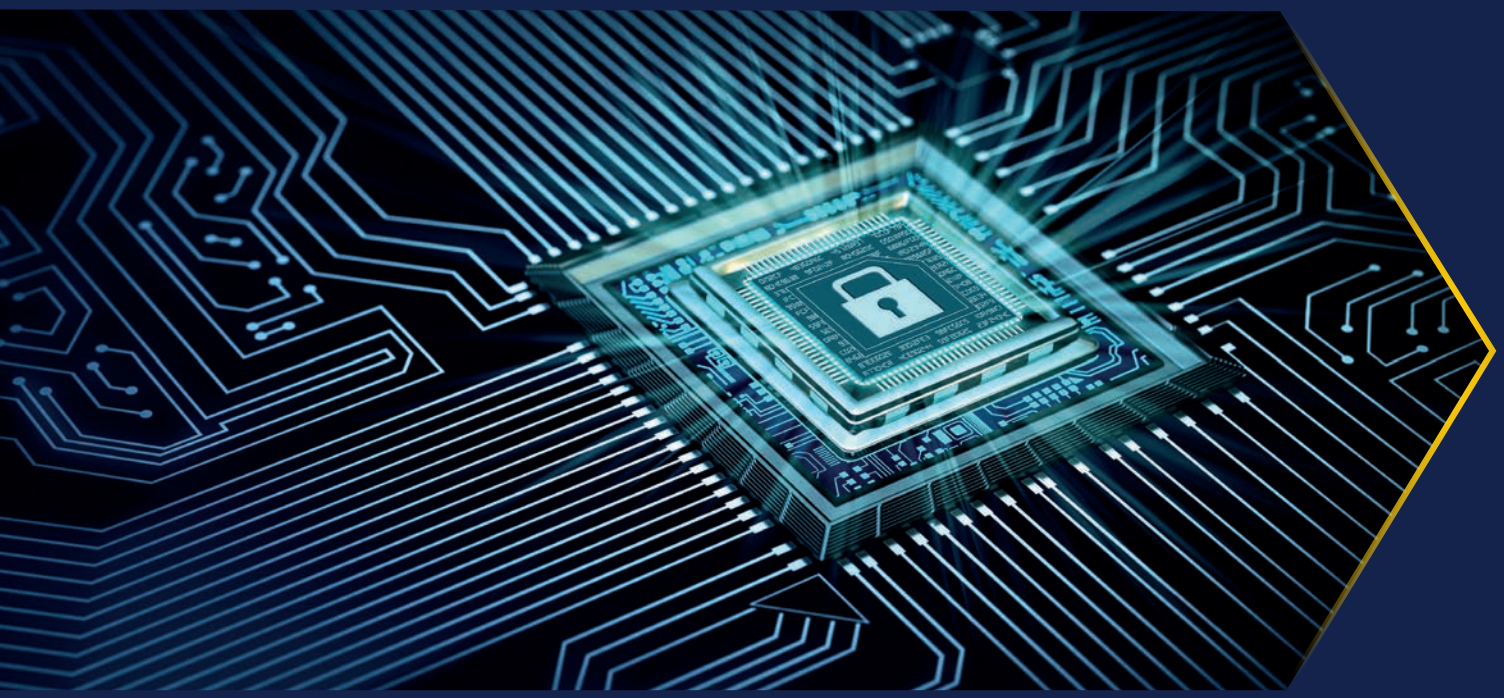
Find out more
www.thebci.org

Thought Leadership

Technology & Business Continuity in Organizational Resilience



SUNGARD® AVAILABILITY SERVICES™

Leading the way to resilience

Contents

Foreword

Until the arrival of COVID-19, the threat to IT resilience was firmly at the top of the agenda for organizations around the world. These threats have not vanished during the pandemic and some of the new working practices, such as widespread Work-from-Home arrangements, have exacerbated the situation by enlarging the organization's IT footprint.

This report provides an overview of the IT resilience landscape and examines how the Business Continuity and IT service continuity disciplines can come together to create optimal IT resilience practices to benefit the whole organization.

As organizations become increasingly reliant on technology, the need for resilient IT systems is more vital than ever. The pandemic has amplified the importance of IT resilience for organizations. This fact is reflected in the survey responses which reveal IT resilience was the most significant factor in a successful organizational response to COVID-19.

The BCI has published a series of organizational resilience reports in recent years, with a common theme being the importance of collaborative working cultures. So, it is encouraging to see that the nearly 600 international responses to the report survey demonstrates a healthy mix from the business continuity, IT, cyber/information security, risk management disciplines as well as top management.

While close collaboration is ideal, we should not ignore the real challenges that practitioners find in their search for resilient IT. The report provides both statistical evidence and practical examples of these difficulties. It is well-known among seasoned business continuity professionals that end-users and IT departments will have different priorities when it comes to IT resilience. The report takes these varied perspectives further and reveals that those working within IT Service Continuity often prioritise IT infrastructure, while those in Business Continuity prioritise IT applications.

Fortunately, the report shows that where Business Continuity and IT teams work closely together, organizations can overcome these differences and achieve real success in IT resilience.

The report also identifies several important factors which will be essential contributors in taking the principles of IT resilience forward to produce a practical result. For example, the ability of business continuity professionals to engage in meaningful resilience discussions with their IT colleagues will be greatly enhanced if it is underpinned by a sound understanding of IT systems and practices. This does not mean we must become IT experts, but it does indicate a need to move outside established areas of proficiency.

This leads to the idea that practical IT Resilience content, along the lines of the BCI's Good Practice Guidelines, might benefit business continuity professionals. A similar suggestion was raised in the BCI's recent report, The Future of Business Continuity, which shows the concept may be worth further consideration.

The BCI greatly appreciates the generous support of Sungard AS in producing the Technology and Business Continuity in Organizational Resilience report. I also thank everyone who participated in the survey and interviews. They have contributed to an insightful report that combines timely analysis and practical lessons which we hope will help to enhance your own organization's IT resilience.

Tim Janes, Hon FBCI
Chair of the BCI Board

SUNGARD® AVAILABILITY SERVICES™

Foreword

2020 has been a year of significant turbulence for organizations around the globe. This timely report shines a light on the importance of integration between IT, the wider business, and senior leadership. In some organizations siloes exist between IT and business operations, some of which see IT as just a 'service provider'. Although, with the cost of downtime estimated by IDC to be $100,000 per hour for a large organization, IT should be an area for significant leadership interest. We are pleased to have partnered with the BCI for this report on the relationship between Business Continuity (BC) and Technology, which captures an encouraging improvement in the degree of IT-Operations integration over the course of the COVID-19 disruption.

Some statistics in this report particularly stand out to us. During the pandemic, 94.7% of organizations have had staff working from home, with 35% reporting all staff have been working from home. This widespread move to virtual working environments has placed greater emphasis on the requirement for resilient and secure IT infrastructure. Remote working placed additional security demands on already stretched IT support teams, with 27.6% of organizations reporting having to add additional security measures to systems during the pandemic. Throughout 2020, we have seen an increase in the incidence of cyber-attacks exploiting the broader attack surface created by remote working.

Traditional Disaster Recovery (DR) solutions were designed with datacentre failure in mind, rather than the corruption of data typically seen in a Ransomware attack. The "weaponization" of data through ransomware should cause leadership to pause for thought as to how they view and prioritise the recovery of data. That close to a fifth of survey respondents indicate that DR procedures were not up to date, with another 17% unsure whether procedures were up to date, demonstrates the lack of a coherent approach. An integrated approach would see organizations addressing the twin DR priorities of datacentre recovery (infrastructure, applications and network) and data recovery. Leadership should set the priorities for data risk management, matched with the provision of the necessary resources for appropriate DR arrangements for Production and Archive data.

Leaders, BC and Technology professionals alike will gain valuable insights from this report and find it useful in formulating strategies and responses to the challenges they face, now and in the future. There is compelling evidence that some senior leadership continue to view IT as a commoditised service, rather than recognising it as a critical enabler for the organization. Where senior leadership has an understanding of the technologies and range of options available, they are better able to provide clear and coordinated direction to the business. This allows a closer alignment of IT Infrastructure and DR to organizational priorities. Regulators are taking a closer interest in Operational Resilience and outsourcing, requiring Boards to approve their business's impact tolerances, and also demonstrate internally and externally that identified vulnerabilities are managed and mitigated. This should encourage a much more coherent approach, rather than the all too often siloed approach to BC, IT DR, InfoSec and Supply Chain Risk Management.

Chris Butler and Tom Holloway
Lead Principal Consultants, Risk and Resilience
Sungard Availability Services

IT Resilience
Executive Summary

Executive Summary

Business Continuity departments which are closely engaged with their IT departments have the most resilient IT systems and processes: IT and IT Resilience Departments which work closely with Business Continuity, practicing "non-siloed" working practices have the most resilient working practices: although 89% of respondents ranked Business Continuity as one of their top five capabilities in the foundation of a resilient organization, the widely considered view by professionals contributing to this report is that the foundations of resilience are built on the sum of many departments, led by strong leadership.

Should IT resilience be managed by Business Continuity or IT? The BC department is more likely to put together the IT resilience Business Impact Analysis (BIA) than the IT department, but IT is responsible for IT Resilience in two-thirds of organizations. This leads to inevitable conflict between the departments in some organizations, and the lack of defined responsibilities can result in system failures and unwanted downtime. Many Business Continuity professionals would rather IT Resilience was managed by the Business Continuity department, whilst IT professionals feel it should fall under the responsibility of IT given the technical nature of IT resilience.

A separate GPG for IT Resilience could serve to create further siloing, but most agree further detail on IT resilience is needed in the current Good Practice Guidelines (GPG): Nearly nine out of ten professionals believe greater detail on IT resilience is needed, either within the current GPG or in an entirely new document. The current lack of detail on crucial areas such as IT Recovery were highlighted by several survey respondents. Some professionals did suggest caution, however. Unless a Business Continuity Manager already had an IT background, some of the most technical components of IT resilience should be addressed by IT resilience experts.

Communication failures can lead to failures in resilience processes: A fifth of organizations are not confident that Business Critical Activities could be continued or restarted in line with their Business Continuity Plan (BCP), and one in ten organizations have failed to map critical processes. Many respondents attributed this failure to a lack of communication between departments, with priority products and services not agreed between departments. The presence of incumbent legacy systems also remains a reason for process failures.

Due diligence of third party IT providers is not being routinely carried out: Less than half of respondents report that their IT providers' KPIs meet their organizations continuity requirements, suggesting that there is a high degree of trust placed on third party providers to be able to provide reliable systems and services.

Different departments have different priorities when it comes to IT resilience: When creating a BCP, those working within IT Disaster Recovery or IT Service Continuity prioritise IT infrastructure, whilst those in BC prioritise IT applications. Although in many organizations the difference is not defined, the results demonstrate how both departments should be involved when creating the BCP to ensure no bias is created.

A significant minority of organizations admit to not having their DR procedures up to date, and less than a fifth are able to carry out a full DR test: Less than two-thirds of organizations report having DR procedures up-to-date and under a fifth admit being able to carry out a full disaster recovery test within their organizations. Demand for continuous uptime and financial constraints from the wider organizations were the principal reasons cited.

A lack of consideration for the potential impact of a pandemic and/or a consideration that all staff may need to work from home at short notice meant some organizations suffered unnecessary downtime: Nearly a third of organizations encountered disruption as they had insufficient hardware to allow staff to work remotely, with remote access and VPN issues also causing significant disruption for a quarter of organizations. Ensuring the breadth of disruption a pandemic can cause to an organization and/or considering how an organization is prepared for all staff to immediately move to a remote working model should now be considered crucial by organizations to stop similar disruption recurring in future crises.

Key recommendations

1. Communication is crucial: Whether IT Resilience is the responsibility of Business Continuity or IT/ IT Resilience, ensure both departments remain in close communication at all times so priorities match avoiding unnecessary tensions in a crisis scenario.

2. Different departments may have different priorities e.g. BC might prioritise business applications and IT may prioritise IT infrastructure. Given that one cannot work without the other, it is important an end to end picture is derived for a service or application. This should include its dependencies on other services and applications and all its dependent infrastructure components including hardware, storage and networks - irrespective of where these things exist in the supply chain. If parts of the jigsaw are missing, resilience will be compromised.

3. Collaboration is key: make sure priority products and services are mutually agreed between departments. This can help ensure the agreed Business Critical Activities can be continued or restarted in line with the BCP, and also ensure the agreed critical processes are mapped correctly.

4. Consider having an individual with a Business Continuity background within the IT Resilience team — or vice versa. Interviewees reported individuals with a good understanding of the processes and requirements of both departments were able to help engender best practice for IT resilience within their organizations.

5. Ensure the necessary levels of due diligence are carried out on third party providers and do not rely on Key Performance Indicators (KPIs) alone. Interrogate providers' plans, uptime guarantees and equipment specifications before the procurement stage as much as possible.

6. If your organization does not carry out a full disaster recovery (DR) test, consider the potential implication of not doing so. Partial testing is not sufficient to uncover issues within systems which could cause catastrophic issues for an organization.

7. Test all scenarios before a crisis hits. Lloyds of London famously shut its underwriting room at the start of the pandemic for the first time in decades to test its contingency systems. Such testing processes can help to uncover issues before such emergency measures have to be resorted to in a real-life scenario. For many organizations, the lack of testing and practising resulted in large scale failings of IT systems during the pandemic.

8. Ensure plans sufficiently cover the potential impact a major disaster could have on the IT systems and hardware of an organization. Purchasing additional equipment in the event of all staff working from home, for example, relies on an organization being able to acquire supplies immediately.

Enterprise Resilience

Respondents believe Business Continuity is the most important capability of a resilient organization

However, the foundations of resilience are built on the sum of many departments.

Which capabilities are important to the foundations of a resilient organization?

89.4%
Business continuity

80.3%
Crisis leadership and management

67.2%
IT service continuity

65.4%
Risk management

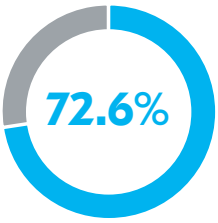
54.4%
Information security

49.4%
IT disaster recovery

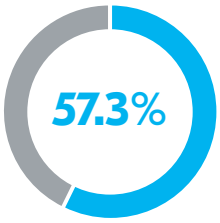
Strong leadership is vital to create a resilient culture

Strong leadership coupled with agile working methods are the lynchpins of a resilient culture.

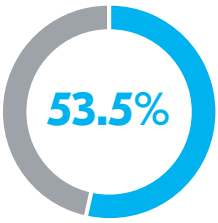
What organizational qualities are important to an organization's resilience?



Strong leadership



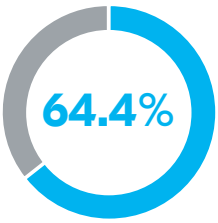
Robust, yet agile, operations



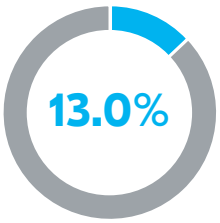
Effective communications and knowledge sharing

IT is responsible for IT Continuity in most organizations, but many respondents feel it should be the responsibility of Business Continuity

Which department currently governs IT continuity in your organization?

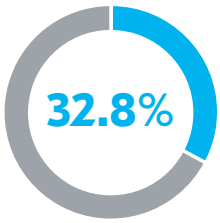


IT department

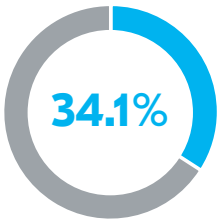


Business Continuity/ Dedicated Resilience Function

Which department do you feel should govern IT continuity in your organization?



IT department



Business Continuity/ Dedicated Resilience Function

Most believe that IT Resilience should be better represented within the BCI's *Good Practice Guidelines (GPG)*, but a minority think a separate IT Resilience GPG is required

Do you believe IT Resilience should be embedded into the BCI's *Good Practice Guidelines (GPG)*?

31.1%
I believe there should be a separate GPG for IT Resilience

56.3%
I believe the GPG should be modified to contain more detail on IT resilience

7.8%
I do not believe it should be included as there is currently enough detail in the current GPG

Communication failures are causing breakdown in resilience processes

Communication failures between departments are cited as the primary cause of failure of Business Continuity processes and procedures

How confident are you that your Business Critical Activities as set by the organization can be continued/restarted in line with your Business Continuity Plan (BCP)?

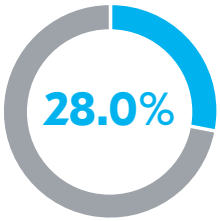
22.5%
Very confident

50.7%
Confident

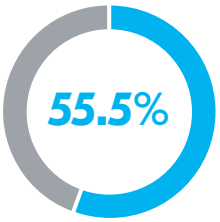
18.5%
Fairly unconfident

2.7%
Very unconfident

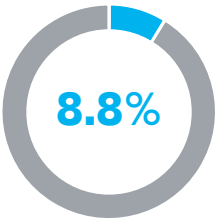
How confident are you that your Business Critical Activities as set by the organization can be continued/restarted in line with your Business Continuity Plan (BCP)?



Yes, for all systems



Yes, for critical systems only



No

Resilience Planning and Risk Management

The ownership of IT risk resides with the IT department in two-thirds of organizations, but one in five IT departments fail to share the risks with the wider organization

Communication failures between departments are cited as the primary cause of failure of Business Continuity processes and procedures

Who in your organization is responsible for technology risks?

