement an effective plan.

Look out for the main challenges:



Communicating with staff



Gathering, validating and sharing accurate information

Locating staff

During a crisis, always ensure:

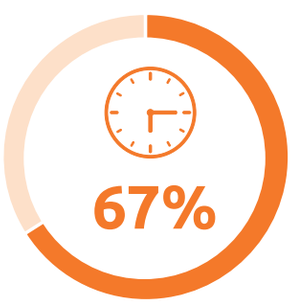
Constant exchange of information

Alerting Experts first and Constant exchange of info second

Two-way communication

What makes a plan succeed?

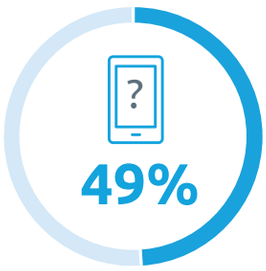
Timeliness: 84% activate their plans within one hour



Escalation: 67% would escalate communications to top management within one hour

Response levels: 80% achieved their ideal response levels

What makes a plan fail?



Inaccuracy: 49% lack accurate staff contact information

Unclear communication: 42% mention lack of understanding from recipients

Human error: 33% experience the failure of manual processes

Training and exercising ensure timeliness

of respondents have training programmes and exercises in place

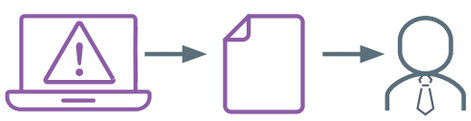
of those who run exercises can activate their plans within one hour

of those who do not run exercises can activate their plans within one hour

Similarly, achieved response rates are much higher among those who exercise their plans.

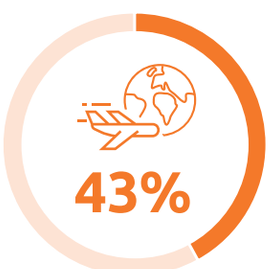
Emergency notification systems ensure readiness

Organizations adopting emergency notification software are quicker at activating their emergency communications plans and escalating the necessary information to top management.

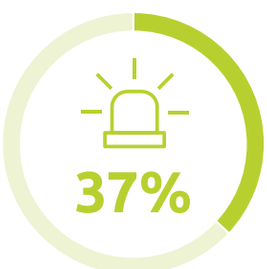


The mobile workforce needs to be able to withstand a crisis too. This is how:

Fulfill duty of care obligations



Have a travel risk management plan



Have an emergency notification software

The ideal emergency communications team includes:

BC manager

Corporate communications

Security manager

In the age of fake news and social media, it is crucial to gather accurate information during a crisis. This is what most practitioners rely on:

Always ensure contact details are up-to-date

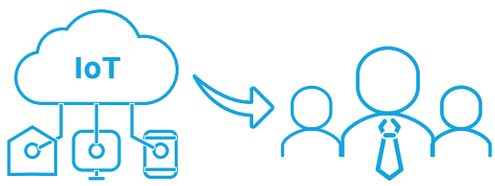
Check weather alerts

Collaborate with local authorities

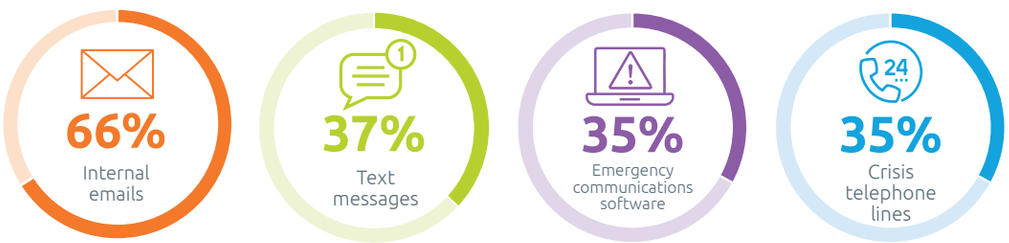
Check official social media account

Check official media accounts

Internet of Things (IoT) solutions can help respond and escalate communications to top management more quickly.



The most widely used emergency communications processes regardless of the crisis scenario are:



However, specific scenarios such as cyber attacks and the loss of a key employee required more tailored measures.

Cyber attack:

Loss of a key employee

2

Main Report

Emergency communications uptake

- **Most organizations employ emergency notification software for their plans;**
- **Communicating, gathering sound information and locating staff remain the biggest challenges**
- **Among those who use messaging apps, the majority adopt free public commercial solutions such as WhatsApp**
- **Those who adopt emergency notification software are able to initiate their emergency communications plans more quickly and escalate information to their top management.**

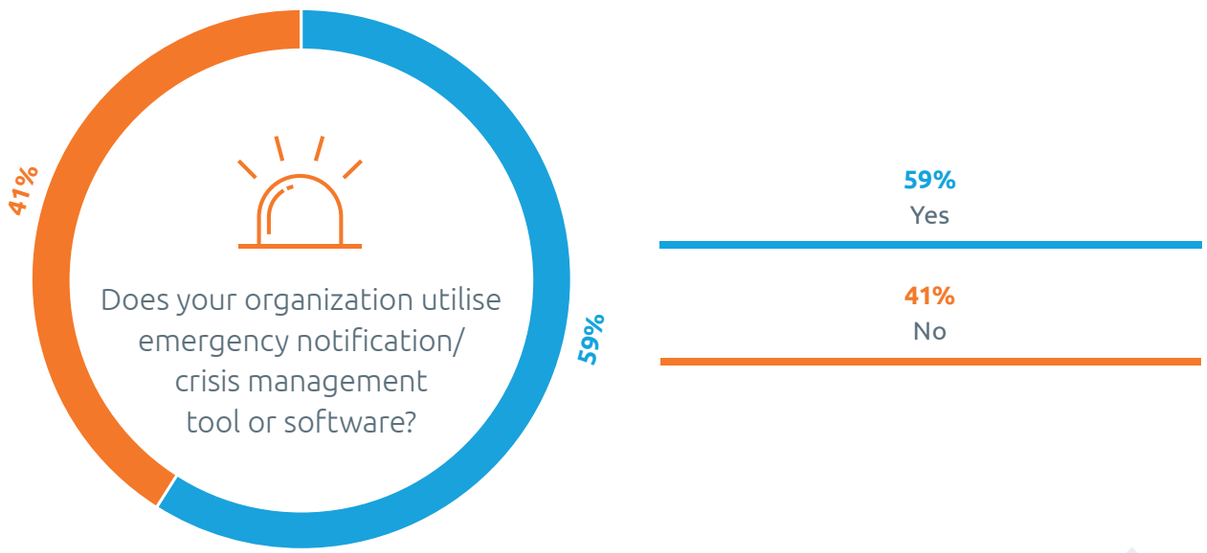


Figure 1. Does your organization utilise emergency notification/ crisis management tool or software? (N=639)

Almost 6 out of 10 organizations utilise crisis management tool or emergency notification (Figure 1). This is welcoming news as this is higher than last year's report (49%). Of these organizations, two-fifths use computer or laptop in managing emergency situations (Figure 2), followed by smartphone (37%), and tablet (19%).

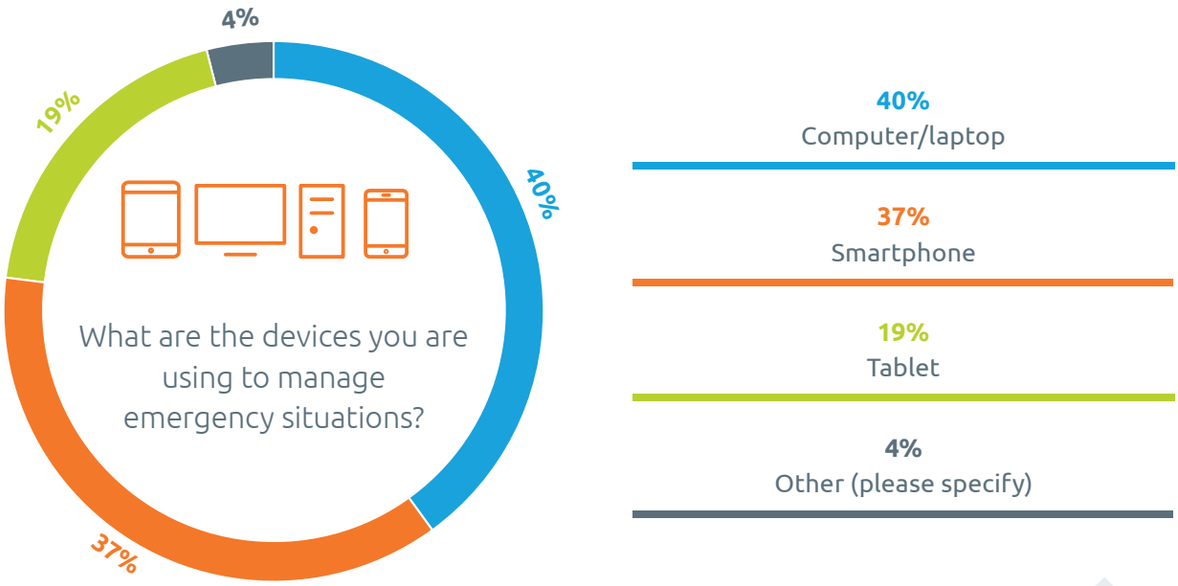


Figure 2. If YES, what are the devices you are using to manage emergency situations? Tick all those applicable. (N=372)

	Able to initiate their plans within one hour	Able to escalate communications to top management within one hour
Organizations with emergency communications software	75%	71%
Organizations without emergency communications software	53%	59%

Table 1. Organizations initiating their plans in an actual emergency.

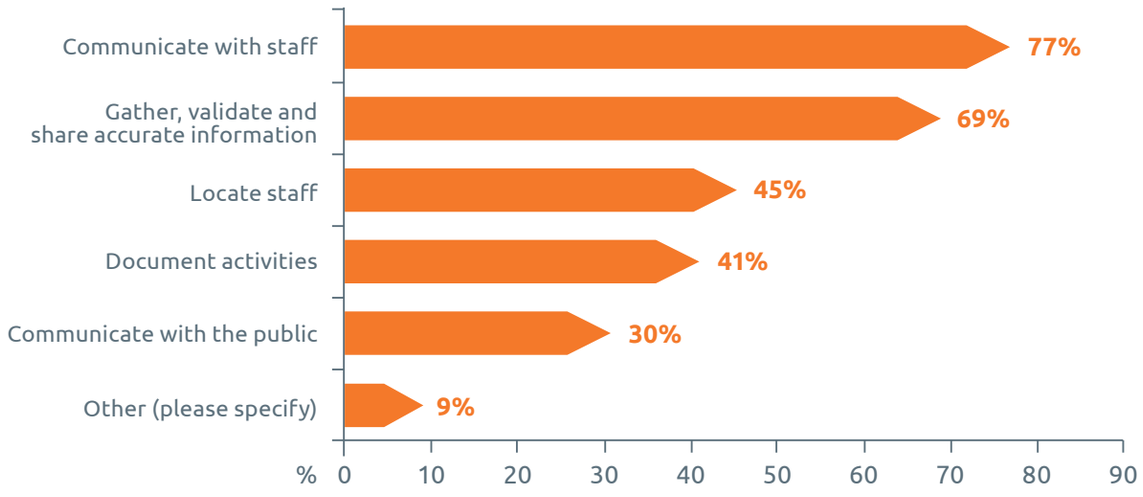


Figure 3. What are your key challenges during emergency notification/crisis management? Tick all those applicable. (N=615)

Communicating with staff (77%) is seen as the greatest challenge during crisis management (Figure 3). This is followed by gathering, validating, and sharing accurate information (69%), and locating staff (45%) ranked third.

21%
We're using messaging apps from private environments e.g. WhatsApp, WeChat and think that's a good solution

24%
We're using messaging apps from private environments e.g. WhatsApp, WeChat but we realise that's not the optimal solution

25%
We would like to use messengers but there are no fitting solutions compliant with data protection requirements etc

30%
We don't use messaging apps and don't think that this will be helpful

Figure 4. What role do secure business messaging apps play in your emergency notification processes? // How important are secure business messaging apps for your emergency communications? (N=537)

While 70% of organizations either use messaging apps or would like to adopt them, some of them raise issues of data protection or utilise commercial solutions such as Whatsapp, which are not built for the purpose of crisis management. These figures reveal the need for either higher awareness on fitting solutions that are out there or for an improvement in those that already exist. (Figure 5). Similarly, 30% of the organizations do not think they can be helpful in emergency communications while 25% of them do not see messengers being compliant with data protection requirements. On the other hand, some organizations (24%) admit that they use these applications but expressed that they are not the optimal solution in communicating during an emergency, while 21% of the respondents disclose that they think it is a good solution.

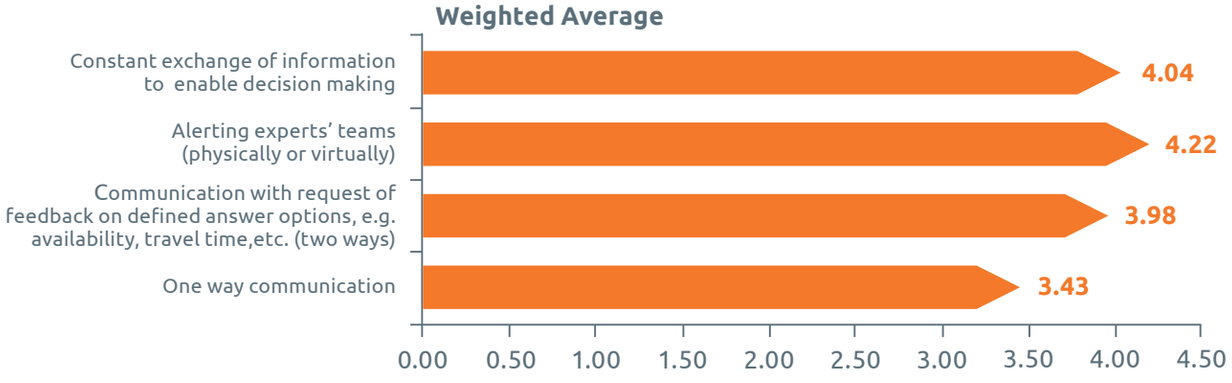


Figure 5. How important are the following tools for your alerting and emergency communications?"1" being the least important and "5" the most important. (N=538)

According to respondents, emergency notification and crisis management tools' most important features include alerting their experts' teams, both physically and virtually, as well as enabling decisions by allowing constant exchange of information among the stakeholders (Figure 5)

Activation time

- **80% achieved their expected response rate**
- **84% can activate their plans within one hour**
- **67% are able to escalate communications to top management within an hour during a crisis**
- **Reasons for failure are heavily influenced by human error rather than technology**

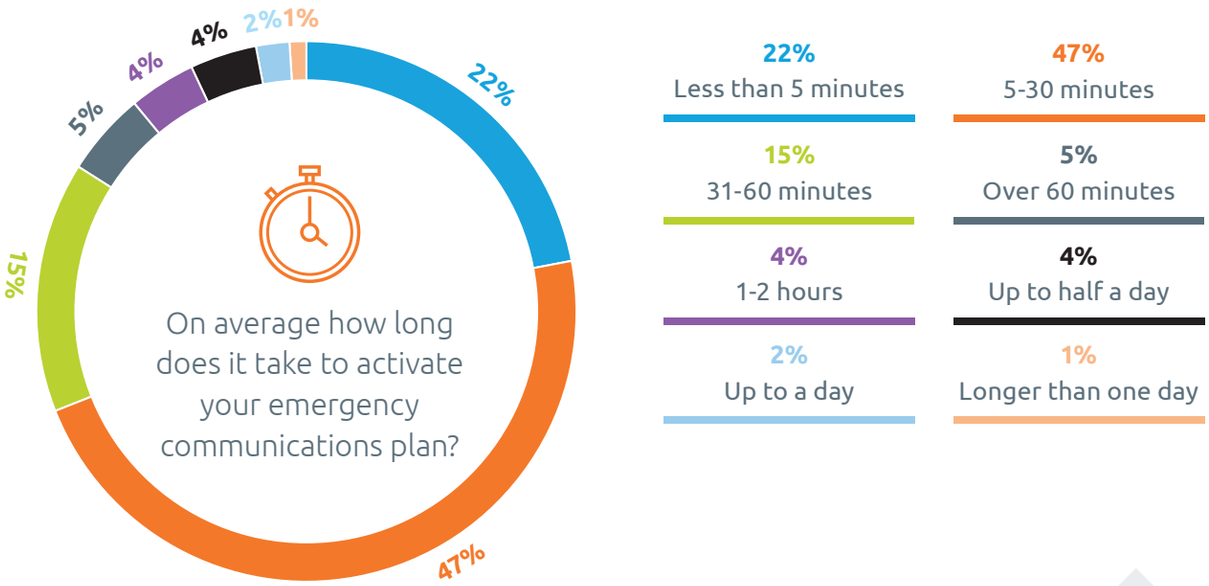


Figure 6. On average how long does it take to activate your emergency communications plan? (N=535)