The IT department takes ownership but shares with the wider organization to be part of the wider risk profile

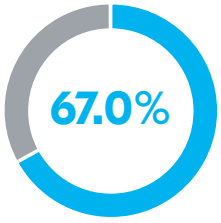
The IT department takes ownership but does not share with the organization to be part of the wider risk profile

Different departments within an organization prioritise underlying IT components differently

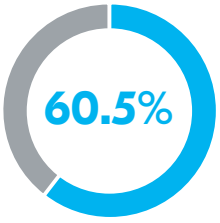
IT departments prioritise infrastructure resilience when creating the BCP, whilst BC professionals prioritise application resilience of failure of Business Continuity processes and procedures

Percentage of respondents giving "high priority" to underlying IT components when creating the BCP

IT Applications



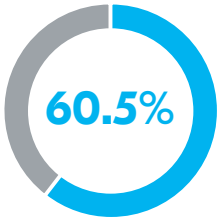
BC Professionals



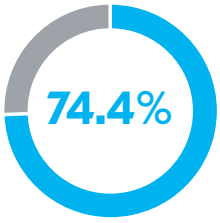
IT Professionals

Percentage of respondents giving "high priority" to underlying IT components when creating the BCP

IT Infrastructure



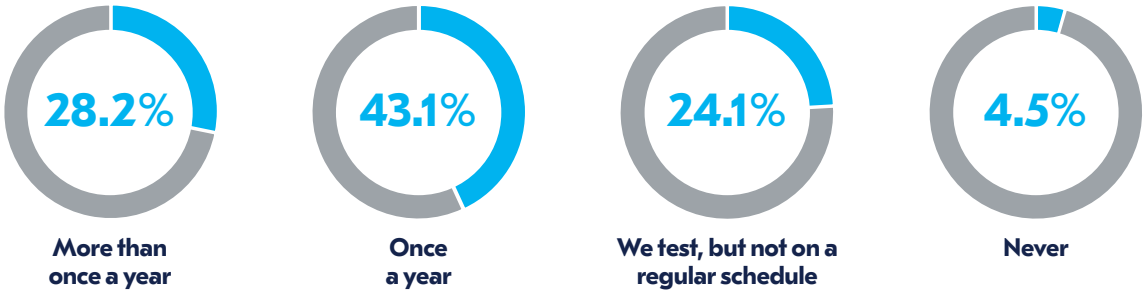
BC Professionals



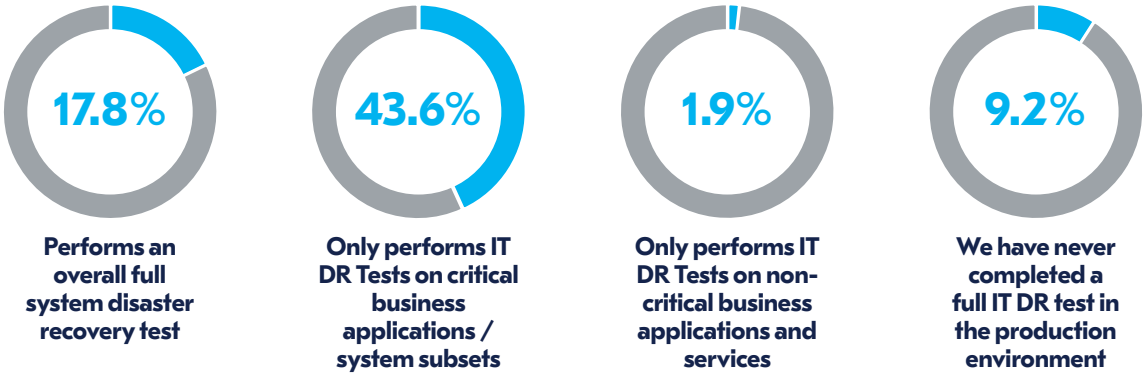
IT Professionals

Three-quarters of organizations carry out testing once a year or more, but less than a fifth carry out a full system test

How often do you test your disaster recovery procedures?



What does your IT department do when performing IT Disaster Recovery (DR) Testing?



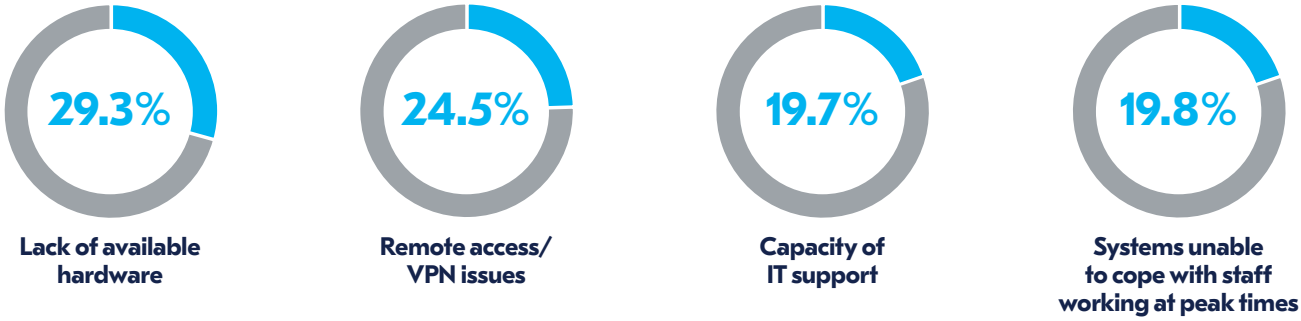
COVID-19 and Technology Resilience

94.7% of organizations have had some or all staff working from home during the pandemic resulting in pressures on IT departments to enable remote working in a secure environment

Which of these statements best applies to your organization's homeworking policy during COVID-19?

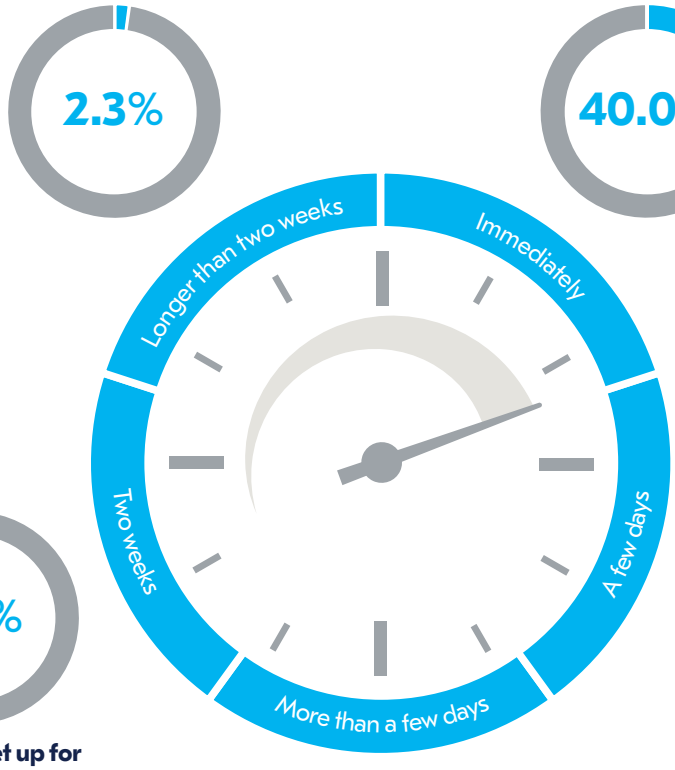
Many organizations experienced disruption as a result of the requirement for remote working

Percentage of organizations experiencing major disruption (staff unable to work or limited in the work they can carry out) as a result of specific technology issues during the pandemic



Less than half of IT departments were fully prepared for staff to work from home immediately

How prepared was your IT Department to support working from home during the pandemic?



2.3%

We were not set up for homeworking,and it took longer than two weeks before staff had the necessary equipment. This had a significant long-term impact on productivity

40.0%

Staff who were required to work from home had the equipment necessary to work from home immediately, with no impact on productivity

0.9%

We were not set up for homeworking and it took two weeks before staff had the necessary equipment. This had a significant impact on productivity

42.8%

Some staff were able to work from home immediately but it took us a few days to acquire sufficient hardware. This had a minor impact on productivity

7.2%

Staff were not set up for homeworking and it took a number of days before we could provide the necessary hardware. this had a measurable impact on productivity

Overview

IT resilience is defined as an organization's ability to maintain acceptable service levels through, and beyond, severe disruptions to its critical processes and the IT systems which support them.

IT resilience is a crucial part of the resilience jigsaw and without it, most organizations would at best flounder, and at worst, cease trading. The importance of a resilient IT infrastructure has become even more relevant during the COVID-19 pandemic as office-based workers have moved to remote working models. This was backed up in recent research for the BCI's *The Future of Business Continuity and Resilience report* where IT Resilience was ranked as the element of resilience which contributed most to the success of their organizational response to COVID-19[1].

Bob Draper (FBCI) suggests that by focusing on the areas of awareness, protection, discovery, preparedness, recovery, review and improvement, an organization will be able to minimise the potential impacts of disruptions to its IT services. At a time when cost saving is critical due to the economic pressures of the pandemic, its importance — and ensuring the Board are aware of its importance — are paramount. Draper covers each area in more detail, pointing out that each cannot be taken in isolation and there will be some inevitable overlap between some parts:

1. BCI, The (2020). The Future of Business Continuity and Resilience. Available at www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html (Accessed 29 September).

Awareness is having the knowledge of what are the normal business requirements of operational functionality; dependencies that might exist; the criticality of IT system components and elements; and the minimum acceptable operational levels. There must also be an awareness of the recovery requirements in terms of time, system capacity and performance in the event of severe disruption to, or failure of, IT systems supporting the business processes. These should be identified by an effective business impact assessment/ analysis (BIA).

Protection is more than having physical and system access security controls. It can also mean reducing the risk of system failure, e.g. removing single points of failure (SPoF) by having load balancing servers or redundant systems or components. Potential exposures to systems deemed to be critical to business processes should be identified and addressed as priority.

Discovery means that the quicker the IT team knows that a system has been disrupted, the sooner they can resolve the issue. The use of effective means of alerts of problems enable the IT group to understand and address problems before they result in severe disruption.

"An additional Discovery complication beyond speed of alerting is the accuracy and coverage of information being alerted. IT services, applications and infrastructure components are often inter-connected, as such problems often encompass multiple elements. To effectively address problems at speed, IT groups need an effective CMDB (Configuration management database) which can detail these interconnections and dependencies. An outdated inventory list will not suffice."

David Morgan
Head of EMEA Consulting
Sungard Availability Services

Preparedness means having detailed plans for addressing the effects of a disruption, such as having seamless failover of systems and components, enabling essential business processes to continue to function with no, or an acceptable minimum, break of service.

Recovery focuses on returning services and operations to business as usual levels within defined timescales and with minimal acceptable data loss following an event causing disruption or failure. This will only be achieved by having an effective and tested recovery plan which meets the business requirements in place.

Review is essential to every IT resilience programme, and includes post-incident reviews to identify the root causes of disruptions. It is a continual process which aims to enable the IT team and the business to understand potential issues and to assess and implement preventative actions to remove, or at least mitigate, the risk of severe disruption.

Improvement is the process of taking the knowledge gained from all the above and taking steps to improve systems and increase resilience, and to continuously refine disaster recovery and business continuity plans.

Bob Draper, FBCI[2]

This is the first report by the BCI to look specifically at the area of IT resilience and will examine the structures, processes and procedures practiced by organizations around the globe to ensure systems are resilient to severe disruptions.

2. Draper, B (FBCI); Childs, C (MBCI); Paul, D (MBCI); Evanson, M. 'Improving your IT resilience and disaster recovery capability'. Continuity Central (15 December 2016). Available at: www.continuitycentral.com/index.php/news/technology/1636-improving-your-it-resilience-and-disaster-recovery-capability (Accessed 29 September 2020)

Enterprise Resilience

The Foundations of a Resilient Organization

- **Business continuity is the most important capability of a resilient organization, but the foundations of resilience are built on the sum of many departments.**
- **A resilient organization is built through strong leadership**
- **The requirement for operational plans to be "agile" has come to the fore during the COVID-19 pandemic**

The foundations of a resilient organization are not built through the actions of a single department, but on the sum of many. The BCI's recent report, *The Future of Business Continuity and Resilience*[3] showed that closer relationships had been forged between departments during the pandemic — most notably between Business Continuity (BC), Crisis Management, IT, Security and the Senior Management Team/Board — and most organizations were hopeful of these closer links continuing post-pandemic.

However, despite multiple departments playing a role, Business Continuity was still considered the most important capability in the foundation of a resilient organization, with 89.4% of respondents to this survey ranking it amongst their top five capabilities. Although it could be considered surprising that there are 11% of respondents who do not view BC as one of their top five, research for the Future of Business Continuity and Resilience report revealed that 12.0% of BC professionals saw their role as entirely operational and not one which should be involved in the strategic direction of the company. The research also showed that the term resilience was often considered to be a more strategic consideration by BC professionals.

Crisis leadership and management was the second most important capability in the foundation of a resilient organization, with 80.3% of respondents selecting this as one of their top five choices. The high number of professionals believing crisis management is the foundation of a resilient organization shows a superior level of appreciation for the work of the crisis management team.

3. BCI, The (2020). The Future of Business Continuity and Resilience. Available at www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html (Accessed 29 September 2020).

Given the heightened importance of technology and IT systems and services during the pandemic, it is surprising to see technology capabilities rank so low when professionals consider the resilience capabilities of an organization. Just two-thirds (67.2%) consider IT service continuity to be a core component of resilience, with IT disaster recovery ranking even lower (49.2%). Just over a quarter of professionals (28.0%) consider high availability services to be in their top five. The lack of prioritisation of technology capabilities suggests greater levels of communication and awareness are needed between IT and other parts of the business, as well as greater collaboration between departments.

The "other" comments to this question revealed that many respondents considered all elements to be contributors to a resilient organization, with many independently adding "executive leadership and management", "organizational culture" or "operational leadership" to their list of capabilities. Indeed, a resilient organization is only created with a resilient culture, led by strong leadership.

Which of the below capabilities are important to the foundation of a resilient organization?

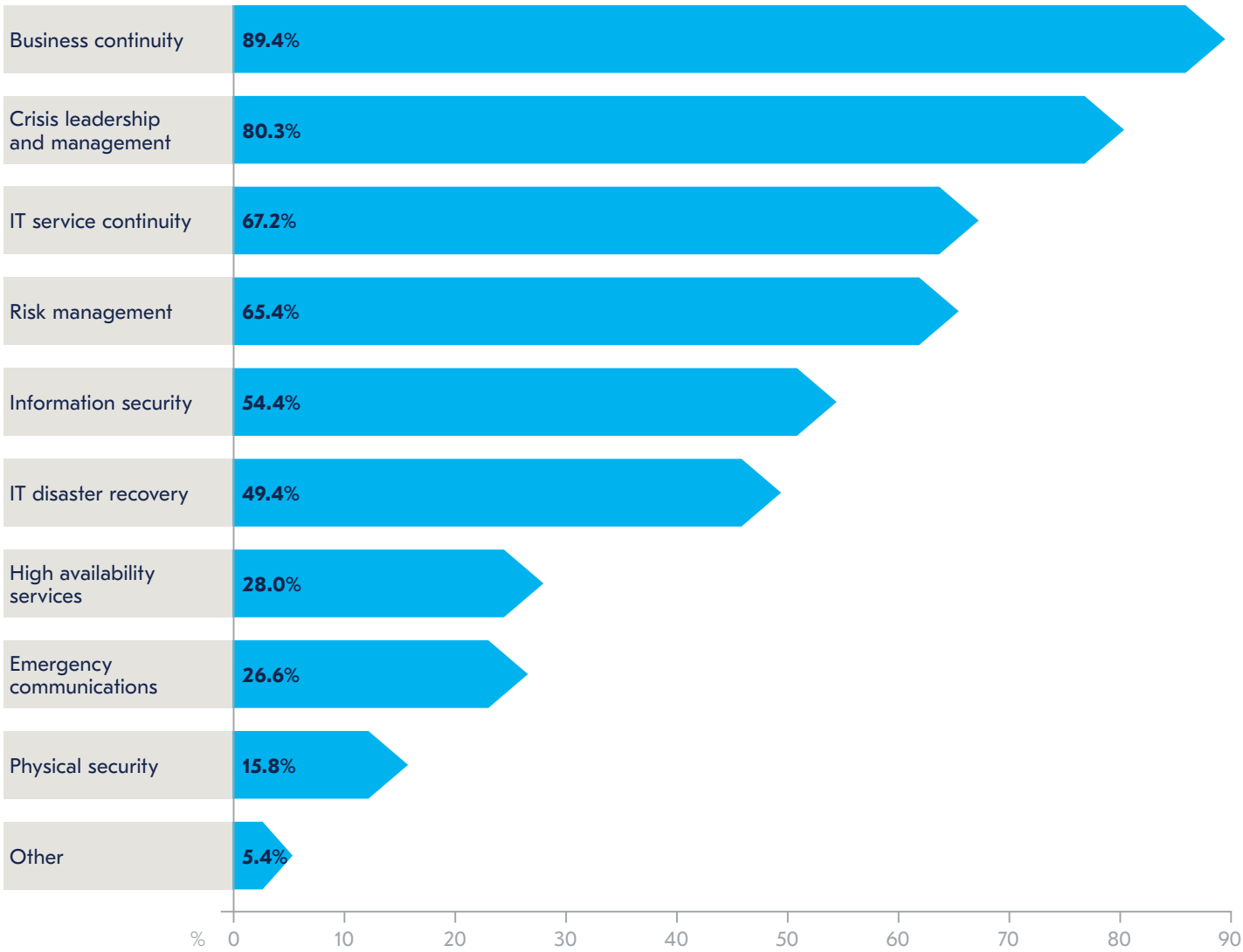


Figure 1. In your opinion, which of the below capabilities are important to the foundation of a resilient organization? Please rank your top five in order of importance

COVID-19 has demonstrated the benefits of non-siloed working, and the approach looks set to continue

Figure 2 exemplifies professionals' view of the importance of strong leadership. Nearly three-quarters (72.6%) consider strong leadership to be an organizational quality in terms of importance to their organization's resilience. Interestingly, it is robust, yet agile, operations which occupies the number two spot with 57.3% considering it to be a crucial organizational capability. The importance of agility has come to the fore during the pandemic: recent BCI research revealed that nearly two-thirds of professionals felt that planning processes should be reviewed during a prolonged incident such as a pandemic. Furthermore, over a quarter found that organizational priorities and practices changed during the pandemic, and Business Impact Analyses and risk assessments had to be improvised to ensure BC cover was provided for these new priorities during the crisis[4].

Effective communications and knowledge sharing ranks in third place, with just over half (53.7%) believing this to be a crucial organizational capability. This is a positive finding: prior to the pandemic, just 41.7% of organizations admitted to a planning process that involved all departments within their organization which led to a siloed and ineffective approach to planning; hardly an incubator for resilience[5]. Given the greater communication between departments as a direct result of COVID-19, nearly four in five professionals believe this increased collaboration will continue post-pandemic[6]. Indeed, in the interviews for this report, many reported how IT departments had been collaborating far more efficiently during the pandemic and were hopeful this would continue going forward.

> **"Many companies, particularly since COVID, have become so IT dependent. In our company and many others, there tends to be a separate process done for operational business continuity and IT business continuity. IT usually look after everything that means resilience to them (extra bandwidth, cloud solutions, etc.) and disaster recovery (DRP), but not enough on getting what's critical back up (i.e. BCP). They try to fix it, but they don't look at what's critical in the true sense of business continuity for their users. In BCP you're not trying to get everything working within 24 hours, you're trying to get what's critical back up and running. And I think more and more business continuity practitioners need to really get involved with IT and fill up those gaps that are there in IT resilience. Hopefully this will now start to happen."**
>
> Security Manager, Professional Services, France

4. BCI, The (2020). Coronavirus: A Pandemic Response. Available at: www.thebci.org/resource/bci-coronavirus---a-pandemic-response-2020.html (Accessed 29 September 2020).
5. Ibid
6. BCI, The (2020). The Future of Business Continuity and Resilience. Available at www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html (Accessed 29 September 2020).