One key element in emergency communication plans is the response time of activating the plans (Figure 6). This year's report shows slower response time as only 22% of the organizations take less than five minutes to activate their plans, which is lower than last year's (28%). In addition, there are more organizations (16%) that take more than an hour to do so than last year (12%). Extra efforts on reviewing, training, and exercising the existing plans are encouraged to shorten the response time.

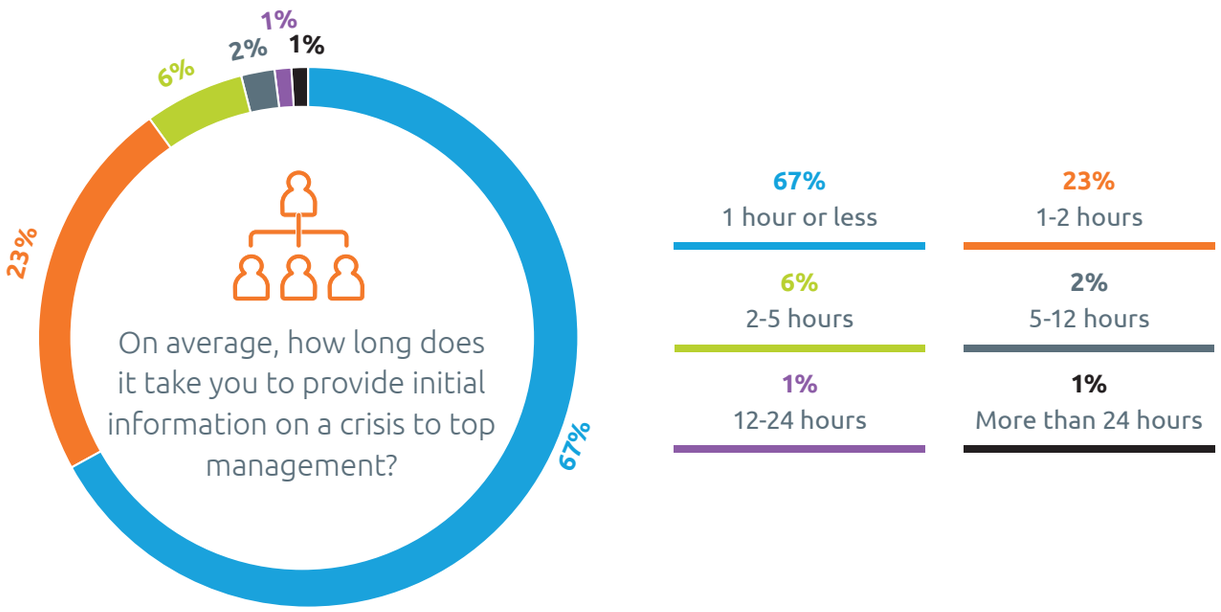


Figure 7. On average, how long does it take you to provide initial information on a crisis to top management? (N=525)

On the other hand, more than three-fifths (67%) of the organizations take an hour or less in providing initial information on a crisis to top management, while 1 out of 10 organizations (10%) take more than 2 hours to do so (Figure 7). Further, most organizations report to achieve their expected response levels (median = 80%).

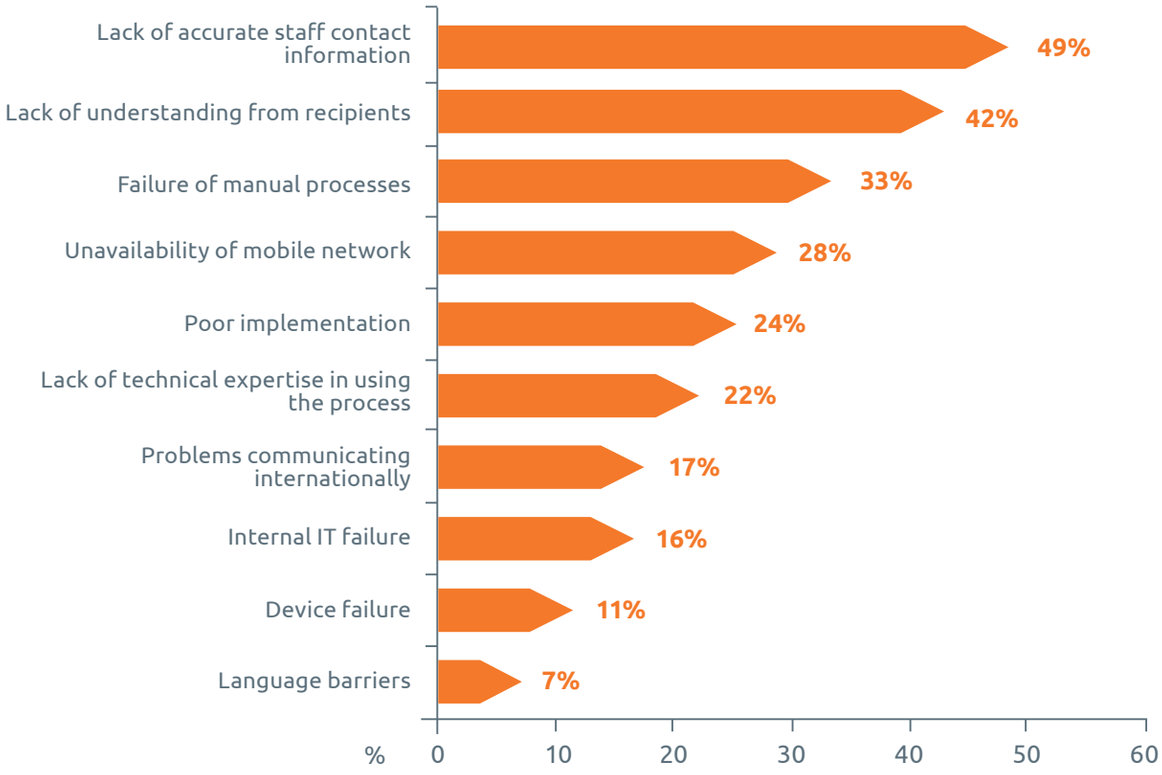


Figure 8. If you failed to achieve your accepted response levels, what caused the failure? Tick as many as applicable (N=425)

Failure of emergency communications (Figure 8) is mostly caused by lack of accurate staff contact information (49%), lack of understanding from recipients (42%), failure of manual processes (33%), unavailability of mobile network (28%) and poor implementation (24%). Human related factors remain a concern in deploying emergency communication plans as understanding and implementing the plans remain in the top concerns of the respondents.