What are the top three organizational qualities in terms of importance to your organization's resilience

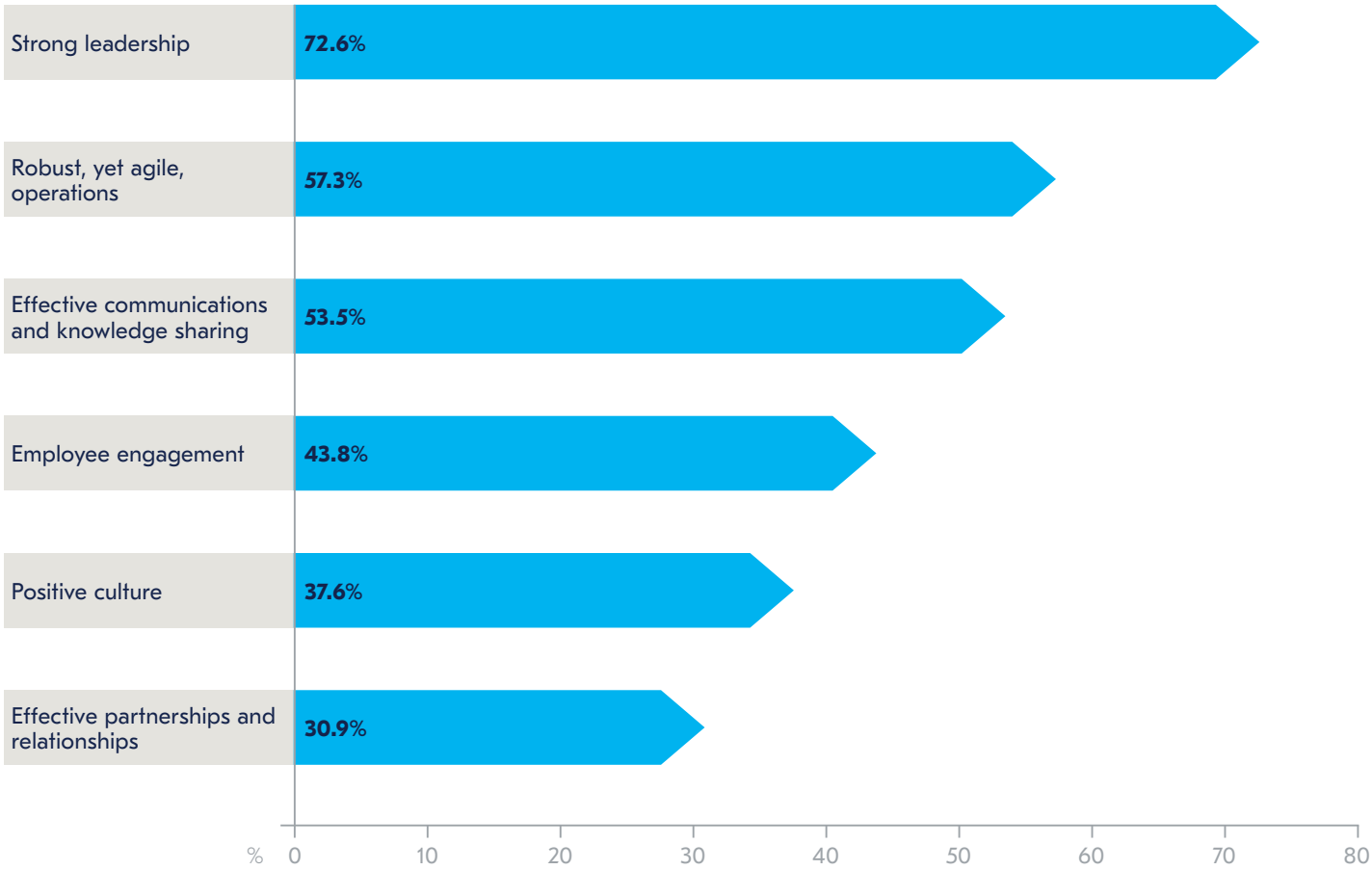


Figure 2. Please choose your top three organizational qualities in terms of importance to your organization's resilience

IT Resilience – where does it sit?

- **IT resilience is the responsibility of the IT department in two-thirds of organizations.**
- **The BIA for IT resilience is still more likely to be produced by Business Continuity than the IT department, and a third of respondents feel the responsibility for IT resilience should lie with Business Continuity**
- **Whichever department is ultimately responsible for IT resilience, professionals still feel there should be better communication between IT and Business Continuity.**

In two-thirds of organizations (64.4%) it is the IT department which governs IT continuity whilst Business Continuity were responsible in just 13.0% of organizations. In 6.0% of organizations, the Board/Executive team have responsibility for IT continuity, although this was principally within smaller organizations: the Board have IT responsibility in 21.1% of organizations employing under 250 people compared to 1.6% in organizations employing more than 5,000.

Although some organizations had a separate function dedicated to IT resilience which typically worked closely with Business Continuity, several respondents commented that their IT departments, particularly those without a dedicated IT Resilience function, tended to work in silos and failed to communicate their resilience strategies with the wider organization. Some IT departments, particularly within smaller organizations and public sector organizations, failed to have robust resilience strategies in place which resulted in multiple IT service continuity issues during the initial response phase as well as hardware shortages. Many of those who encountered such failures attributed this to a lack of communication between departments. Ultimately, this demonstrates that those organizations where IT and/or IT Resilience works closely with Business Continuity have more resilient infrastructures than those that practise a more siloed working culture. It also emphasises the importance of not just having resilience strategies in place, but also considering the scenarios feeding into those strategies.

Some organizations have structured IT departments so IT infrastructure, application management and liaison with the wider business is carefully managed so each department is in regular communication and have open channels for information exchange. Some IT Resilience specialists also report that they have entered their current position from a BC background (or vice versa) and their knowledge of the requirements of both departments ensure they are able to work seamlessly together.

> **"At the moment we have an infrastructure team which deals with anything and everything related to IT infrastructure: data centres, networking, communications - and vendors as well at the moment. The team I am in specifically looks at process governance where we look after change management, problem management, incident management, typical ITIL processes. We also have a separate IT division that looks at the application side of things. They are the "top layer" if you like and they liaise with the business. We work together well as two teams."**
>
> IT Risk Manager, Energy & Utilities, United Kingdom

> **"But in the larger organizations, the real question is how close are [DR and BC] tied together? A lot of times they're not. What's nice in our organization is a BC director used to do DR at other firms. So he's got some IT background. I have the same in BC so we were able to play off each other; our different skills, knowledges in the areas. It makes it a more effective partnership."**
>
> IT and Business Resiliency Director, Financial Services, United States

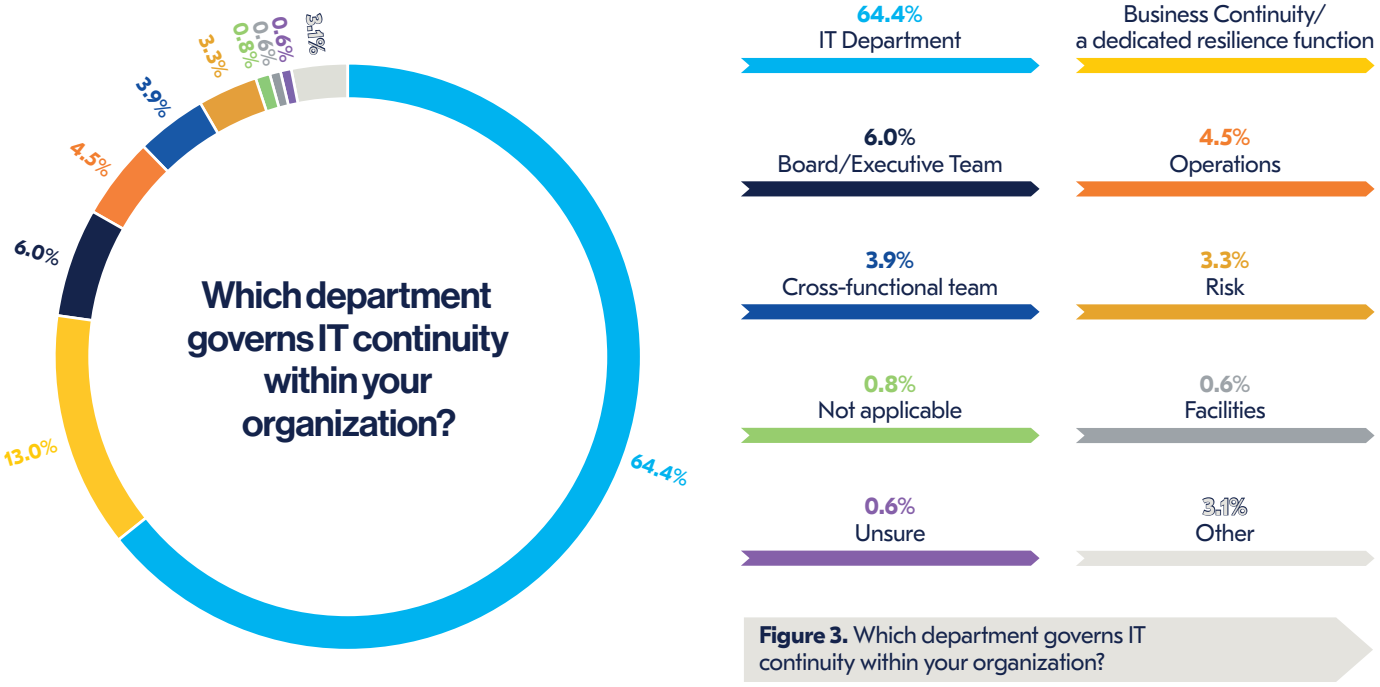


Figure 3. Which department governs IT continuity within your organization?

Because of the failures encountered during the COVID-19 pandemic, it is perhaps not surprising that there was a significant disconnect between the number of respondents who currently have IT governing IT resilience within their organization vs those who thought IT should govern IT resilience. Just over a third of respondents (34.1%) felt IT resilience should fall into the domain of Business Continuity, and under a third (32.8%) felt it should continue to be managed by the IT department. Demonstrative of an increased level of collaboration during COVID-19, 13.0% felt it should be managed by a cross-functional team — a method used by just 3.9% of organizations currently. 9.7% felt it should be the Board/Executive Team who should govern IT resilience, although this was primarily the case amongst those working for smaller organizations.

There was a commonality within the comments section to this question which highlighted the importance of the role of risk governance within an effective IT resilience strategy. One respondent commented that "a risk governance committee [can help] to ensure [the] level of IT continuity is suited to the risk as they do for business continuity". Another believed there should be "joint governance between IT and BC and escalation to risk governance if there is a disagreement". Whatever the ideal solution, these comments echo the importance of a collaborative solution to ensure that other parts of the organization — whether Risk, Business Continuity or the Board/Executive Team — have sight of IT Resilience plans and processes to ensure the same failures many organizations encountered during the pandemic are not repeated.

32.8% IT Department

34.1% Business Continuity/ a dedicated resilience function

9.7% Board/Executive Team

2.7% Operations

13.0% Cross-functional team

4.5% Risk

0.8% Not applicable

0.2% Unsure

2.3% Other

Figure 4. Which department do you feel should govern IT continuity within your organization?

Whilst the IT department governs IT resilience in most organizations, the production of the Business Impact Analysis (BIA) for technology resilience is still more likely to be compiled by Business Continuity than it is by the IT department. 38.2% of respondents reported that the technology resilience BIA is produced by the BC department vs 32.9% where it is produced by the IT department. In 6.2% of organizations, it is Risk which produces the technology resilience BIA — although this tends to be in smaller organizations where Business Continuity is the responsibility of Risk. A significant minority of organizations — 8.4% — report not having a BIA for technology resilience. For some organizations, this means IT is included within a larger, organization-wide BIA. For others, the presence of a IT service continuity-specific Gap Analysis serves as the primary tool to help define key applications and IT services, to assess whether products and services require adequate resiliency and to also offer prioritised recommendations to help rectify any gaps discovered.

38.2% Business Continuity/ a dedicated resilience function

32.9% IT

8.4% We do not have a BIA for technology resilience

6.2% Risk

3.3% Operations

3.1% Board/Executive Team

1.4% Unsure

0.4% Facilities

1.2% Not applicable

4.9% Other

Figure 5. Who is responsible for producing the Business Impact Analysis for technology resilience within your organization?

When respondents were asked about how IT continuity strategies and plans were conceived within their organizations, answers were split. Around a third (37.9%) said they were derived from the BIA, 28.9% were based on the needs of the business and only around a quarter (26.2%) by the IT department themselves. Many would argue that all three points refer to the needs of the business and are not mutually exclusive, but the different options emphasise the basis for the plans. Also, for some organizations, particularly those without a mature Business Continuity programme in place, the three options are standalone.

During a prolonged crisis such as a pandemic, the business priorities may change before the BIA has been updated to reflect the new working priorities, and an interim IT continuity plan may need to be rapidly conceived before a full BIA can be carried out. It would be best practice to include the IT department, Business Continuity and Senior Management within these discussions to ensure the priorities align to any new strategic considerations. The other consideration in made by respondents within the question was cost, particularly at this current time due to the financial constraints on businesses because of the pandemic.

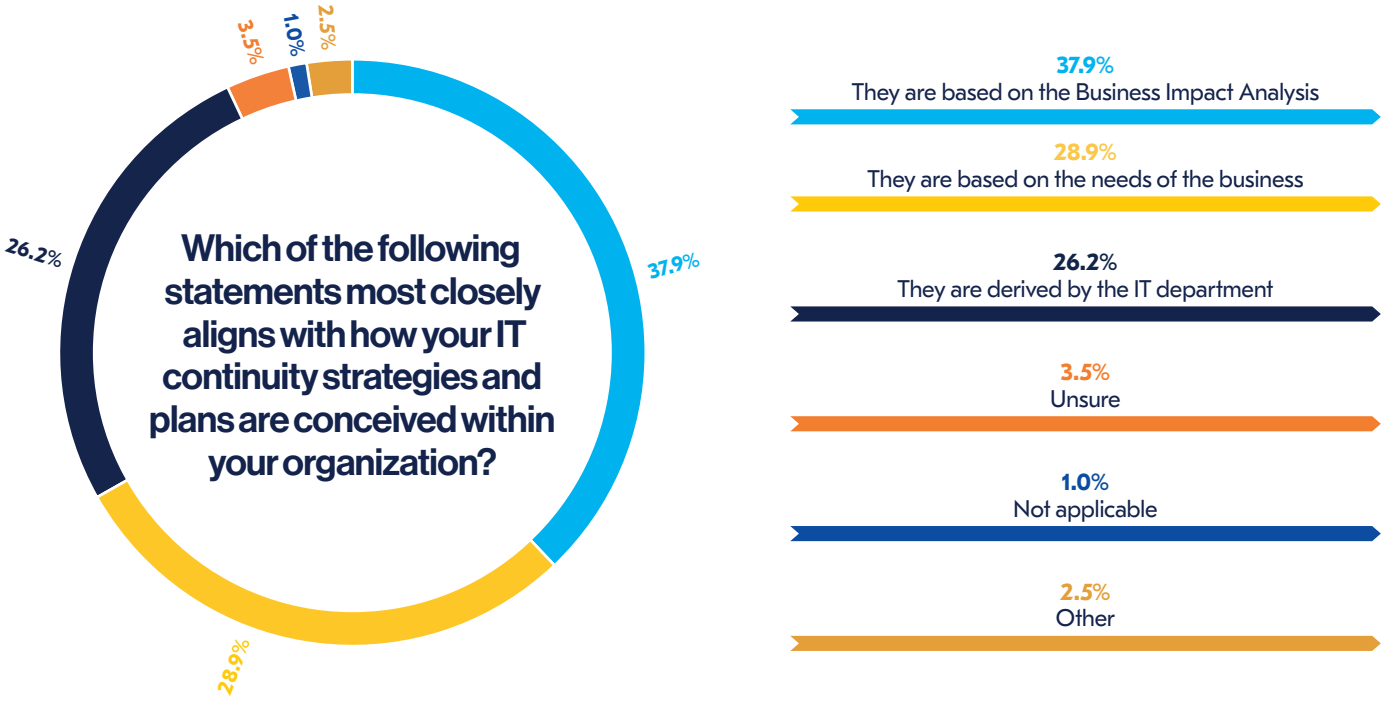


Figure 6. Which of the following statements most closely aligns with how your IT continuity strategies and plans are conceived within your organization?

Should there be a separate Good Practice Guidelines (GPG) for IT resilience?

- **87.4% of professionals believe that more detail on IT resilience is needed within the GPG or in a separate GPG.**
- **Under a third (31.1%) would value the creation of a separate GPG: most feel a separate publication would create further walls between BC and IT.**
- **Even without separate guidelines, most felt more detail would be a welcome addition to the guide, whether through a new chapter or through additions in current chapters.**

Several BCI members felt that it might be timely to introduce a separate GPG for IT Resilience. Those in favour of its introduction believed such a guide was necessary due to the specialist detail required within an effective IT resilience strategy, and also because IT continuity strategies should be based on current technologies and would therefore need to be updated more regularly than the GPG. Some felt it was a necessary guide for IT resilience professionals who come from a technical background and have more limited experience of the "People, Processes, Premises" concept. Interviewees commented that such individuals tend to naturally veer towards the technical aspects of resilience rather than the wider aspects of resilience when considering an IT strategy.

However, the survey shows that most professionals are not in favour of introducing a separate GPG: under a third (31.1%) thought a separate GPG for IT Resilience should be conceived. Many believed a new GPG was unnecessary as ITIL IT Service Continuity coupled with the ISO 27031 guidance standard (ICT Readiness for Business Continuity) already served the purpose. Others raised concerns that a separate GPG, particularly if the IT Resilience GPG was aimed at IT professionals, would lead to addition siloing of processes between the Business Continuity and IT departments.

"IT resilience should not be separate - that defeats the whole purpose of the concept of resilience."

Anonymous Survey Respondent

"IT should not have a separate GPG; a siloed approach is unlikely to be effective. The business also needs to realise and appreciate this. IT is no longer just a service organization, IT and business are partners. When a crisis happens, it is even more important to work together to make informed decisions. I think the best way to approach it is to have a new section in the GPG to actually include all dependent IT components for critical processes as a part of a structured breakdown. Organizations need to have business and IT people together working on this."

IT Continuity Services Manager,
Higher Education, Australia

An interviewee was concerned that having a separate GPG for IT Resilience would encourage further separation between the IT department and the Business Continuity department; something he had worked hard to stop happening within his own organization.