Training and exercising

- **The overwhelming majority of organizations validate their plans with training and exercising activities.**
- **Most organizations had to activate their plans due to an actual emergency in the past year.**
- **Organizations conducting training and exercising activities are able to activate and escalate their plans more quickly.**

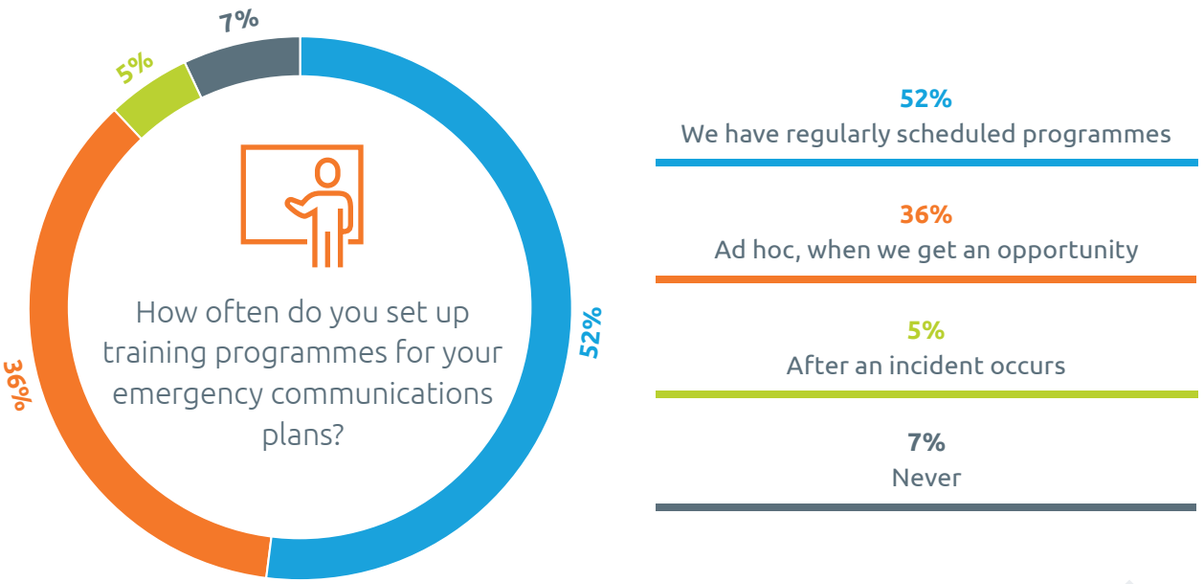


Figure 9. How often do you set up training programme for your emergency communications plans?

Five out of ten organizations have regular scheduled training programmes for emergency communications plans (Figure 9). Further, only one in twenty organizations report to have conducted training after an incident occurs and more than a quarter (39%) report conducting training on an ad hoc basis.

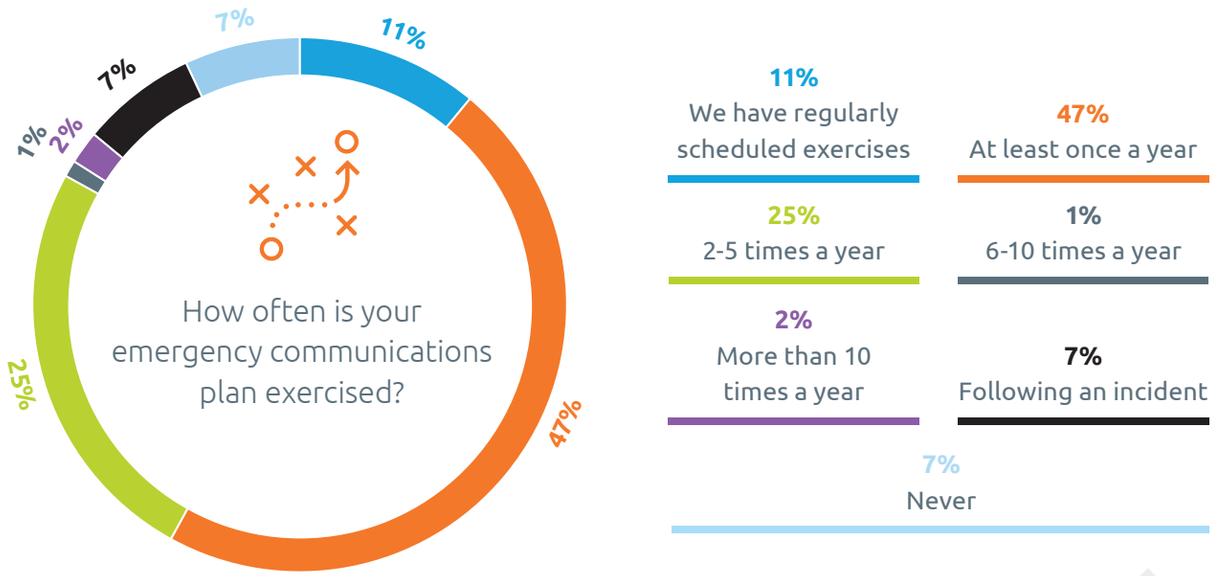


Figure 10. How often is your emergency communications plan exercised?

Exercising emergency communications plans is vital and helps organizations not only to mirror reality but also to measure their level of preparedness in case of actual event. Figure 10 shows that 47% of respondents exercise their plans at least once a year; this shows a 5% increase from last year (42% to 47%). This is really encouraging, given the fact that, last year a contraction of 7% was recorded. On the other hand, this year we witnessed one of the sharpest declines in the number of organizations that claim to have regularly scheduled exercise by 19% (30% to 11%). Moreover, 14% of the organizations either never exercise their plans or do so on an ad hoc basis.

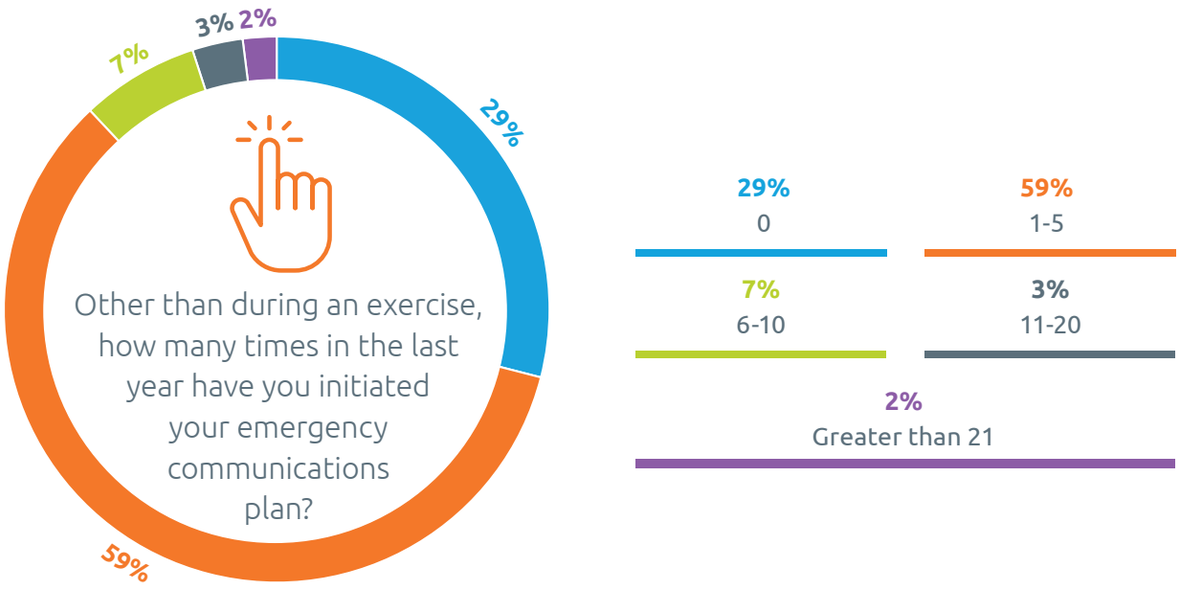


Figure 11. Other than during an exercise, how many times in the last year have you initiated your emergency communications plan?

Over two-thirds (71%) of organizations activated their emergency communications plans at least once in the last twelve months (Figure 11). This is consistent with last year's results and it proves the importance of emergency communications plans, as the majority of professionals reveal how they have had to deploy them in a real emergency.

	Organizations initiating their plans at least once in the previous twelve months
2018	71%
2017	71%
2016	69%
2015	62%

Table 2. Organizations initiating their plans in an actual emergency.

Communicating with a Mobile Workforce

- **Most organizations operate in more than one country;**
- **Roughly one in three operate in high-risk areas**
- **Organiations protect their mobile workforce through Duty of Care arrangements, travel risk management programmes and emergency communications software**

43% 1

18% 2-5

10% 6-10

29% 11+

Figure 12. How many countries does your organization operate in?