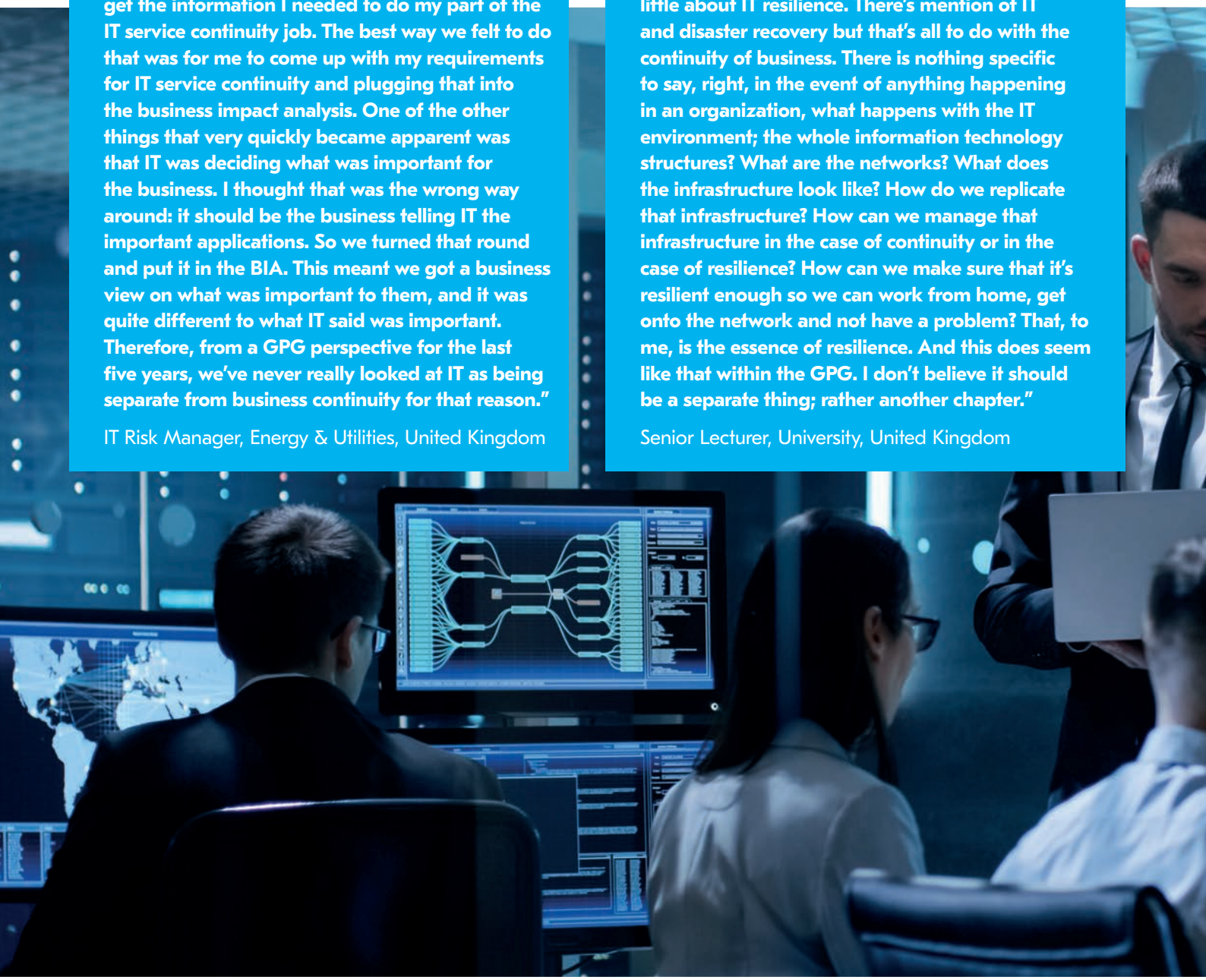
A far greater proportion (56.3%) of respondents, however, thought that the GPG should be modified to contain more detail about IT resilience. Many felt the importance of technology during the recent pandemic had demonstrated the importance of requiring more detail on IT resilience. Others believed that specific areas of IT resilience, such as IT Recovery, are not covered in enough depth in the current GPG.

"One of the things I felt quite strongly about when I joined was working with Business Continuity to get the information I needed to do my part of the IT service continuity job. The best way we felt to do that was for me to come up with my requirements for IT service continuity and plugging that into the business impact analysis. One of the other things that very quickly became apparent was that IT was deciding what was important for the business. I thought that was the wrong way around: it should be the business telling IT the important applications. So we turned that round and put it in the BIA. This meant we got a business view on what was important to them, and it was quite different to what IT said was important. Therefore, from a GPG perspective for the last five years, we've never really looked at IT as being separate from business continuity for that reason."

IT Risk Manager, Energy & Utilities, United Kingdom

"I measure the maturity levels within an organization based on the GPG. There's very little about IT resilience. There's mention of IT and disaster recovery but that's all to do with the continuity of business. There is nothing specific to say, right, in the event of anything happening in an organization, what happens with the IT environment; the whole information technology structures? What are the networks? What does the infrastructure look like? How do we replicate that infrastructure? How can we manage that infrastructure in the case of continuity or in the case of resilience? How can we make sure that it's resilient enough so we can work from home, get onto the network and not have a problem? That, to me, is the essence of resilience. And this does seem like that within the GPG. I don't believe it should be a separate thing; rather another chapter."

Senior Lecturer, University, United Kingdom



Some organizations felt there was a very defined need for more information to be contained in the current GPG as there are now a number of people who work within IT resilience who have not come into the job from an IT-related discipline. Interviewees reported some make fairly basic errors when considering aspects of IT resilience, and a new document and/or more detail in the current GPG would help to plug this information gap.

A significant minority, 7.8% of respondents, believe that there is already sufficient detail within the GPG and no updates were required. They felt the current GPG contained sufficient guidelines for implementing business continuity within IT, and the technical components of IT resilience were better addressed by IT resilience experts.

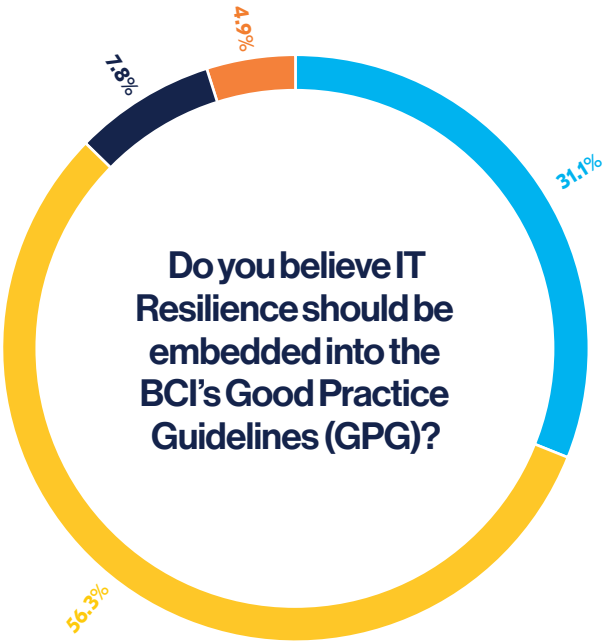
"I think it makes sense to have a very focused IT service continuity-type document. There are people who have my role that have not come up through an IT line and therefore need to understand a bit more about IT resilience; they need to understand what to ask for. One of the things that you regularly hear is 'we're very resilient because we're on cloud.' That, of course, doesn't make you resilient because it depends on how you've configured cloud. Have you tested your fail backs? Have you tested the strategy that you have implemented? So, I genuinely think we need to make sure that the business side of business continuity has an understanding of IT so that they can ask the right questions to challenge having the wool pulled over their eyes."

Business Continuity Manager, Financial Services, United Kingdom

"The GPG is light on details about IT resilience. This is a highly specialised area, and I would not recommend a non-IT specialist taking control of this area. As an IT resilience specialist, I sit within the IT dept not resilience. It is impossible to keep up with technological change and organizational developments within this department, as things change almost daily."

Anonymous Survey Respondent

Whilst it is unlikely that a separate IT Resilience GPG will be produced within the near future, it is clear that many would welcome greater detail on IT resilience within the GPG. A starting point could be better alignment of the GPG and ITIL ITSCM and also considering strategies on how the two departments could work better together.



31.1%
I believe there should be a separate GPG for IT Resilience

56.3%
I believe the GPG should be modified to contain more detail on IT resilience

7.8%
I do not believe it should be included as there is currently enough detail in the current GPG

4.9%
Unsure

Figure 7. Do you believe IT Resilience should be embedded into the BCI's Good Practice Guidelines (GPG)?

Communication failures are causing breakdown in resilience processes

- A fifth of professionals are not confident that Business Critical Activities could be continued or restarted in line with their Business Continuity Plan (BCP).
- One in ten organizations have not mapped critical applications or infrastructure.
- The primary reason for failure was due to lack of communication between departments, and confusion about who is responsible for processes.
- Old, legacy technology is an issue for many organizations as they cannot upgrade systems to reflect the contemporary requirements of the organization.

When it comes to confidence with organizations' own business continuity processes and procedures, a mixed picture has emerged. Whilst three-quarters (73.2%) of respondents were either "very confident" or "confident" that Business Critical Activities could be continued/restarted in line with their Business Continuity Plan (BCP), but a concerning minority of 21.2% of professionals were "fairly unconfident" or "very unconfident" with this statement. When it came to mapping critical applications and infrastructure, there was a slightly more positive picture: 28.0% of organizations reported that mapping had been carried out for all systems, and a further 55.5% for critical systems only. Just under one in ten respondents (8.8%) said that no mapping had been carried out at all.

When interviewing respondents, many felt that a lack communication between departments, typically between IT and other departments within an organization, was the primary reason for the lack of confidence.

Other organizations admitted that plans had not been updated for several years which meant gaps had formed, particularly from a support perspective.

> **"The DR that we have was set up several years ago. There's been some additions to it, but it's never been fully updated and this is what we are going through now. We're in the process of mapping the applications to the critical business processes. So I expect to find gaps where some supporting applications are not in DR. That is the reason I'm currently unconfident, but in six months' time we will fully know our requirements and be in position to resolve."**
>
> IT and Business Resiliency Director, Financial Services, United States

In contrast, some found that regular communication with other parts of the business helped to ensure business critical activities could be continued or restarted in line with their BCP. One interviewee explained that by asking departments to identify what their critical applications are, they ensured that the infrastructure was there to support each application. Although a straightforward operation in itself, it does rely on good communication processes between the IT department, business continuity and the wider business — something which many organizations still struggle to implement effectively. From a business perspective, it also requires departments to be realistic about criticality. This requires strong governance to achieve realistic requirements and priorities regarding IT spend.

"In order to get the information we need, we ask the business to tell us what their applications are. We are getting that information straight away; as soon as a new application is needed. Because we're the infrastructure team who look after the boxes and cables etc, we know how it all connects together. We therefore have the confidence that what we've got works. And because we've tested it, we've proven that it does."

IT Risk Manager, Energy & Utilities, United Kingdom

In fact, it is the line of communication between the IT department and the BC department which is cited as the frequent cause of failure. Larger organizations tend to have more practised processes and procedures in place, and often even have the presence of a separate IT resilience function. However, some organizations operating across multiple sites, particularly those within a public sector or educational environment, have adopted a centralized approach to IT which can lead to siloing of information and processes. Ultimately, this can result in the needs and requirements of individual sites or departments — including the identification of critical applications — being not fully addressed.

"The problem is that we have two campuses that are a long way apart; one is a long way out of town. If somebody has an IT problem there, they're going to wait a day or two before it's rectified. I think from a business continuity perspective, they should decentralize the IT department so it is available on different sites. Centralization can work from a process perspective, but we are not sure what's going on in the department most of the time."

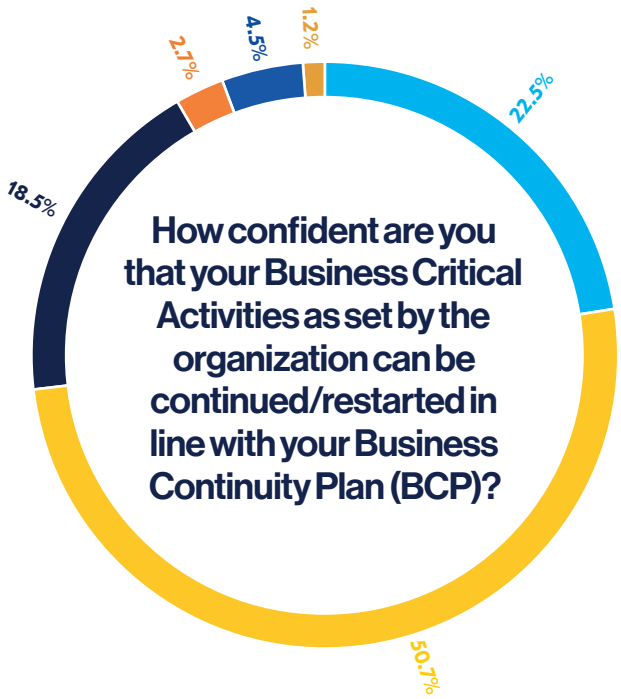
Senior Lecturer, University, United Kingdom

A further issue frequently encountered when trying to build resilient systems is the constraints driven by legacy systems. In the BCI's *Disruptive Technologies Report 2019*, more than half of survey respondents (51.2%) cited the existence of outdated, legacy systems as a primary reason for technology not being upgraded[7]. The resulting reliance on older systems is therefore likely to impact not just on an organization's ability to restart Business Critical Activities in line with the BCP, but also carrying out the mapping processes in the first place.

"I think it's typical of a lot of universities. Lots of them have grown out of quite dated IT systems and there's never been the investment to bring in new technologies. It's difficult to embrace the new world whilst some of the IT systems and legacy systems like JANET still exist within universities. It creates a lot of problems. Whereas a big organization can just scrap everything and buy in a whole new system, it's difficult to do that in a university."

Senior Lecturer, University, United Kingdom

7. BCI, The (2019). Disruptive Technologies. Available at www.thebci.org/resource/bci-disruptive-technologies-report-2019.html (Accessed 29 September 2020).



22.5%
Very confident

50.7%
Confident

18.5%
Fairly unconfident

2.7%
Very unconfident

4.5%
Unsure

1.2%
Not applicable

Figure 8. How confident are you that your Business Critical Activities as set by the organization can be continued/ restarted in line with your Business Continuity Plan (BCP)?

28.0%
Yes, for all systems

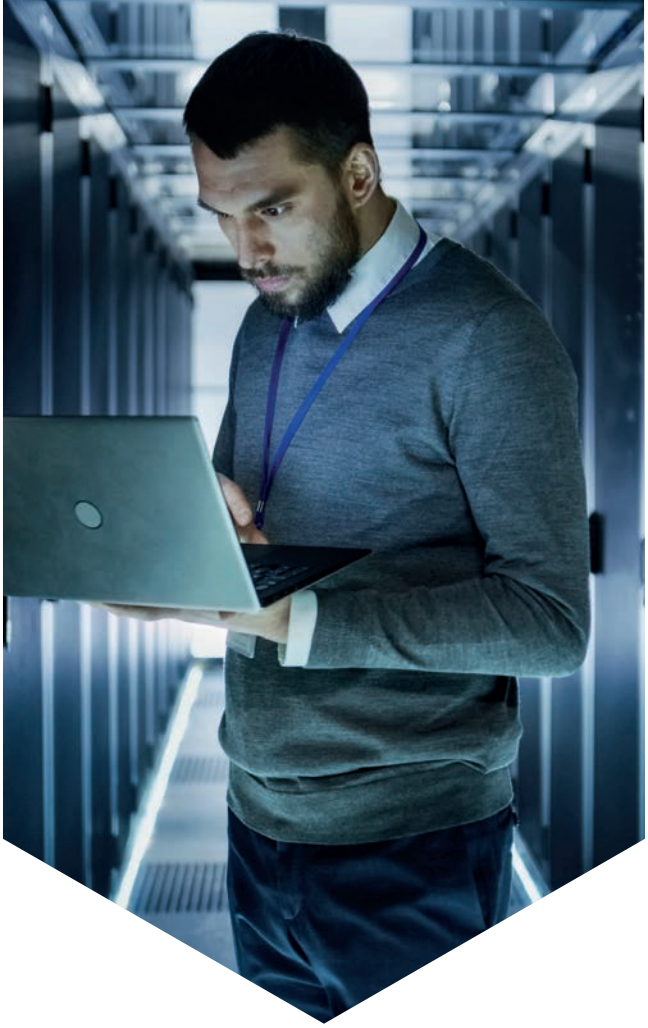
55.5%
Yes, for critical systems only

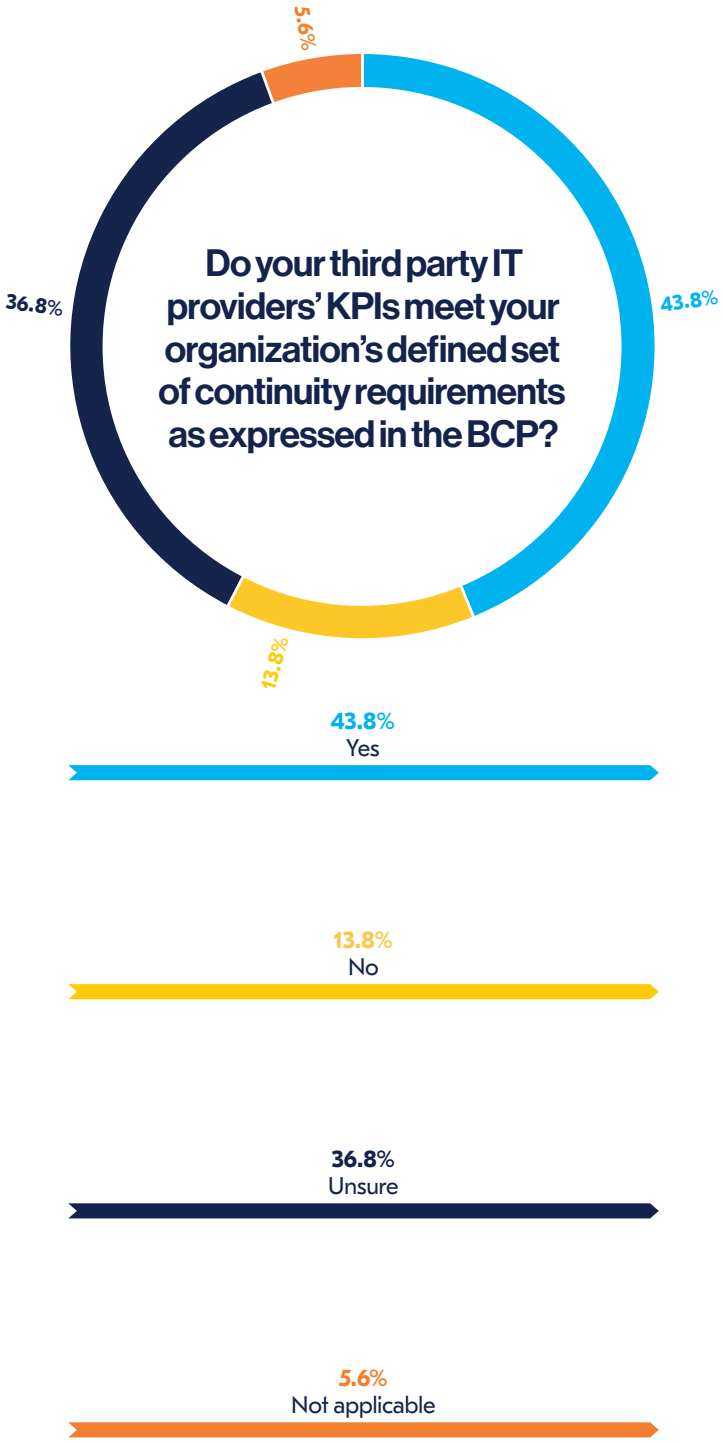
8.8%
No

6.8%
Unsure

1.0%
Not applicable

Figure 9. Has your organization mapped out the critical applications and infrastructure that support business critical activities as identified in the BCP?