36% YES

64% NO

Figure 13. Does your organization consider the countries they travel to as high risk? (N=470)

Figure 14. How does your organization ensure the implementation of effective emergency communications plans for travelling or remote-based staff? Tick all those that apply. (N=442)

	More than 50% of staff travel globally	Less than 50% of staff travel globally
Duty of Care	58%	57%
Travel risk management programme	53%	41%
Emergency communications software	39%	35%

Table 3. Mobile workforce arrangements compared to % of staff travelling globally.

Over half (57%) of organizations operate in at least two countries (Figure 12) and on average 15% of their staff travel internationally. Of these organizations, roughly one third consider the countries their staff travel to as high risk (Figure 13). Furthermore, organizations adopt different measures to ensure effective implementation of their respective emergency communications plans. The most popular ones include fulfilling duty of care obligations (57%), having a comprehensive travel risk management plan (43%) and deploying emergency communications software (37%) (Figure 14).

The figures also reveal that organizations with a higher number of employees traveling abroad tend to make a wider use of best practice such as Duty of Care, travel risk management policies and the adoption of emergency communications software (Table 3). This shows the popularity of these tools in order to manage a global mobile workforce.

Emergency Communications Processes

- **Business continuity teams tend to be in charge of emergency communications plans;**
- **Adverse weather is the main trigger of emergency communications plans;**
- **Most organizations ensure the acquisition of reliabile information through: accurate contact details, weather alerts, collaboration with local authorities, official social media accounts, official media accounts**
- **Organizations mainly resort to manual processes, such as manual lists on excel, when updating contact details.**

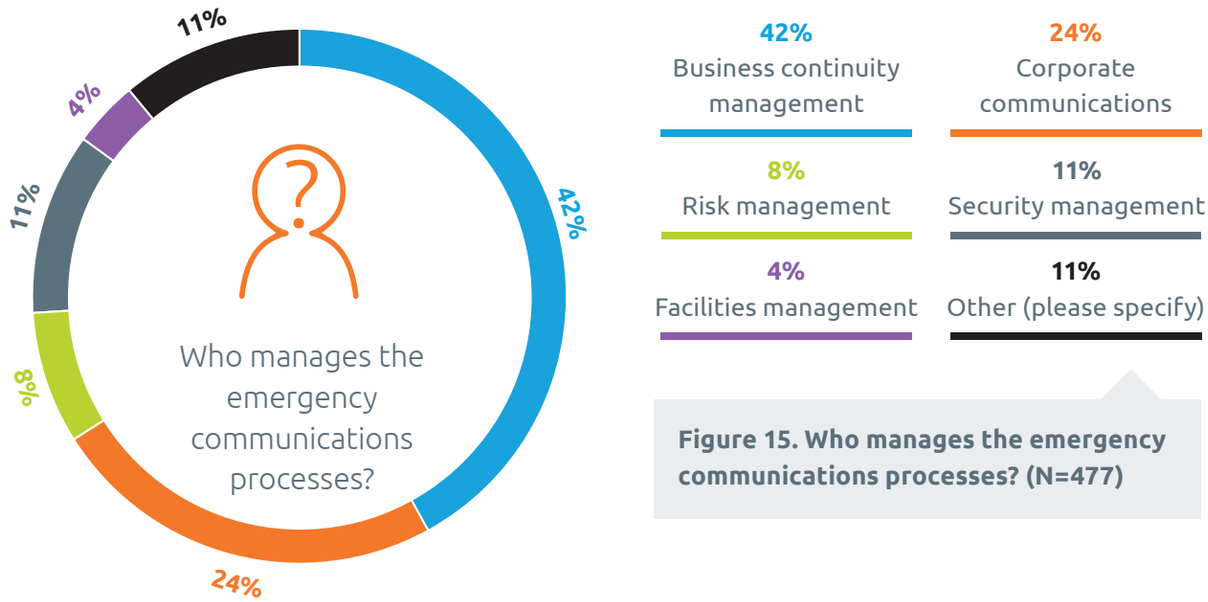


Figure 15. Who manages the emergency communications processes? (N=477)

Our findings show that business continuity is the main function that manages the emergency communications processes (42%). It is followed by corporate communications (24%), security management (11%) and risk management (8%) sections respectively (Figure 15). Whilst different sections are tasked to manage the emergency communications plans (depending on the organization), it is paramount for organizations to encourage cross-functional working, so that effective implementation of the emergency communications plans can be achieved.

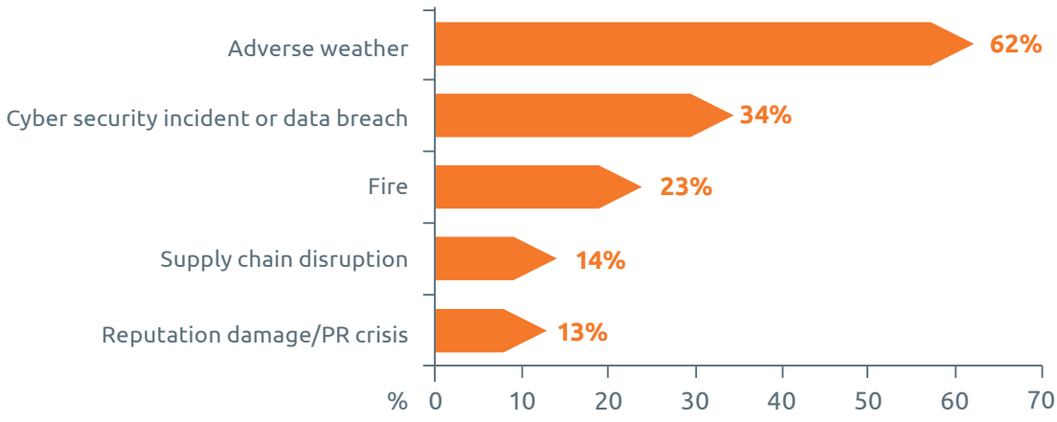


Figure 16. Which of the following triggered your emergency communications plan in the past twelve months? Tick all those applicable. (N=432) (Top 5)

Adverse weather (62%) is the number one trigger of emergency communications plans (Figure 16); this shows an increase of 8% from the previous year (54% to 62%). Cyber security incidents or data breach (34%) is ranked second, and the rest of the top five are: fire (23%), supply chain disruption (14%) and reputation damage/PR crisis (13%). It is interesting this year that supply chain disruptions make it to the top five, which can partly be attributed to the severe snowstorms witnessed in the early part of 2018 across Europe and North America. It is also not surprising to see reputation damage among the top five, given the number of major PR crises witnessed in the past year, such as those involving H&M, Starbucks and Facebook.

Figure 17. How do you ensure the acquisition of relevant sources of information in the context of managing an emergency case / crisis scenario? (N=448)

Organizations use different sources to ensure acquisition of relevant information to manage an emergency case or crisis scenario (Figure 17). Roughly two-thirds of the respondents either always ensure employees' contacts are up to date or check weather alerts (69% and 64%). Further, 53% collaborate with local authorities to get reliable information or check official social media accounts, whilst 52% check official media accounts.

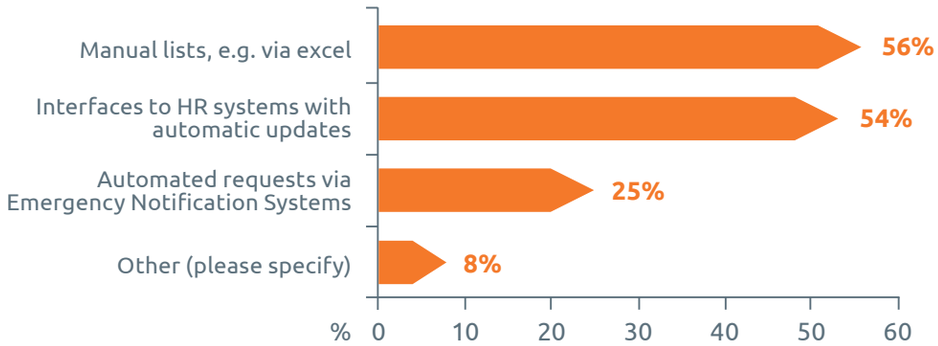


Figure 18. How do you ensure contact data of employees, experts, etc. is up-to-date? Tick all those applicable. (N=448)

More than half of the respondents either use manual lists or interfaces to HR systems with automatic updates to ensure contact data of staff etc. is up-to-date, whilst only 25% use automated requests via emergency notification systems (Figure 18). It is important to highlight however, the majority of the respondents use manual lists (56%) via Excel as their key instrument for ensuring contact data of staff etc. is up-to-date.