The annual BCI *Supply Chain Resilience report* emphasises the importance of carrying out thorough due diligence on suppliers. The 2019 report revealed that whilst just under two-thirds of organizations (64.0%) check for the presence of a Business Continuity Plan from their critical suppliers, only a third (35.5%) actually seek details of the whole BCM programme, and not just the plan[8]. Doing the due diligence on a supplier's BCP at procurement stage would not only be advisable, but it could help to prevent an unexpected — and perhaps catastrophic — failure of a supplier once they have been engaged.

The same level of due diligence should be carried out when it comes to third party IT providers. With so many organizations becoming reliant on cloud-based services and remote hosting, ensuring an IT provider's KPIs meet your organization's defined set of continuity requirements (as expressed in the Business Continuity Plan) is crucial to prevent unnecessary downtime and unwarranted system failures. However, less than half (43.8%) of respondents claim their IT providers' KPIs meet their organization's continuity requirements, with 13.8% admitting they do not. Over a third (36.8%) of respondents say they are unsure. Interestingly, the majority of those who were "unsure" were Business Continuity professionals, and those working directly within IT Resilience or IT Risk were more likely to know. This in itself serves as an example of how business critical knowledge can be easily siloed if clear pathways for information exchange are not created.

Figure 10. Do your third party IT providers' KPIs meet your organization's defined set of continuity requirements as expressed in the BCP?

8. BCI, The (2019). Supply Chain Resilience. Available at www.thebci.org/resource/bci-supply-chain-resilience-report-2019.html (Accessed 29 September 2020).

Resilience Planning and Risk Management

The ownership of technology risk resides with the IT department

- The ownership of IT risk resides with the IT department or the IT Resilience department in over two thirds (69.1%) of organizations.
- Nearly one in five IT departments, however, fail to share technology risks with the wider organization.
- Business Continuity manages technology risk in 14.9% of organizations, but typically have a BC Manager with a background in IT/technology who can understand the technology risk landscape.

The previous section showed examples of organizations siloing crucial information for IT resilience purposes, either by the IT department or by the Business Continuity department. Although normally unintentional, barriers can easily form if the issue is not addressed.

When it comes to IT Risk, it is the IT department or a specialist IT Resilience department which commonly takes ownership of technology risks. In over half of organizations (55.4%), the IT/IT Resilience department follows good practice and shares the risks with the wider organization as part of the wider risk profile. However, not all IT departments are as diligent with their information sharing processes: 13.7% of respondents report the IT department takes ownership but does not share the risks with the wider organization. Although some IT professionals argue that they should take control of the IT Risks owing to the "technical" nature of them, such an approach could lead to some risks not being included correctly or being poorly represented within the wider risk profile.

In 14.9% of organizations, it is the BC department or another resilience function which takes ownership; working closely with the IT department to ensure they have the necessary plans in place to remediate from an operational perspective. Many organizations who adopt this process frequently report having a Business Continuity Manager in situ who has a technology-related background and is able to work very effectively and efficiently with the department.

8.1% of organizations have a separate department to manage all risks. For larger organizations, this is typically a Risk Department. For smaller organizations, it is typically the Executive Team who take ownership of risks.

55.4%
The IT department takes ownership but shares with the wider organization to be part of the wider risk profile

14.9%
Business continuity or another resilience function takes ownership and works closely with the IT department to ensure they have the necessary plans in place to remediate from an operational perspective.

13.7%
The IT department takes ownership but does not share with the organization to be part of the wider risk profile

8.1%
Another department manages all risks including technology

1.1%
We do not consider technology risks within our BC risk profile.

3.4%
Unsure

0.9%
Not applicable

2.6%
Other

Figure 11. Who in your organization is responsible for technology risks?

The prioritization of components of the BCP is dependent on the department creating it

- IT professionals prioritise the resilience of infrastructure when creating the BCP, whereas BC professionals prioritise the resilience of applications.
- Data storage is given the least priority by both IT and BC professionals when considering resilience.
- There are still organizations who "presume" data is secure when hosted in the cloud and fail to interrogate the KPIs or performance history of storage providers.

When it comes to creating a Business Continuity Plan, 88.4% give the resilience of business applications "a high degree" or "some degree" of consideration. However, just 60.1% of respondents give the resilience of IT infrastructure the same level of consideration.

Interestingly however, the consideration varies according to the functional role of respondents: for those who have a role within IT Disaster Recovery, Cyber Security or IT Service Continuity, some 78.1% believe infrastructure should be given a high degree of priority, compared to 60.1% of Business Continuity professionals. This in itself is indicative of the roles and responsibilities of those within different job functions and suggests that BC have more responsibility in ensuring the IT applications used by the business are resilient, whereas those within IT Disaster Recovery (DR) or IT Service Continuity (SC) have a greater responsibility in ensuring the resilience of the IT infrastructure.

Business data storage is the least considered aspect in a Business Continuity Plan when it comes to considering resilience. 15.0% of respondents give the resilience of data storage "little" or "no" consideration when building the Business Continuity Plan, whilst just 54.2% give it "high" consideration. For IT DR/IT SR professionals, the figure is even lower with just 51.6% believing it to be a high priority. As highlighted in the previous question, with so many organizations now becoming reliant on the cloud, it would be good practice to ensure the resilience of third party data storage providers; interrogating any published KPIs and ensuring a suitable backup is available.

When creating the BCP, to what extent do you consider the resilience of the following underlying IT components?

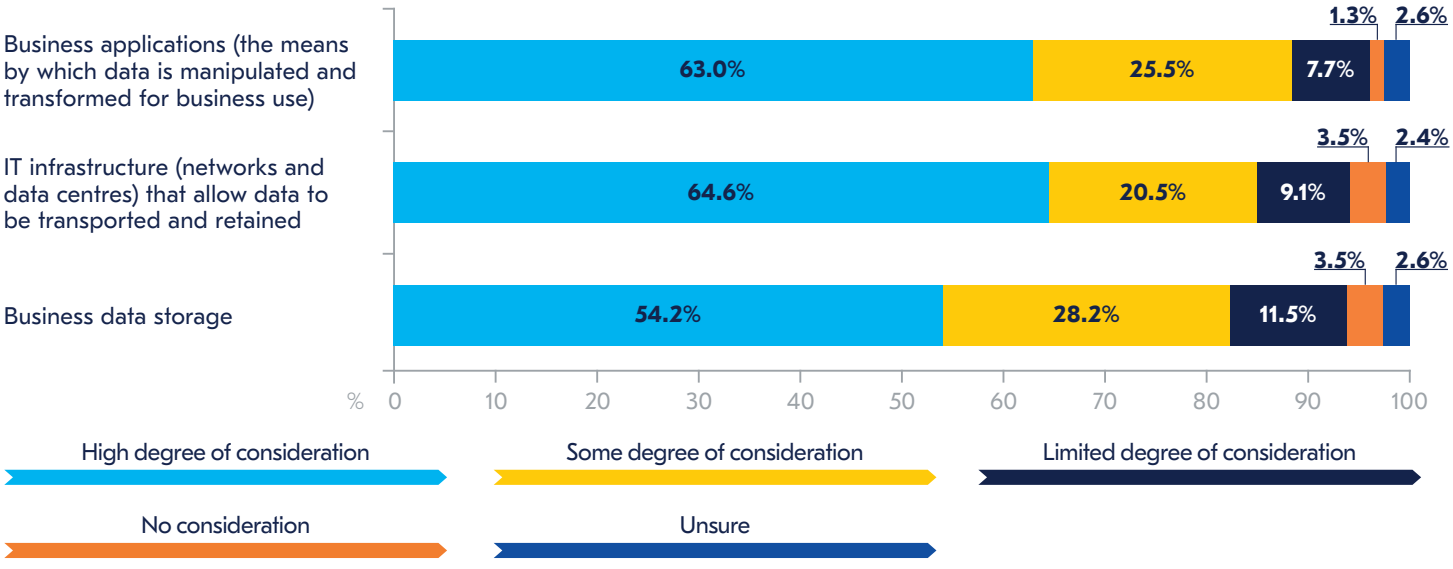


Figure 12. When creating the BCP, to what extent do you consider the resilience of the following underlying IT components?

Many organizations do not have up-to-date Disaster Recovery procedures, but most perform regular testing

- A fifth of organizations do not have their Disaster Recovery procedures up to date.
- Three-quarters of organizations perform DR tests once a year or more, with many carrying out extra testing in the early months of the pandemic.
- Just 17.8% of organizations carry out full DR tests, with 43.6% just performing tests on critical systems and subsets.
- The impact on production services and the risk on impact to the business were the primary reasons for organizations not carrying out full testing.

Perhaps of more concern than a lack of priority given to data storage is the significant minority of organizations who admit to not having their Disaster Recovery procedures up to date. Whilst nearly two-thirds of respondents (62.8%) report that procedures are up to date, nearly a fifth (18.6%) answered that procedures were not up to date. A further 17.3% were "unsure" whether procedures were up to date: a further demonstration that Business Continuity and IT DR still work autonomously within some organizations. Having an up-to-date Disaster Recovery plan is crucial to stop unwarranted downtime. IDC recently estimated the cost of an infrastructure failure to be $100,000 per hour for a large organization, with critical failures leading to even higher costs of up to £1m per hour[9]. Given around 35% of failures take around 12 hours to rectify, it is easy to see how the costs can mount up.

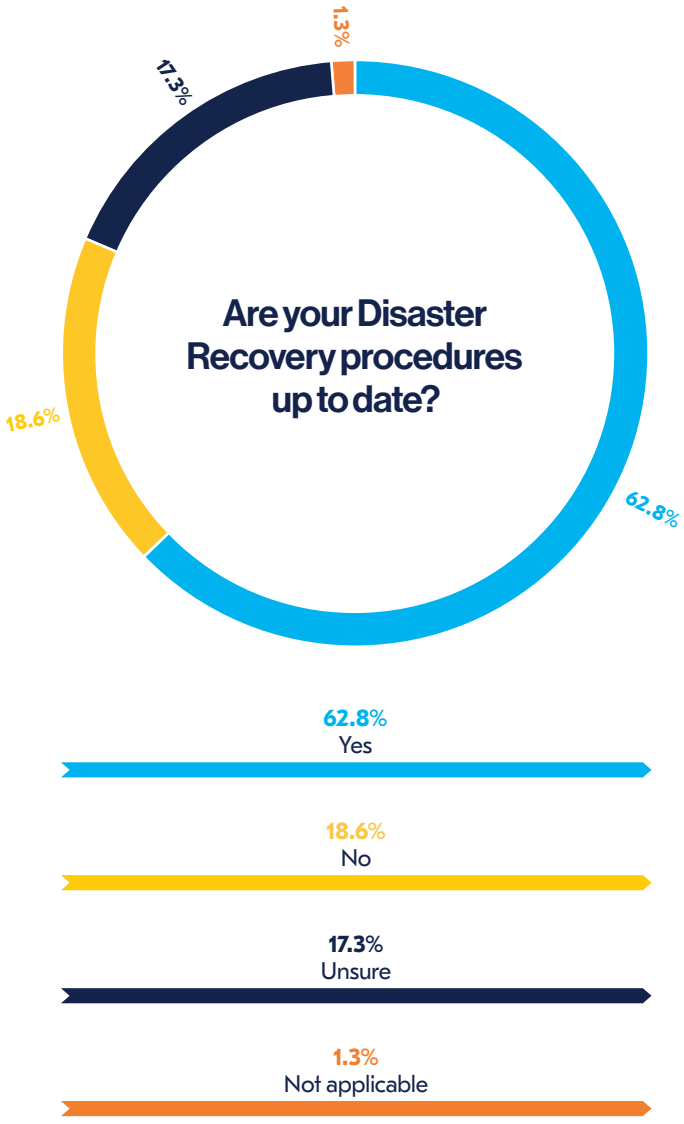


Figure 13. Are your Disaster Recovery procedures up to date?

9. Elliot, S (2014). 'DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified'. IDC (December 2014). Available at kapost-files-prod.s3.amazonaws.com/published/54ef73ef2592468e25000438/idc-devops-and-the-cost-of-downtime-fortune-1000-best-practice-metrics-quantified.pdf (Accessed 29 September 2020)

Testing is the primary method of ensuring disaster recovery processes and procedures work in practice, and regular testing should be carried out as a matter of course. Although there are no firm guidelines on how often testing should take place, it is generally considered good practice to carry out a full disaster recovery test at least once a year . Given that 65% of organizations fail their own disaster recovery tests, it is clear to see why testing is so important .

On the basis of the survey, it appears that most organizations are following good practice and performing regular DR tests: over a quarter of organizations (28.2%) test disaster recovery procedures more than once a year, with a further 43.1% testing once a year. A further quarter (24.1%) admit to performing testing, but it is not done to a regular schedule. Although some of these respondents may be testing more frequently than annually (some noted that extra testing was performed in the first few weeks of the COVID-19 outbreak), there are likely to be some organizations included with this quarter who are not performing sufficient testing. Furthermore, a far from insignificant 4.5% claim to "never" perform any kind of disaster recovery testing. Although the majority of these are from micro-sized businesses employing 10 staff or less, ensuring systems can be recovered effectively is still vital: losing important electronic documents are stored data could be even more catastrophic for a small business with no back-up plans in place.

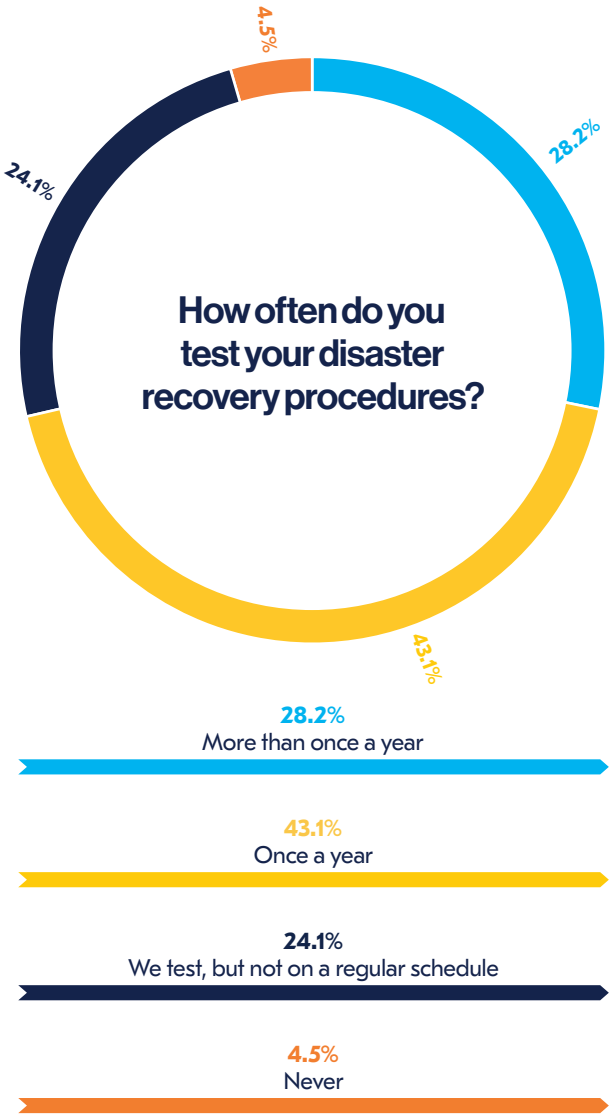


Figure 14. How often do you test your disaster recovery procedures?

10. Bowker, D (2016). 'Testing your disaster recovery plans: A best practice guide'. CloudTech (2 November 2016). Available at: cloudcomputing-news.net/news/2016/nov/02/testing-your-disaster-recovery-plans-best-practice-guide (Accessed 29 September 2020)
11. Disaster Recovery Council (2014). 'Disaster Recovery Preparedness Benchmark Survey'. Disaster Recovery Council (2014). Available at: www.unitrends.com/wp-content/uploads/ANNUAL_REPORT-DRPBenchmark_Survey_Results_2014_report.pdf (Accessed 29 September 2020)

Although many organizations are following good practice and performing a full DR test once a year, the number of organizations that do this in reality is far less. Less than one in five organizations (17.8%) claim to perform a full DR test, with the bulk of respondents (43.6%) admitting to performing DR tests on critical business applications and system subsets. Some organizations are mandated to do full disaster recovery tests due to regulatory demands: this is often the case for financial services organizations, for example. However, taking this into account, there are clearly few organizations outside unregulated industries which feel they have the capability to perform full DR tests.

"Given the interconnected nature of IT services, applications and infrastructure; performing subset testing will most likely not enable successful recovery from a disaster. Equally, performing testing on one subset may not lead to the recovery capability of a different subset."

David Morgan
Head of EMEA Consulting
Sungard Availability Services

"We have a global network and in some countries operate as a banking institution. We are regulated and some country regulators require us to have a full disaster recovery test once or even twice a year. In those countries, we conduct a full test. We switch off everything and switch on everything, we work with people and combine it with business resumption and disaster recovery testing. The first time you do it, you do tend to encounter issues, but that's the point of it. You just find the problems and improve them. We make sure all teams are aware of the schedule in a calendar maintained by our team."

Director of Information Security and Business Continuity, Financial Services, Georgia

However, the same interviewee admitted that an issue with regulation-driven DR testing was that regulators were slow to adopt new scenarios into their own processes. For many organizations, they are obliged to meet current requirements of merely switching systems off and on again. The interviewee said that the issues encountered in a long-lived disaster such as a pandemic required new scenarios to be tested and was concerned that such scenarios would take too long to filter through as new guidance.

"Regulators should look to adopt new scenarios as well. Our scenarios do not deviate much from current scenarios like switching on, switching off. The standard disaster recovery test. Disaster data centre recovery is probably not the most relevant scenario for a pandemic and for the new normal. There are new models, new scenarios which should be taken into account. Relocating staff from one office to another office was standard prior to coronavirus whereas the new normal involves sending people to work from home and other remote location, isolated from each other. Nany types of testing are now no longer relevant. The new normal will bring new scenarios and we will adapt accordingly. Hopefully the regulators will too."

Director of Information Security and Business Continuity, Financial Services, Georgia

For a small subset of organizations (1.9%), DR testing is only carried out on non-critical business applications and services and 9.2% claimed never to have completed a full DR test in a production environment. Most of these responses originated from organizations who reported they were unable to take critical systems out due to systems being required to be up "at all times".

"I strongly suspect if I asked to do [a full DR test], I would not get support from my senior management team, first and foremost, because it's just too operationally invasive."