Technology

- **One-third of organizations have either adopted IoT devices in their emergency communications plans or are planning to do so;**
- **Those who embed IoT devices are able to respond and escalate communications more quickly.**

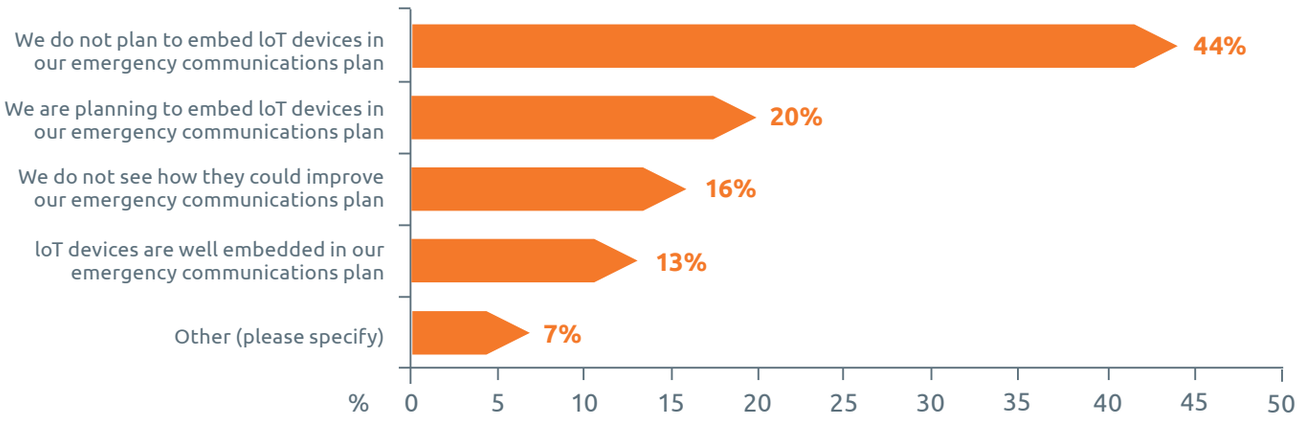


Figure 19. How do you see the implementation of Internet of Things devices within emergency communications? (e.g. fire sensors sending out alerts) (N=431)

	Organizations activating emergency communications plans within one hour	Organizations able to escalate communications to top management within one hour
Organizations employing IoT technology	88%	76%
Organizations not employing IoT technology	78%	66%

Table 4. IoT Technology in emergency communications.

A third of organizations (33%) either have well embedded IoT devices within their emergency communications plan or are planning to do so (Figure 19). Organizations that prove to be the most advanced in using this technology come from financial & insurance services, IT & telecommunications and public administration and defence. There is also a good amount of small and medium enterprises (20%) that rely on IoT to communicate during a crisis. On average, organizations that employ IoT tend to be able to activate their plans earlier and are able to escalate communications to top management more quickly than those who don't.

Crisis Scenarios

- **Internal emails remain the primary means of communication during a crisis, regardless of the crisis scenario (Figure 20 A-G).** Furthermore, there appears to be a balanced mix of technology and more traditional tools when it comes to emergency communications. Emergency communications software, manual call trees and crisis telephone lines are indeed widely used across nearly every scenario.
- **On the other hand, it is interesting to point out specific solutions for some scenarios, such as recurring to crisis telephone lines and a website announcement in the case of a cyber attack.** In this instance, it would make sense for organizations to use these tools, especially if experiencing some downtime following a breach, so that frontline staff is still able to communicate with the public. On a similar note, social media is used specifically for the loss of a key employee, which highlights the need once more for monitoring of modern platforms when handling a crisis.
- **The popularity and usefulness of employing internal emails during a crisis, however, can turn into a double-axed sword, in the case IT systems were not functioning properly.** Previous BCI research found out that cyber attacks have been the main concern for organizations in the last three years and that IT outages are the main consequence of a cyber attack[1]. One way to remedy to this is to be assisted by a notification software with an independent IT infrastructure, which some organizations do, in order to diversify and back-up their emergency communications plans.

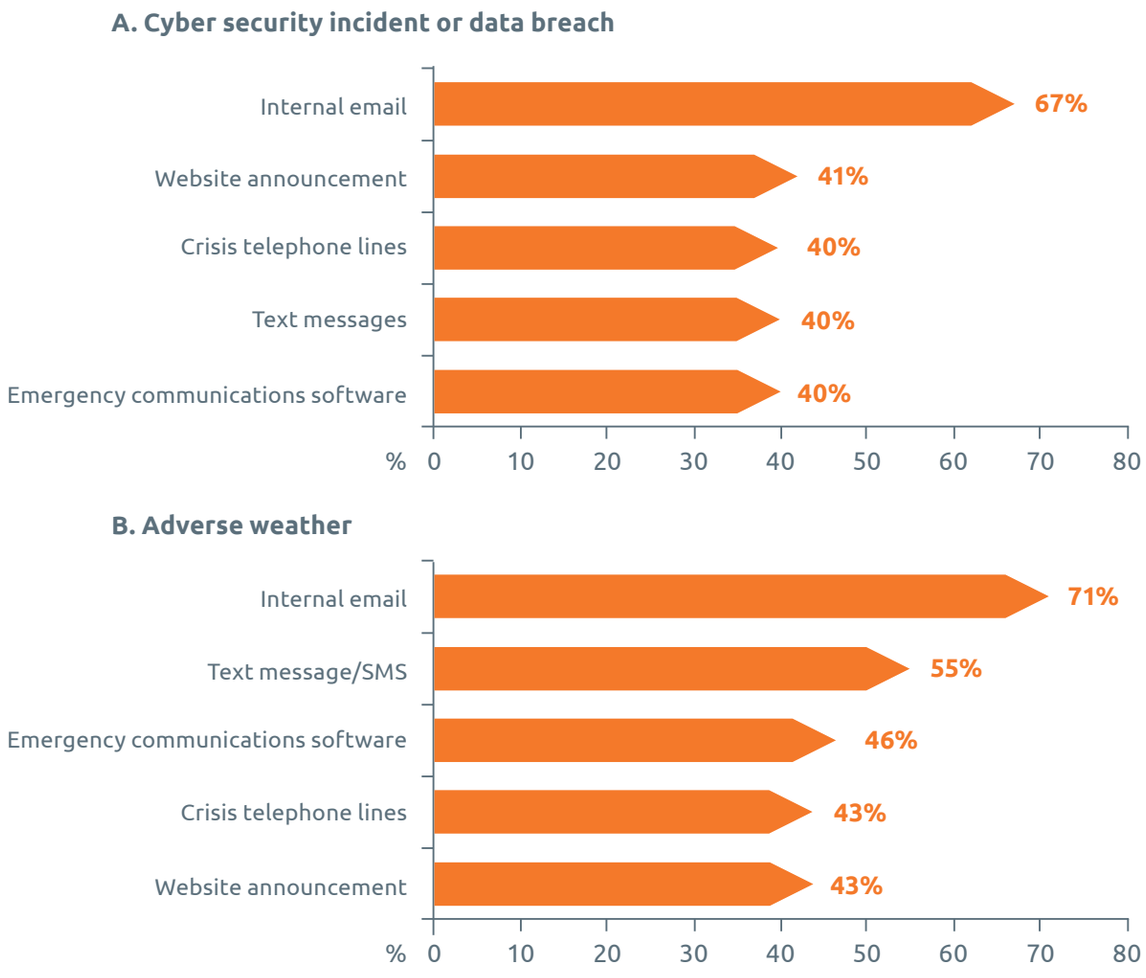
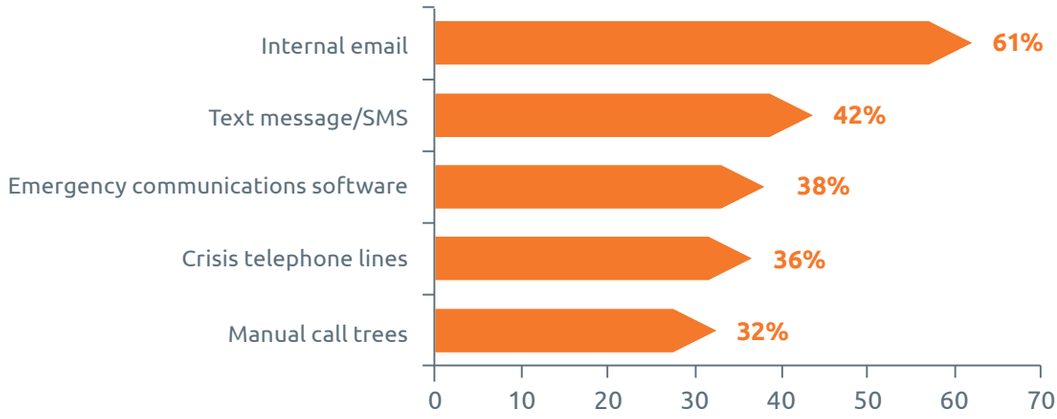