Head of IT & Resilience, Public Sector, United Kingdom

There would be few who would argue this was not a risky strategy to adopt, and such organizations would be advised to seek advice on how effective testing could be carried out with minimal business disruption. Some organizations such as those with links to the trading market are more restricted on when testing can be carried out, but many of those reported in interviews that they are still able to carry out full testing; albeit often in "slices". These are characteristically organizations where Management have bought in to the importance of testing and encourage testing to be carried out.

"We use the four different levels from ITIL to categorise our testing. We have 'mission critical' as the most severe one. Most of those are in the primary part of the organization; the trading part. A lot of them are connected to market traders. We therefore know we can't always test everything on there because trading happens 24/7 all around the world. We therefore test what we can. In terms of infrastructure testing, we have enough redundancy in network links and equipment that when we did the testing earlier this year with third parties we didn't experience many problems. The business tends to be fairly supportive of testing activities because they get a benefit from it. If we have unplanned outages, they see that we can get things up and running and the impacts are negligible, so they're supportive of doing these things."

IT Risk Manager, Energy & Utilities, United Kingdom

"We have not got a virtual DR environment. We therefore have to do our DR tests in a live production environment. That means we can't do the full fail over testing because it just takes too long as a global company. For example, we have Saudi Arabia and Dubai working on a Sunday so even if we started at a pre-agreed time on a Friday, once the US and San Francisco and Canada are finished, it's a very small window to try and do a full end-to-end DR test. Therefore, what we've done is we've taken very specific slices, and we've done DR testing of those slices of that value chain but not a full one. This in itself does cause problems because it doesn't help expose all the gaps and assumptions are still in place. However, it is the best we can do for now."

Business Continuity Manager, Financial Services, United Kingdom

"In university environments, even though we're not doing anything mission-critical like life depends on it, we do always have everything on. This is because the students, the study and the research continue 24/7, even though we're not geared to support 24/7. So, processes and systems have been built to continue 24/7 even without our intervention. So, if we are to stop systems for DR testing, it is going to impact the business. We, therefore, need to plan our testing carefully. We include at least one or two weekends into the university's maintenance calendar for DR testing when disruption will be minimal. But when we get to that point, there are a lot of objections and some schools say they cannot have systems out. So far we have managed to perform regular DR testing exercises, but it is becoming more difficult."

IT Continuity Services Manager, Higher Education, Australia

12.7% of organizations reported doing partial testing, but said they were limited in their ability to do a full disaster recovery test. For those who were restricted in being able to perform a full DR test, more than half (52.4%) said it was due to the impact on production services and a similar percentage (51.1%) said it was due to the risk of impact on the business. Over a third (38.7%) said the availability of technology resources to be able to perform a full test was a factor.

One in five organizations (21.6%) said their inability to perform full testing was down to a lack of suitable plans or run books, and a further 18.7% said it was due to financial constraints. Such responses are indicative of a lack of dedicated resource to be able to formulate plans or author a set of defined procedures to ensure testing can take place. Recent research by the BCI shows that approaching the board for additional resource now could be advantageous: the BCI's *Future of Business Continuity and Resilience report* showed that 40.7% of professionals were confident of getting additional financial and/or resource support as a direct result of COVID-19 as Management have been showcased the importance of resilience in traversing a crisis with the longevity of the current pandemic[12].

Interviews with respondents further highlighted a lack of support from the business being a primary inhibitor to allowing all systems to be tested. Although some respondents realised this was an issue, the majority felt that they were still able to perform sufficient testing through a targeted testing programme covering each aspect of the IT infrastructure, albeit not at the same time.

12. BCI, The (2020). The Future of Business Continuity and Resilience. Available at www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html (Accessed 29 September 2020).

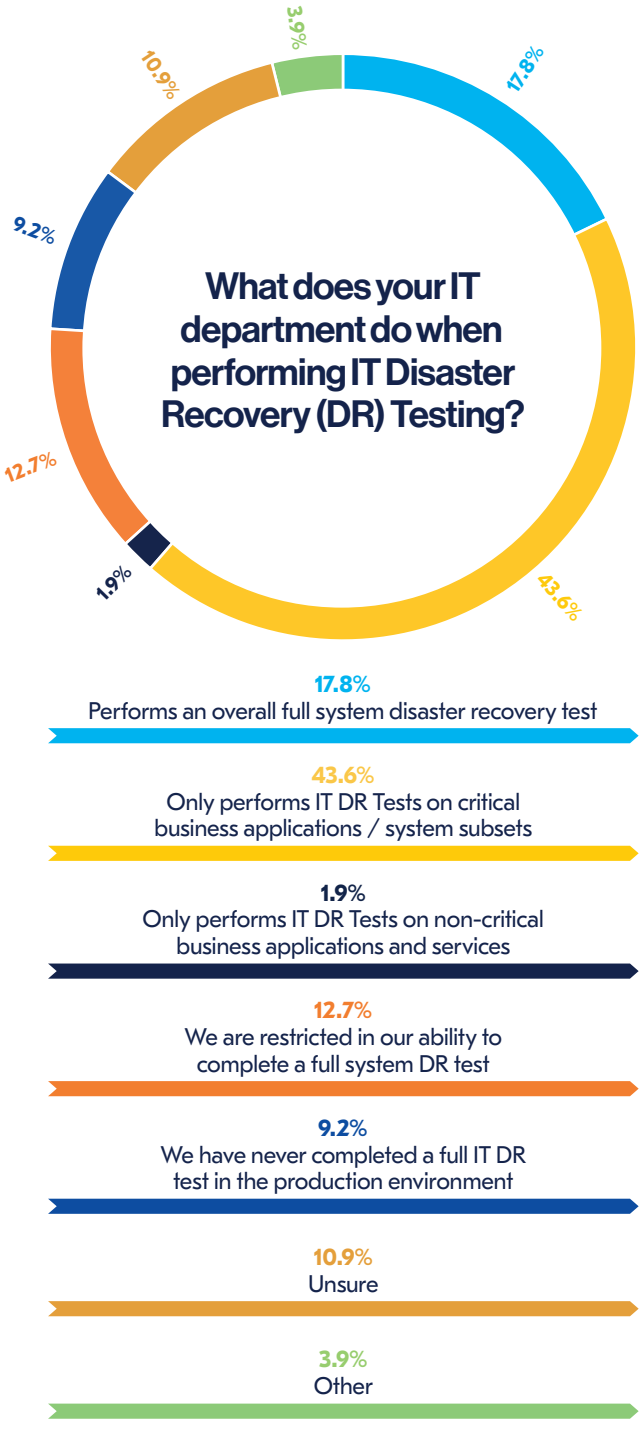


Figure 15. What does your IT department do when performing IT Disaster Recovery (DR) Testing?

If your IT department is restricted in being able to perform an overall full system disaster recovery test, which of the following factors are applicable?

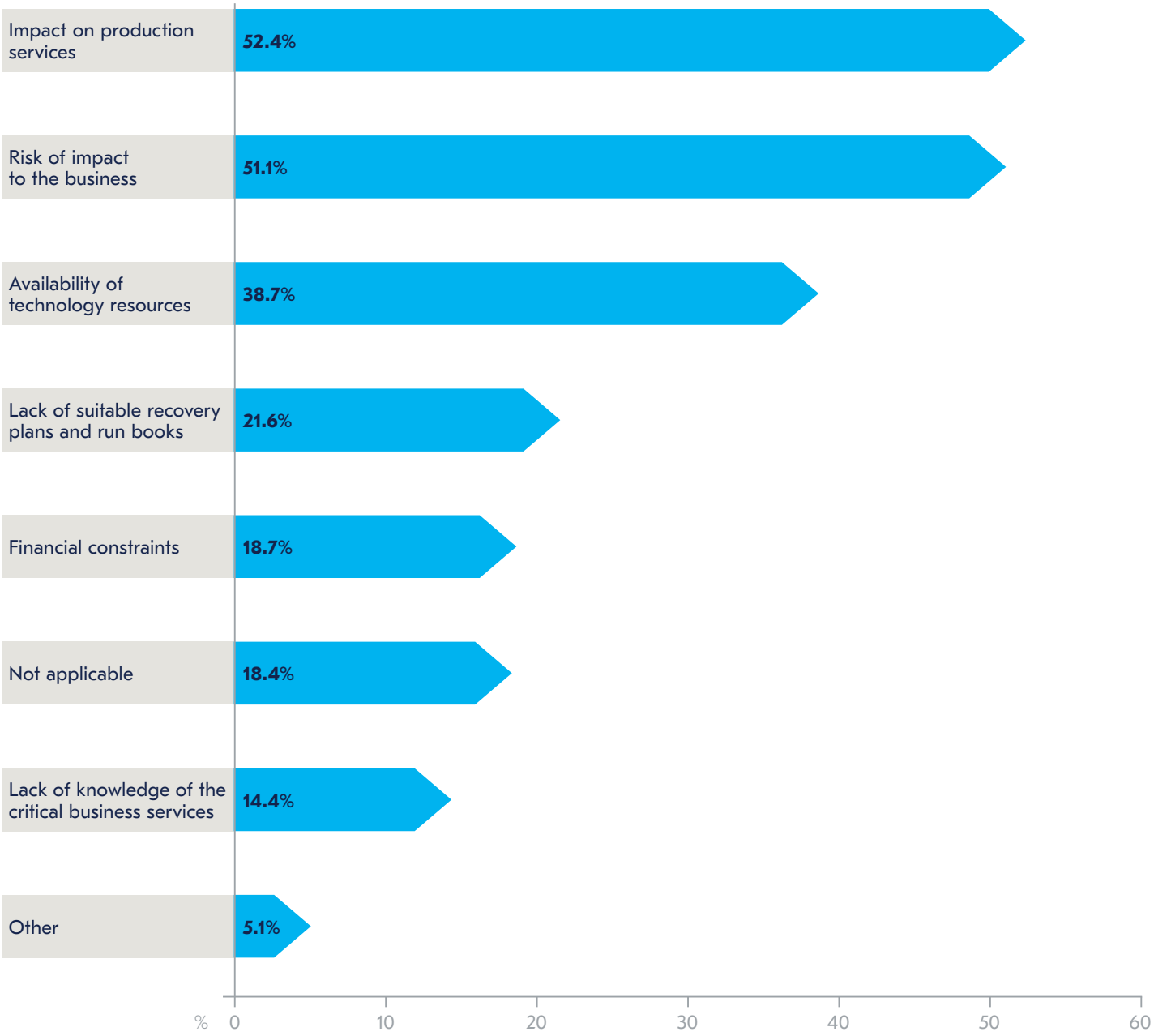


Figure 16. If your IT department is restricted in being able to perform an overall full system disaster recovery test, which of the following factors are applicable?

Covid-19 and Technology Resilience

With many staff working from home, IT systems have faced resilience challenges

- 94.7% of organizations have had staff working from home during the pandemic, with 35.0% reporting all staff have been working from home.
- Although many organizations were able to quickly revert to a working-from-home model, those which had limited experience with remote working frequently encountered issues.
- Acquiring new hardware proved to be a major inhibitor to facilitating remote working.
- Organizations have been diligent about ensuring the necessary security measures are in place to support remote working, but many were slow to implement the necessary measures.
- Some organizations were agile and adaptive with measures adopted to help staff work from home effectively, even working with local Governments and network providers to ensure staff could access systems where internet access is strictly controlled.

With offices moving to virtual environments as a direct result of COVID-19, the requirement for resilient technology infrastructure is now of paramount importance. The BCI's *Future of Business Continuity and Resilience report* revealed that of all the types of resilience at play within an organizations infrastructure, it was IT resilience which professionals viewed more than any other type of resilience as the most major contributor to the success of their response to COVID-19[13].

Indeed, when respondents were questioned about their organization's own homeworking policy during the pandemic, a third (35.0%) reported that all staff had been working from home throughout the pandemic and a further half (49.1%) said that some staff had been working from home. Split team working has been the favoured option for some organizations, with 10.6% operating a model where staff those who work similar roles are rostered between homeworking and being in the office; a particularly favoured option in the financial services sector where the trading community are suited to working in an office environment. 0.9% of organizations are adopting a split team working model where no staff are working from home. Such a working model was often the only choice for organizations who had specialist equipment within offices (such as manufacturing organizations) or industries which had a high proportion of customer-facing roles such as retail, leisure & hospitality or manufacturing.

For organizations employing foreign nationals, many had the additional problem of staff wanting to return to their home countries to work remotely whilst they were still able to travel. Although the majority of staff were able to seamlessly work in another country in the European Union for example, many wanted to work in areas such as Africa where either laptops were not compatible with the infrastructure available, or they were not set-up to cope with the risk landscape of a different country. Larger organizations had the resources to be able to make the necessary changes to user hardware and software but for some smaller organizations, the extra demands on stretched IT departments are likely to have resulted in delays or barriers for staff wanting to remote work from their home countries.

"When you're dealing with risks and vulnerabilities in IT you have to see the big picture, what may be resilient in Europe, may not adapt to certain types of risks that you would have in other parts of the world. So it was very important for us, as quickly as possible, to find out where everybody was during lockdown and to make sure that all the PCs were covered for any eventual cyber-attack or phishing attack. Each territory does it in different ways and we were keen not to be caught out by that with our staff. This was something else that we had to add to the USR (User Security Rules) for remote working."

Security Manager, Professional Services, France

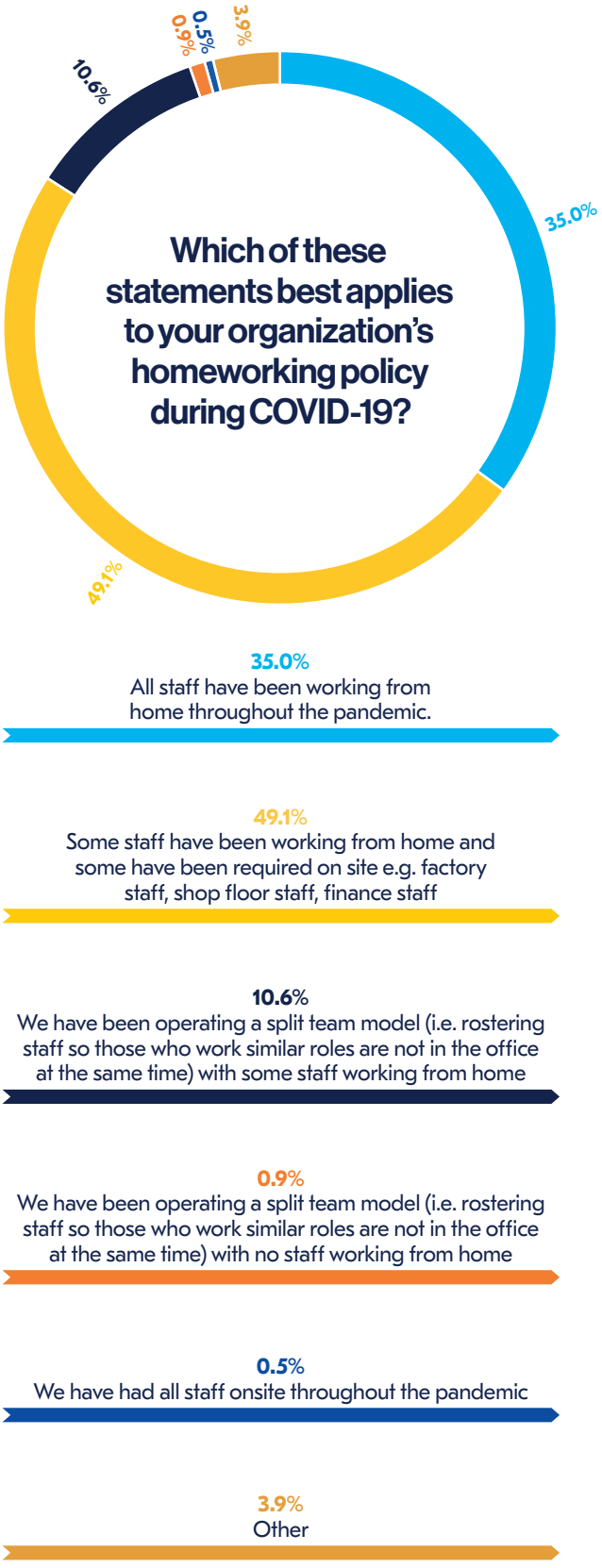


Figure 17. Which of these statements best applies to your organization's homeworking policy during COVID-19? (If your company is multinational, please answer for your geography only). When answering, please assume this relates to non-furloughed staff only.

13. BCI, The (2020). The Future of Business Continuity and Resilience. Available at www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html (Accessed 29 September 2020).

Moving to remote environments, particularly for organizations which did not already have a universal work-from-home policy in place, meant IT departments had to adapt quickly to ensure staff were not only able to work remotely, but were able to work in a secure environment. Research carried out by the BCI at the beginning of the pandemic showed that whilst most organizations had made provisions for staff to work remotely from a hardware perspective, the necessary security measures were often only addressed later. The *BCI Coronavirus Report Issue 2*[14] showed that by early April, less than two-thirds of organizations (65.2%) had added additional security measures to reflect new working from home measures, and just 59.2% had reviewed their plans in the event of a cyber security threat. By mid-May, 80.4% of organizations had added additional security measures for staff working from home, and two-thirds (66.1%) had reviewed the disaster recovery plan in the event of a cyber security threat[15].

Indeed, the research carried out for this report mirrors that carried out in the research at the outset of the pandemic. In the survey for this report, some 63.0% of organizations reported having the necessary cyber security arrangements in place at the start of the pandemic and 27.6% of organizations reported having to add additional security measures to systems during the pandemic.

Whilst it is to be applauded that most companies did add additional security measures, the length of time it took to implement these could have resulted in security issues leading to unplanned downtime, particularly as cyber criminals have targeting remote workers during the pandemic: phishing attacks increased by 600% in the first quarter of 2020[16], something echoed by survey respondents. 11.1% of organizations actively identified an increase in the social engineering and/or cyber-attacks on employees during the pandemic. However, despite this notable increase, the survey further suggests that organizations have done little to prepare employees for the increase in cyber-crime: just 27.6% of organizations reported that staff had received extra training on working from home and cyber security.

Ensuring strict security measures can be implemented quickly in the case of a future major crisis should now be a priority for organizations going forward. Such a lag between a major incident happening and the necessary security processes being implemented could result in significant security issues.

"Cyber-attacks and subsequent data loss and/or corruption need to encompass a completely different way of thinking compared to the traditional facility focused disaster recovery view. Such attacks often consume not just production environments but also recovery and back-up before they are even identified."

David Morgan
Head of EMEA Consulting
Sungard Availability Services

14. BCI, The (April 2020). Coronavirus Organizational Preparedness Report; Issue 2. Available at www.thebci.org/resource/bci-coronavirus-organizational-preparedness-report---2nd-edition.html (Accessed 29 September 2020).
15. BCI, The (May 2020). Coronavirus Organizational Preparedness Report; Issue 5. Available at www.thebci.org/resource/bci-coronavirus-organizational-preparedness-report---5th-edition-.html (Accessed 29 September 2020).
16. Sjouwerman, S (2020). 'Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600%'. KnowB4 (9 April 2020). Available at: blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600 (Accessed 29 September 2020).