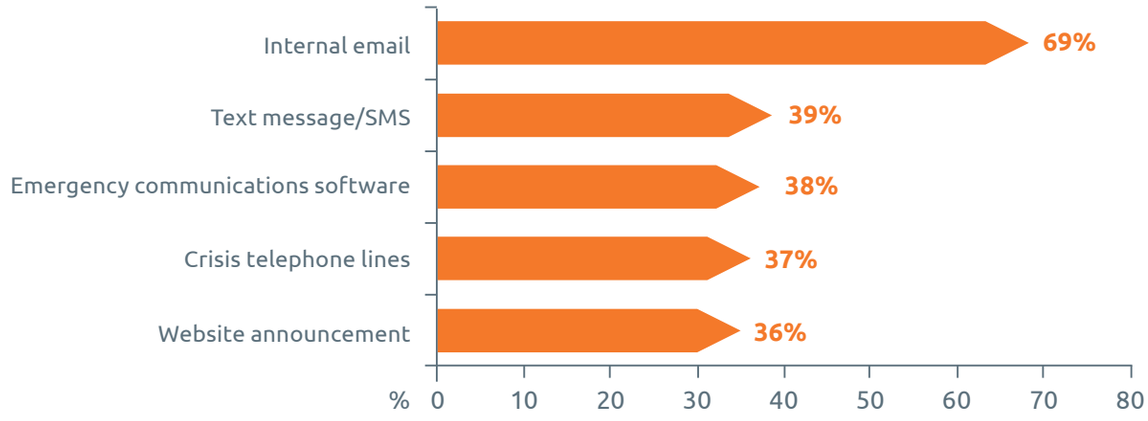
Figure 20. Which processes would you use to communicate during each of the following scenarios? (N=405)

1. BCI Horizon Scan Report 2018; BCI Cyber Resilience Report 2018.

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



D. Disease outbreak



E. Health and safety incident

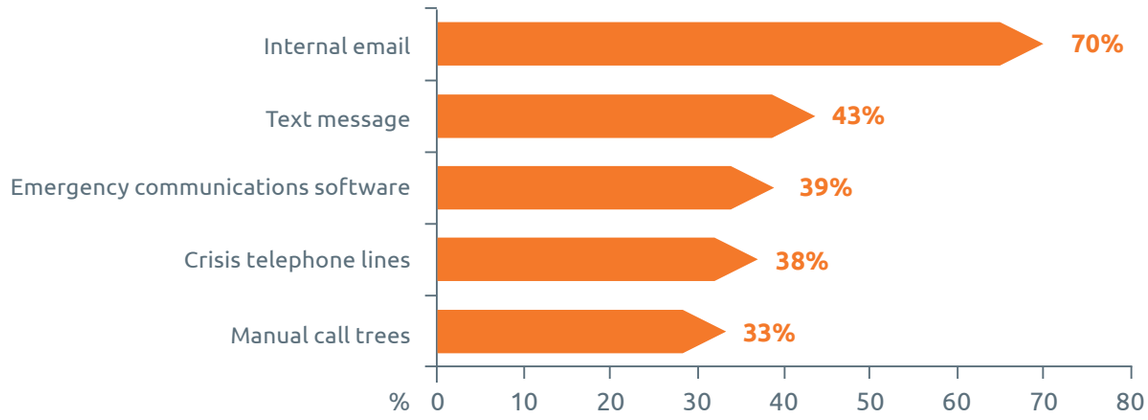


Figure 20. Which processes would you use to communicate during each of the following scenarios? (N=405)

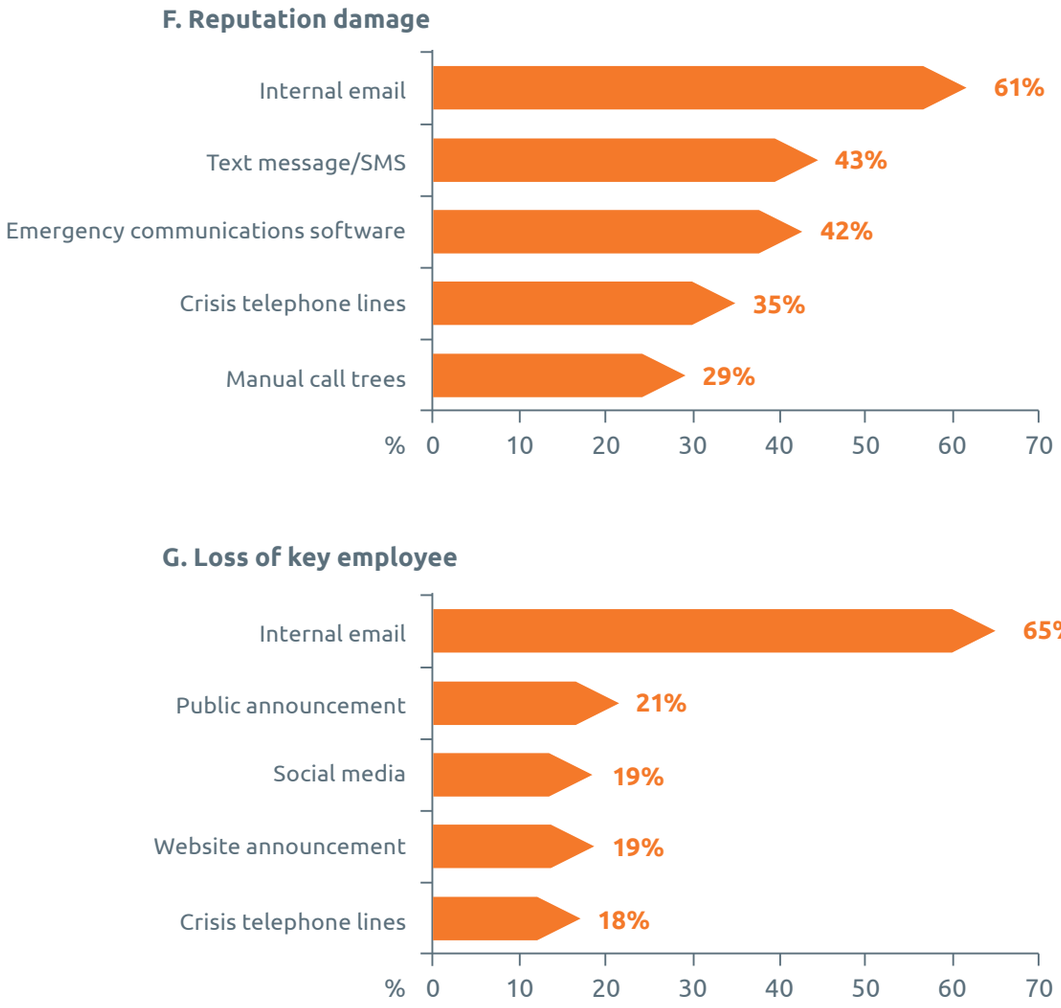
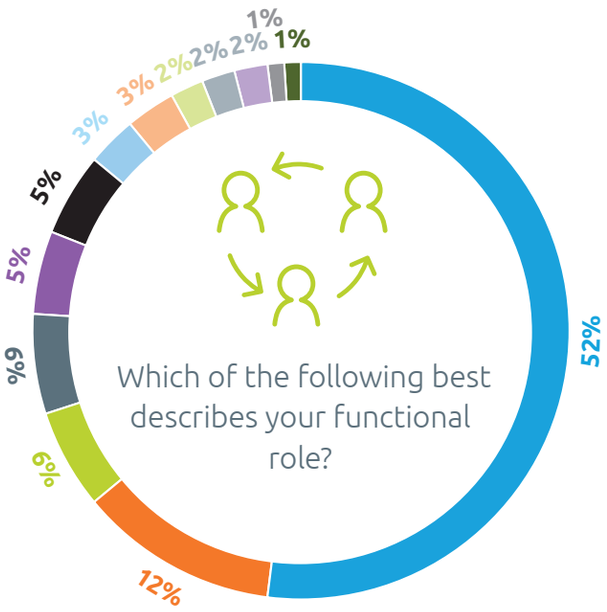


Figure 20. Which processes would you use to communicate during each of the following scenarios? (N=405)

3 Annex

Annex



52% Business continuity

12% Risk management

6% Emergency planning

6% Crisis management

5% IT disaster recovery/IT service continuity

5% Other (please specify)

3% Information security

3% Top management

2% Health and safety management

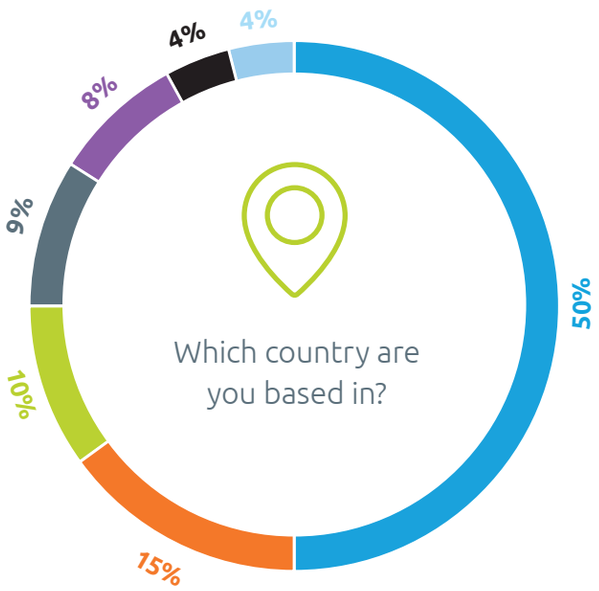
2% Quality/Business improvement

2% Physical security

1% Supply chain and logistics

1% Internal audit

Figure 21. Which of the following best describes your functional role? (N=650)



50% Europe

15% North America

10% CALA

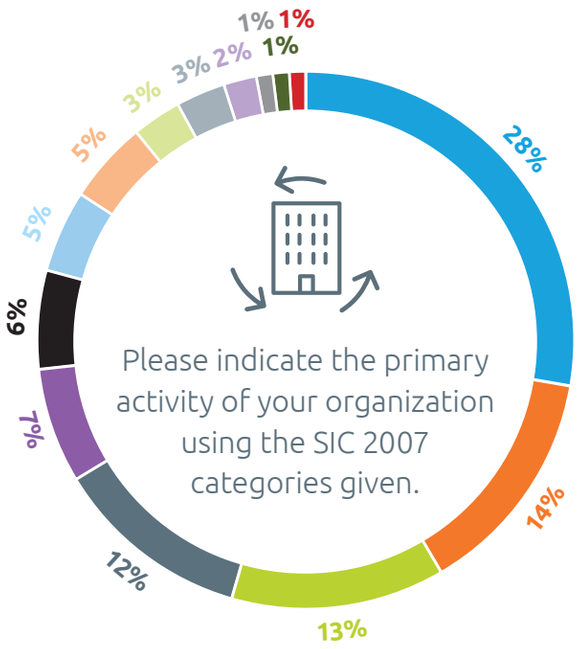
9% Asia

8% Australasia

4% Mena

4% Sub-Saharan Africa

Figure 22. Which country are you based in? Please select from the dropdown menu. (N=650)



28% Financial & Insurance Services

14% IT & Communications

13% Professional Services

12% Public Administration & Defence

7% Other (please specify)

6% Health & Social Care

5% Manufacturing

5% Energy & Utility Services

3% Transport & Storage

3% Education

2% Retail & Wholesale

1% Support Services

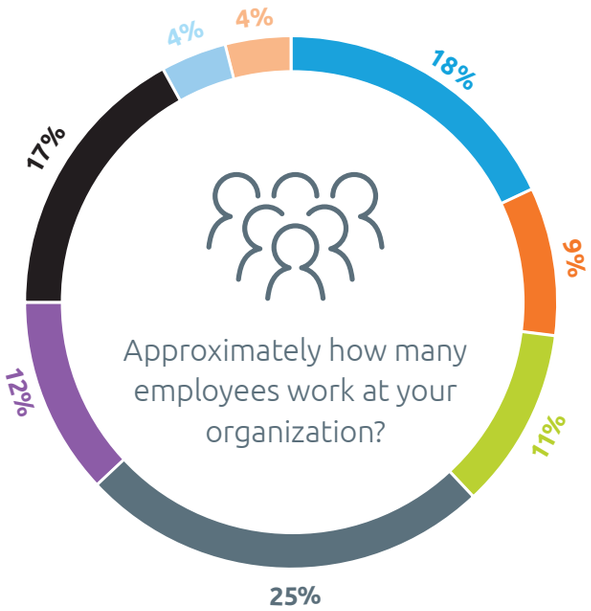
1% Media & Entertainment

1% Engineering & Construction

0% Mining & Quarrying

0% Agriculture, Forestry & Fishing

Figure 23. Please indicate the primary activity of your organization using the SIC 2007 categories given. (N=650)



18% 0-250

9% 251-500

11% 501-1,000

25% 1,001-5,000

12% 5,001-10,000

17% 10,001-50,000

4% 50,001-100,000

4% Greater than 100,000

Figure 24. Approximately how many employees work at your organization? (N=650)

About the Authors

Gianluca Riglietti CBCI
(BCI Research & Insight Manager)

Gianluca Riglietti is Research & Insight Manager at the Business Continuity Institute. He has experience writing academic and industry publications, speaking at international conferences and delivering projects on cyber security, business continuity, risk and resilience for companies such as BSI, Siemens, Zurich, International SOS and SAP. Previously he obtained a Masters in Geopolitics, Territory and Security from King's College London. His past professional experience includes working for the International Affairs Unit in the Italian Presidency of the Council of Ministers.

He can be contacted at gianluca.riglietti@thebci.org.

Lucila Aguada
(BCI Research & Insight Analyst)

Lucila Aguada (BCI Research & Insight Analyst) is a licensed psychometrician with expertise in quantitative and qualitative research. She has a Bachelor degree and is a Masters candidate in Psychology from the University of the Philippines. She has conducted research on behalf of non-profits, pharmaceutical and healthcare clients. She is also a qualified teacher with more than seven years of experience, specializing in early childhood and special needs education.

She can be contacted at lucila.aguada@thebci.org

Kamal Muhammad
(BCI Research & Insight Analyst)

Kamal Muhammad is a Research Analyst at the Business Continuity Institute, he 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.

Acknowledgements

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

F24

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 8,000 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

Lucila Aguada
BCI Research & Insight Analyst, 10-11 Southview Park, Marsack Street, Caversham, RG45AF, United Kingdom
+44 118 947 8215 | **bci@thebci.org**

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.

11 locations and more than 1,700 customers

Founded in 2000, F24 AG is headquartered in Munich, Germany, and supports companies and organisations in more than 80 countries around the globe with its subsidiaries in London, Madrid, Paris, Luxembourg City, Zurich 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 1,700 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 and 2016.

Further information can be found here: www.f24.com

Contact F24

Patrick Eller
Corporate Marketing & PR Manager
Ridlerstraße 57, 80339 Munich, Germany
+49 89 2323638 81 | **patrick.eller@F24.com** | **www.f24.com**

Business Continuity Institute

Business Continuity Institute

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

bci@thebci.org
www.thebci.org

F24