In relation to your cyber security arrangements during the pandemic, which statements apply to your organization relative to remote/homeworking?

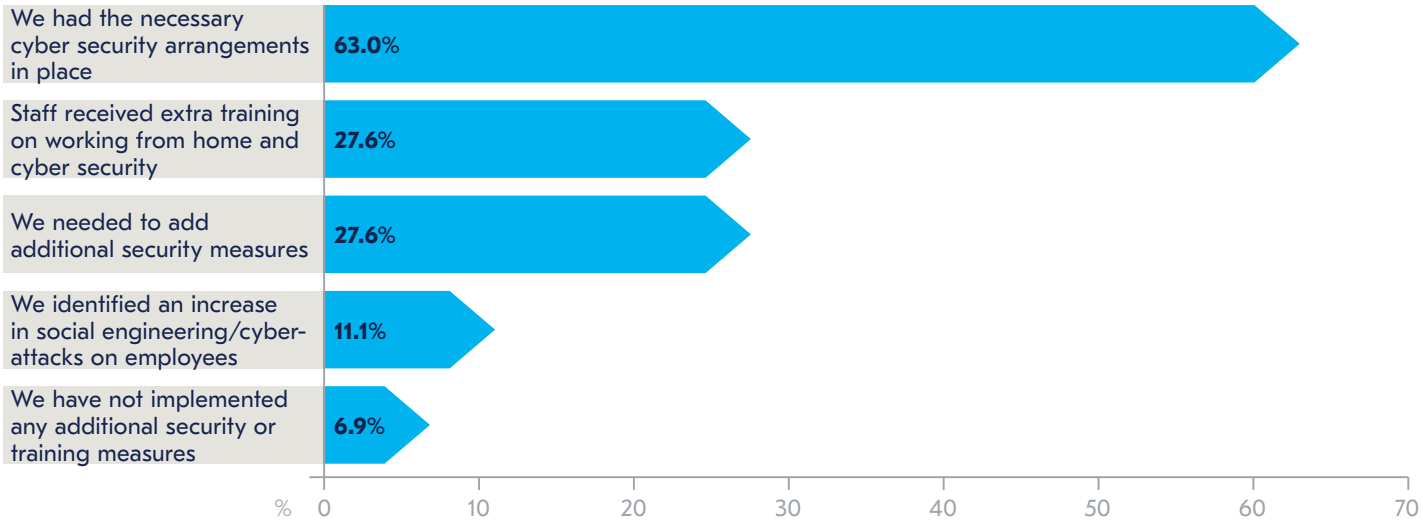


Figure 18. In relation to your cyber security arrangements during the pandemic, which statements apply to your organization relative to remote/homeworking?

It does appear that organizations have taken note of the extra security concerns being imposed on organizations as a result of the pandemic. Cybersecurity and Privacy was the area which looks most likely to receive priority funding as a direct result of COVID-19, with more than half of organizations (52.3%) considering it to be a "high priority investment" or "priority investment".

The following three priorities — connectivity/bandwidth, collaboration tools and video/voice services — all echo a movement towards technology being an enabler to remote working practices. Connectivity/bandwidth is a "high priority" or "priority" investment for 47.7% of organizations, collaboration tools for 56.8% of organizations and video/voice services for 40.4% of organizations. In contrast, tools associated more with more traditional office IT environments are given a much lower priority in terms of future spending: backup systems (e.g. power, network etc) are will be a "high priority" or "priority" investment for just 30.8% of organizations and desktop imaging systems a priority for even less organizations (17.1%).

Indeed, whilst COVID-19 may have been sending major shock waves around the global financial markets, it seems many IT departments are still able to acquire the additional investment they need for equipment because senior management are aware of the importance of having robust systems in place to ensure continued productivity during the pandemic.

"During COVID-19 I have rarely heard my chief executive tell me that money isn't an option — even though we had just invested in new IT kit for our councillors [just as the pandemic broke out]. Once they suddenly realised that we had to get our councillors and committee meetings also working and meeting virtually because of COVID-19, I again encountered that very rare occurrence where I was told that money wasn't an option and I just had to make it happen."

Head of IT & Resilience, Public Sector, United Kingdom

Given your experience with COVID-19, which of the following services/tools will your company now invest in?

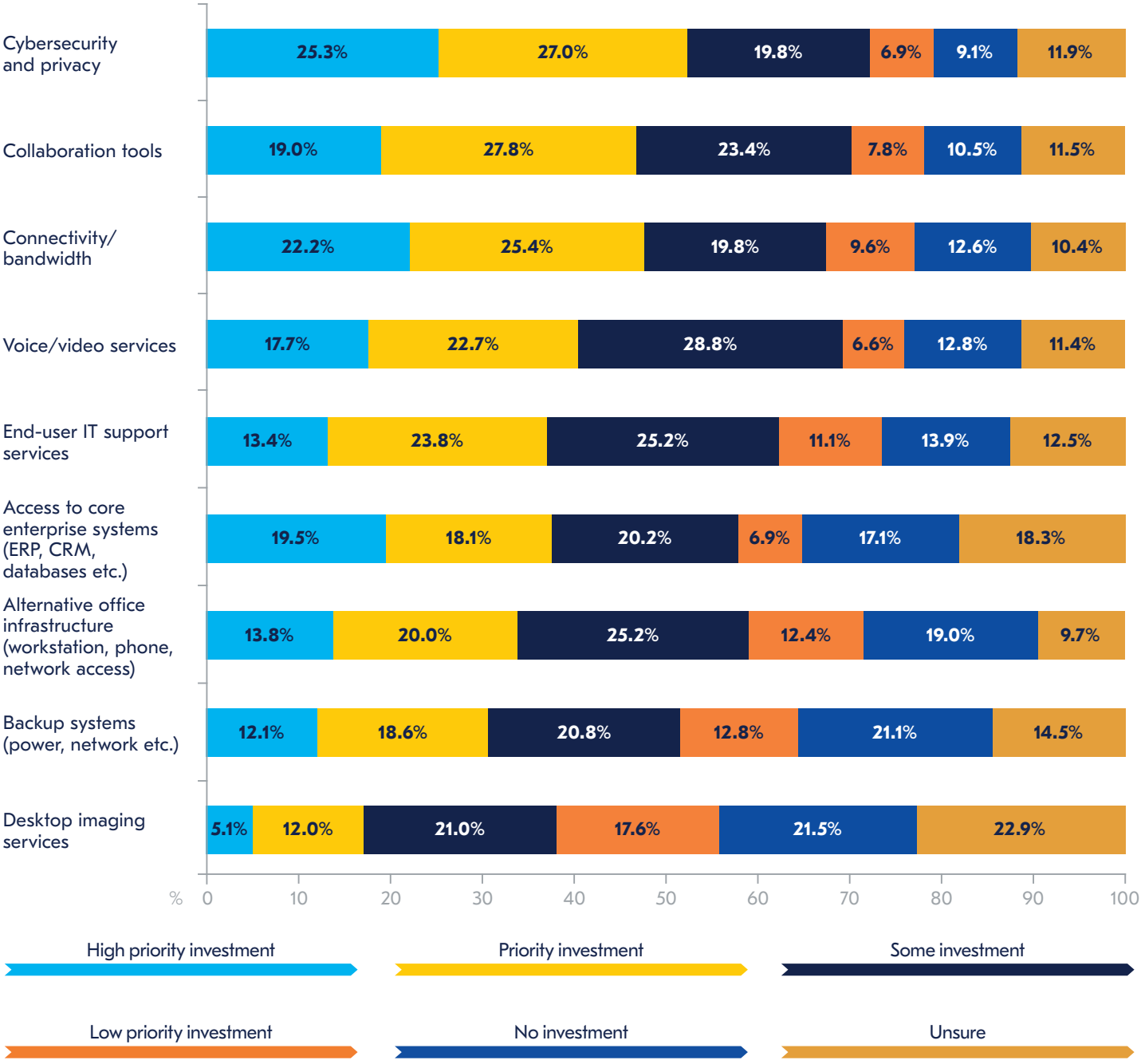


Figure 19. Given your experience with COVID-19, which of the following services/tools will your company now invest in? Please rank the importance of each (5=high priority investment, through 1=low priority investment)

When analysing the technology issues faced by organizations because of the pandemic, hardware availability was the issue which caused the most disruption for organizations. Organizations which had staff working in call centre environments for example, typically relied on desktop computers and internal IT infrastructure for staff. With organizations unable to invoke their Work Area Recovery sites due to their primary office not closing, many found themselves unable to purchase sufficient laptops to enable staff to quickly revert to a working from home environment. This survey has revealed that for 5.6% of organizations, the lack of available equipment caused major disruption and staff were unable to work. A further quarter (23.7%) admitted that the lack of equipment was a cause of disruption. In fact, just a third of organizations (33.5%) said that the lack of equipment was not an issue at all. This suggests a lack of scenario breadth was considered when analysing the potential organizational risks for an organization or, if an impact-based analysis was used, a lack of consideration for a sudden lack of availability of equipment.

For some organizations, remote working had not been widespread before the pandemic but they were well-prepared for it after having to adopt the practice during previous incidents. One interviewee from a public sector organization — where remote working tended not to be encouraged — had made adaptions during a previous crisis which helped to ensure staff were immediately able to revert to a working from home model immediately.

"Because we had a few days' notice, we had been working to try and get staff to take home their laptops home every evening voluntarily. We demanded that they did so during the Beast from the East and, as a result, we had about 80% our workforce working remotely for two or three days then. And then obviously, during COVID-19 the Government told everybody to work from home, and so everybody did — and we're well-rehearsed at it because of the Beast from the East. If I'm truthful, we've been working towards this in a continuity and flexible working perspective for three or four years, but it was COVID-19 that made the last doubters who said 'it couldn't possibly work for me' go and work from home and make it work."

Head of IT & Resilience, Public Sector, United Kingdom

Remote access and VPN issues were a further inhibitor to staff being able to work effectively from home. 7.3% of organizations reported the issues were so severe that staff were unable to work at all, with a further 17.3% reporting it caused some disruption. Other respondents said their organizations were not prepared to support the increased reliance on technology and the resulting issues encountered with multiple staff working from home, whilst others admitted their system capacity could not cope with staff working at peak times. Both these issues resulted in one in 20 organizations having staff unable to work.

Having robust plans in place for staff to revert to a remote working model and ensuring these plans are regularly exercised would have helped many organizations to overcome these issues. Such a strategy does not need to be included with a pandemic-specific plan, and should form part of a more generic, impact-based planning process — as recommended by the BCI's *Good Practice Guidelines* (GPG). Indeed, recent research by the BCI for the *Future of Business Continuity and Resilience report* showed that some 10.9% of Business Continuity professionals experienced anger from the Board that they had been unable to anticipate the exact scenarios posed by COVID-19. Although sympathy may be offered in the first instance due to the unpredictability of the pandemic's path, such frustration can be partially understood if business operations were unable to continue due to not being included in plans.

Some organizations had the foresight in the early months of the pandemic to anticipate that staff may have to quickly revert to a remote working environment by monitoring the situation in other geographies where their organization operates or monitoring the measures other organizations were employing. In some cases, organizations told of the necessity of having to be one step ahead of their own Government when implementing new working practices. For some organizations, this meant ensuring they had sufficient hardware in place. For other organizations, network capacity was a key consideration. One interviewee explained how they were confident they had sufficient equipment in place, but still had to make plans to ensure networking capacity was able to support mass remote working and staff had the relevant applications and VPN software installed on machines.

"We've got workforce of just over 500, 250 of which are in a call centre. Half of the workforce could work from home relatively easy. We then went out to all the staff and asked who could work from home and who had the facility to do it. For those that couldn't, we immediately started sourcing equipment. So, we had our first order in for extra kit around about 3 March – 20 days before we entered into lockdown."

Operational Resilience Manager, Financial Services, United Kingdom

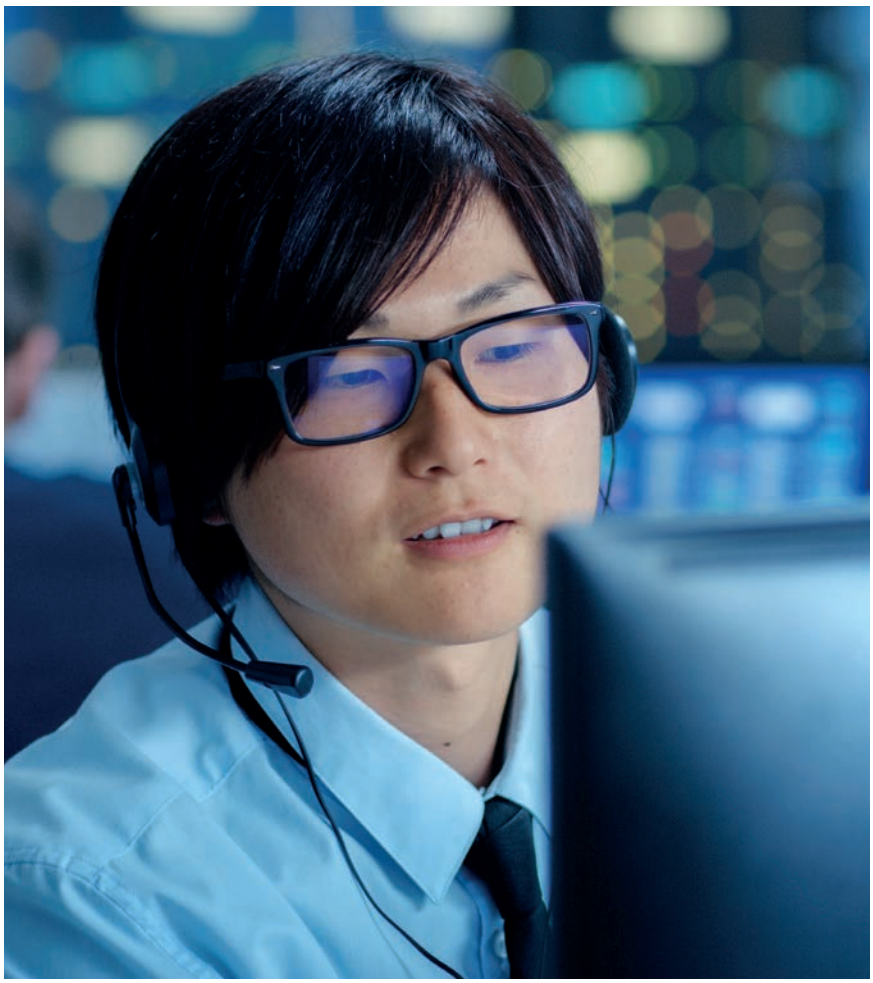
"[The IT Resilience Team] engaged with the business continuity team, our desktop support people and our networking people back in January. At that point, we said 'we think this is coming, and we think it's going to be serious. Go and check your applications, check your network, check your VPN capacities and make sure we've got enough.' So we reach the end of February and we had virtually the entire organization working from home; tens of thousands of people. This is where the confidence comes from. We'd already done it once full lockdowns came in. We already had everybody working at home, we didn't have any capacity issues on the network and the VPN was fine."

IT Risk Manager, Energy & Utilities, United Kingdom

Other organizations went above and beyond with their planning processes when it came to remote working. An Australian university which had a large contingent of Asian international students, for example, set up a VPN in China so Chinese students could continue to access resources despite the heavily moderated internet access in the country.

"We have a lot of international students, especially from Asia including China; and obviously we have lost them temporarily as a result of the pandemic. They were unable to come to Australia. This meant some of those students, particularly those in China, were restricted from working due to the country's great firewall. We had to work with their hosting provider, Alibaba providing special access to the required resources to continue study on-line. That has enabled over 1,000 students based in China to continue to study during Covid-19."

IT Continuity Services Manager, Higher Education, Australia



What technology issues have you encountered when trying to ensure staff can work from home and how much disruption did it cause?

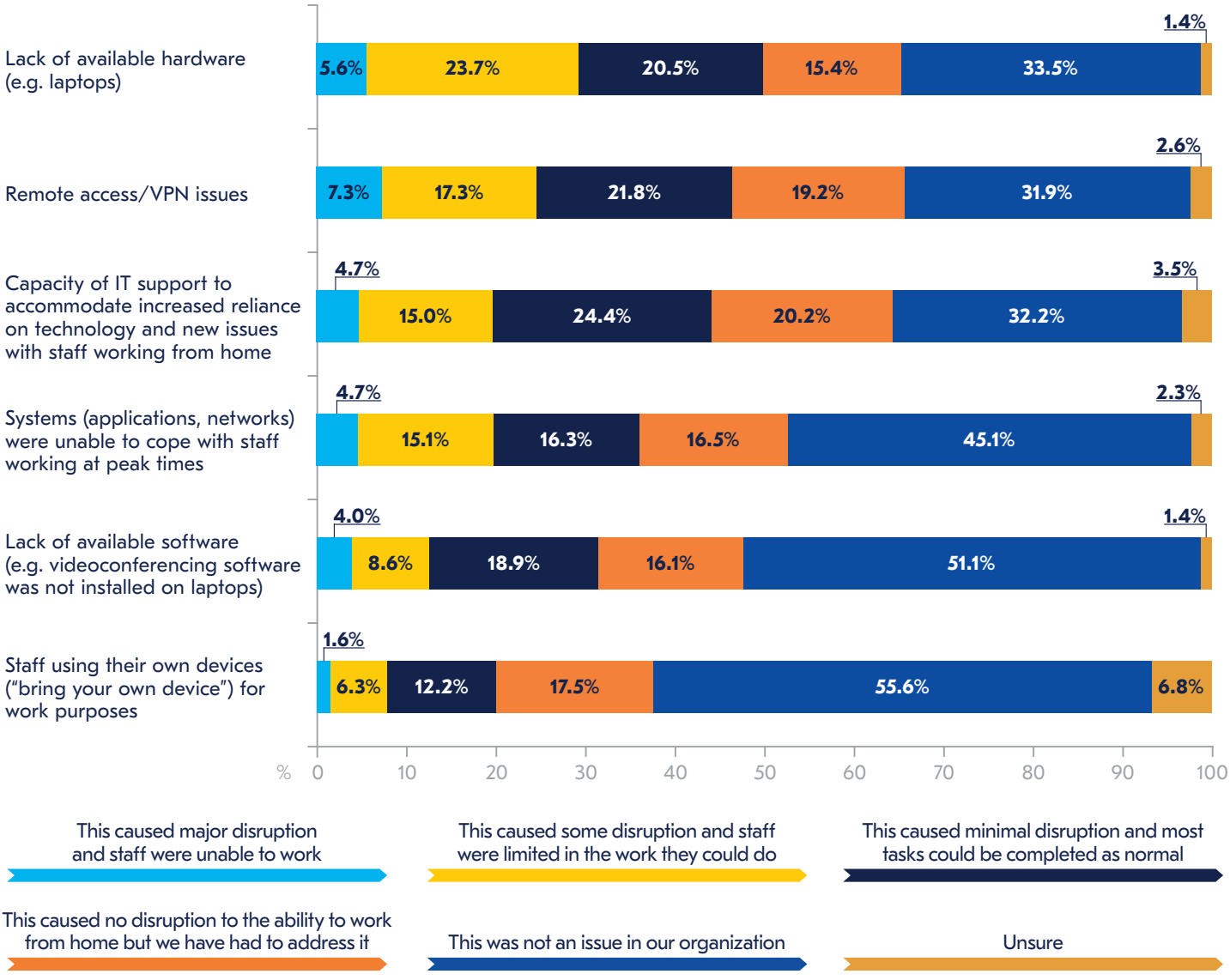
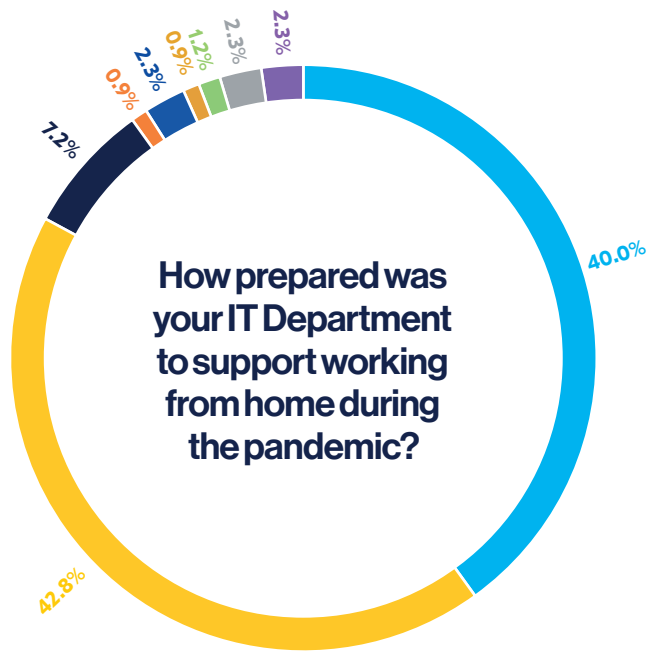


Figure 20. What technology issues have you encountered when trying to ensure staff can work from home and how much disruption did it cause?

The survey also asked more specifically about availability of hardware for staff who were required to from home. Just 40.0% of organizations said that staff were who were required to work from home had the necessary equipment to do so immediately, with no impact on productivity. A slightly higher proportion, 42.8%, said that whilst staff were able to revert to a working from home environment immediately, it took several days before all the necessary equipment could be provided to staff. One in ten organizations had very limited provisions made for homeworking and were not able to start working until they had acquired the necessary equipment. 7.2% of organizations took a few days before they were able to start working, and 2.3% said it took longer than two weeks for staff to have the necessary equipment.



40.0%
Staff who were required to work from home had the equipment necessary to work from home immediately, with no impact on productivity

42.8%
Some staff were able to work from home immediately but it took us a few days to acquire sufficient hardware. This had a minor impact on productivity

7.2%
Staff were not set up for homeworking and it took a number of days before we could provide the necessary hardware. this had a measurable impact on productivity

0.9%
We were not set up for homeworking and it took two weeks before staff had the necessary equipment. This had a significant impact on productivity

2.3%
We were not set up for homeworking,and it took longer than two weeks before staff had the necessary equipment. This had a significant long-term impact on productivity

0.9%
We relied on staff using their own personal devices

1.2%
Unsure

2.3%
Not applicable

2.3%
Other

Figure 21. How prepared was your IT Department to support working from home during the pandemic?

For the third of organizations that were unable to implement the required work from home arrangements immediately, nearly half (48.3%) admitted it was because their Business Continuity Plan (BCP) did not consider mass working from home. Many organizations had considered the scenario of staff not being able to work in the office, but their primary back-up was a Work Area Recovery provider. With many organizations not able to invoke their shared recovery contract due to their primary sites not being closed however, this left some companies without appropriate backup for the pandemic scenario. This serves as an example of the importance of ensuring contracts are fully scrutinised when formulating a BCP.

One in five organizations (20.7%) were unable to implement arrangements immediately and admitted it was because their plans relied on them being able to acquire equipment quickly. Again, whilst such a plan may be viable for an organization being affected by a single site outage, it shows the importance of considering the wider environment when making plans. A plan could assume an organization is able to acquire 300 laptops with relative ease for example, but when millions of other organizations have the same back-up strategy within their plans, the plan is likely to fail.

For those organizations, the impact on productivity — and ultimately the balance sheet — was tangible. Many of those organizations told us they are intending to keep the purchased equipment and refresh it in line with standard policy so they would not encounter the same difficulties in future.

For one in ten organizations, their inability to immediately work from home was as a direct result of miscommunication between departments: 5.7% of IT professionals assumed that Business Continuity would have plans in place to allow staff to remotely, and 5.2% of BC professionals assumed that IT would have plans in place. Again, this highlights the problem of different departments working in silos, and the need for a co-ordinated, multidepartment approach to resilience being adopted.

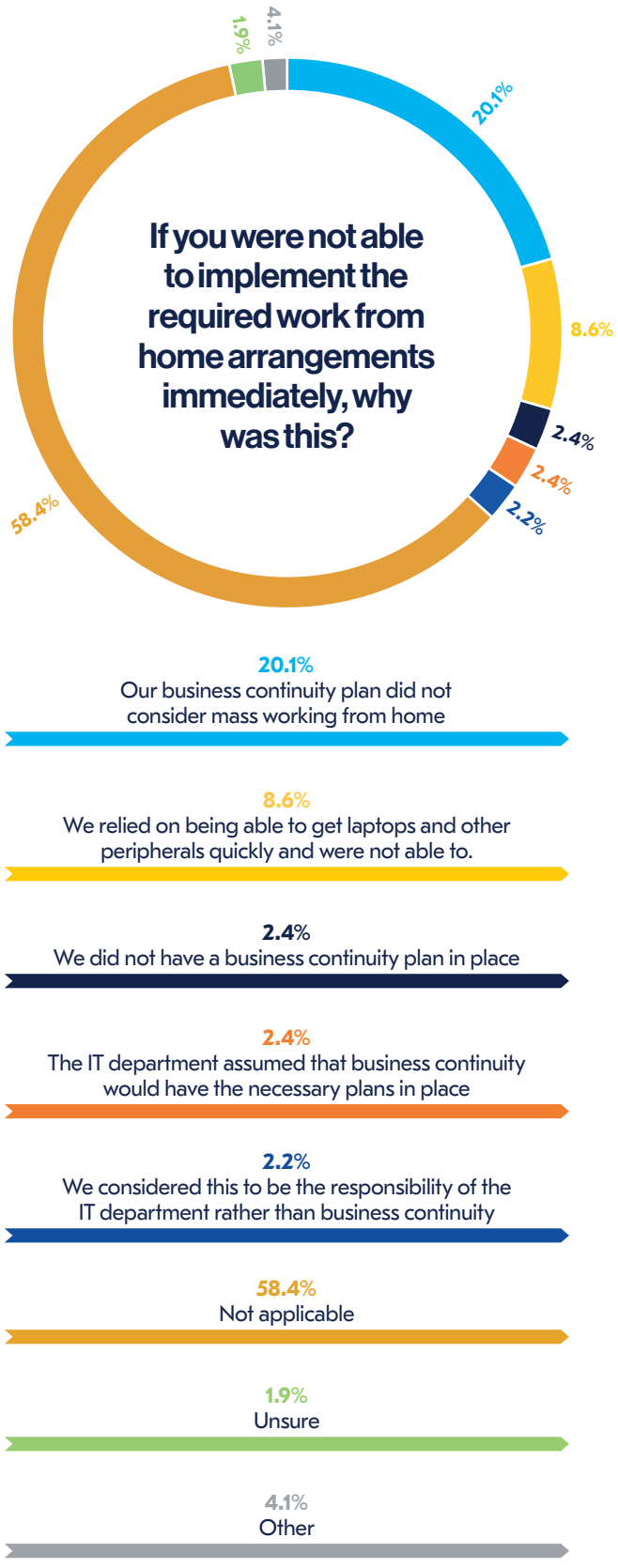


Figure 22. If you were not able to implement the required work from home arrangements immediately, why was this?

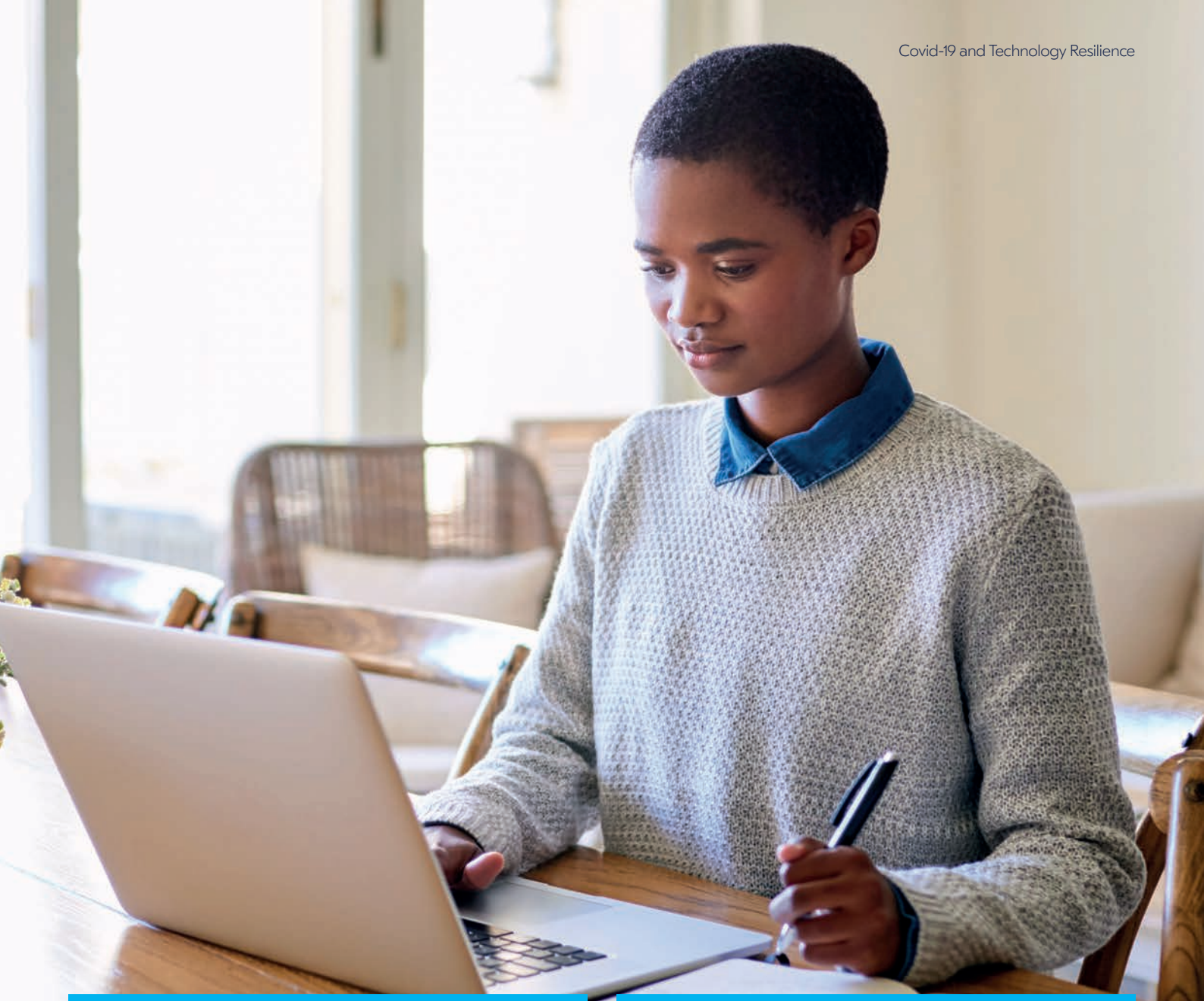
However, it was not just the technology which caused disruption during the pandemic, but workers' physical environments as well. Many workers who were not accustomed to working in a remote environment did not have facilities within their own households to work effectively and efficiently. Some had no home office, others had to fit their work around children who had their schools closed and others had household members who were also trying to work from home at the same time.

It is therefore not a surprise that a quarter of respondents (25.4%) said that distractions at home caused so much disruption that staff were either unable to work at all or were limited in the work they could carry out. A further fifth (20.7%) reported the same disruption levels for staff who did not have an appropriate working environment.

Even though many organizations were able to operate with staff working remotely, many had not carried out the appropriate risk assessments to ensure staff were working in a risk free environment — and many have no plans to in the immediate future. The BCI's *Future of Business Continuity and Resilience report*[17] revealed that less than half of organizations (42.0%) will be ensuring that home environments are part of their organizational resilience and risk reduction programmes, and only 56.9% will be defining specific standards for the home working environment and the supporting processes. This is a disappointing statistic: given the number of organizations who had to quickly revert to a remote working model during the pandemic and the resulting issues encountered, some organizations are clearly not making any preparations to ensure homeworking environments are risk free going forward. Although many organizations will ultimately return to the office, having safe and functional environments for staff to work in should they need to work remotely again should be a consideration for most organizations. COVID-19 may have been the catalyst for homeworking in 2020, but there are multiple other scenarios organizations could be and will be presented with in future that will mean entire company staff rosters will have to work remotely again.

Some organizations have recognised that some staff need extra support during the sustained period of remote working and have been providing workers with new equipment to ensure they can work from home effectively. Others have been providing employees with grants so they can make the required equipment purchases themselves.

17. BCI, The (2020). The Future of Business Continuity and Resilience. Available at www.thebci.org/resource/bci-the-future-of-business-continuity---resilience.html (Accessed 29 September 2020).



"We initially provided a stipend to junior levels of staff so all those at Associate Vice President level or below were invited to have $150 for the first few months. We then reissued a second stipend in August. This second stipend was because we started to realize that we had a lot of health and safety and ergonomic issues beginning to kick in. At the start, we sent out videos and said things like "you might not have the same setup as you have at home, but you could maybe use a couple of books to put your monitor on". We were trying to make do of our own version of ergonomics on the fly for the first part, but then it was clear that a lot of people do not have sufficient home setups. Some have been sitting on a sofa, and then that's causing them to have shoulder and neck problems. The further stipend was released to enable people to buy items such as chairs and desks to help with postural issues."

Business Continuity Manager,
Financial Services, United Kingdom

"But we recognized in our BIAs that we had quite a number of people, whether it was because of their role or because of a physical handicap, that had special equipment in the office. And so we had to make sure that this equipment got to them. All of our staff have portable PCs, but if people needed special printers, special scanners, special robots, etc. – we had to look into it. So we had to update our due diligence on that to say, in what circumstances they could use it, how they should use it, etc. when working from home. At first, we didn't think in the long term and thought they can do without those extra pieces of equipment if it's a few days out of the office or even a week or so. However, when we were two months in, we thought we're going to have to make them comfortable and give them all of the special equipment that they needed to work from home."

Security Manager,
Professional Services, France

What working environment issues have you encountered when trying to ensure staff can work from home and how much disruption did it cause?

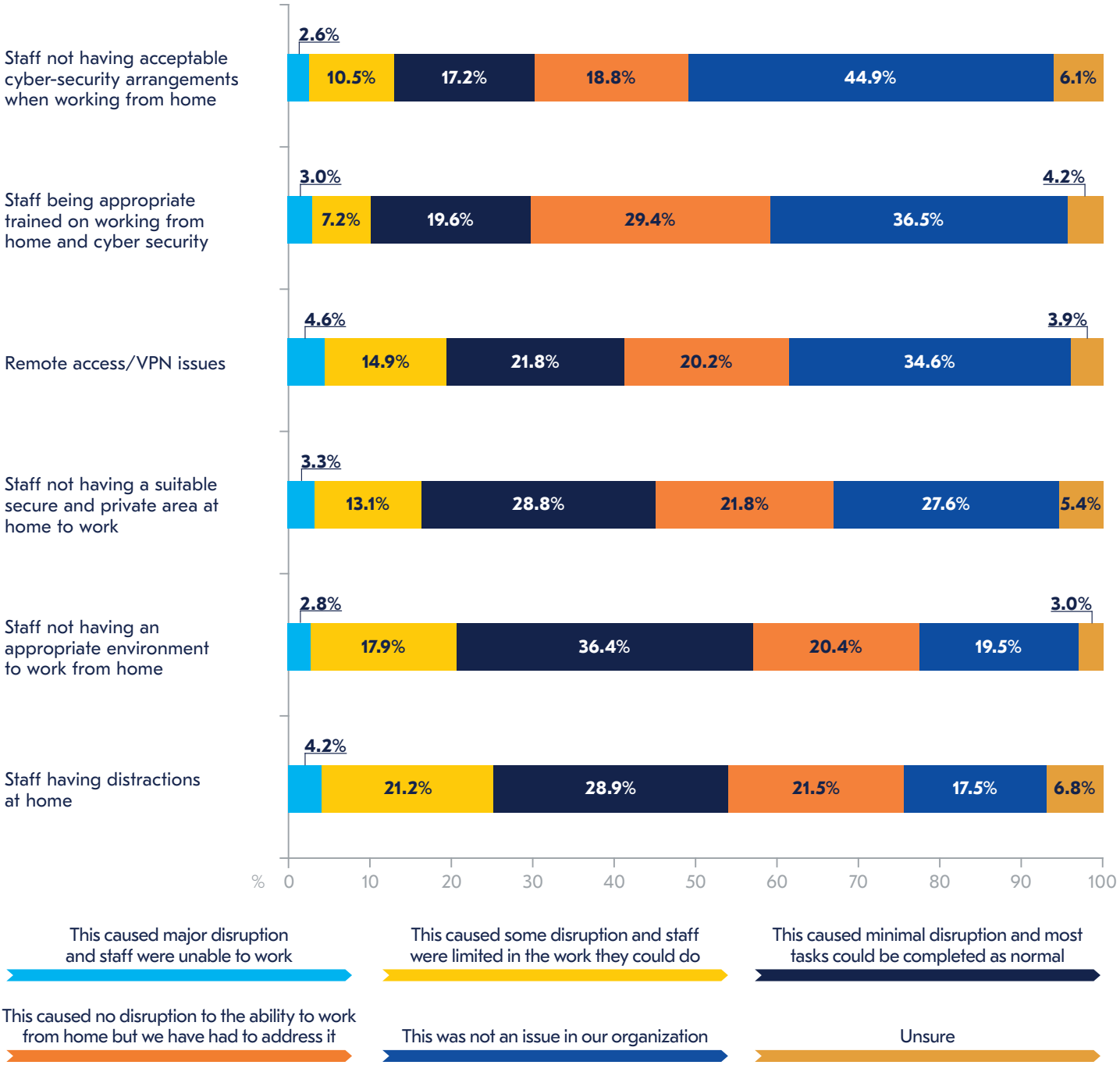
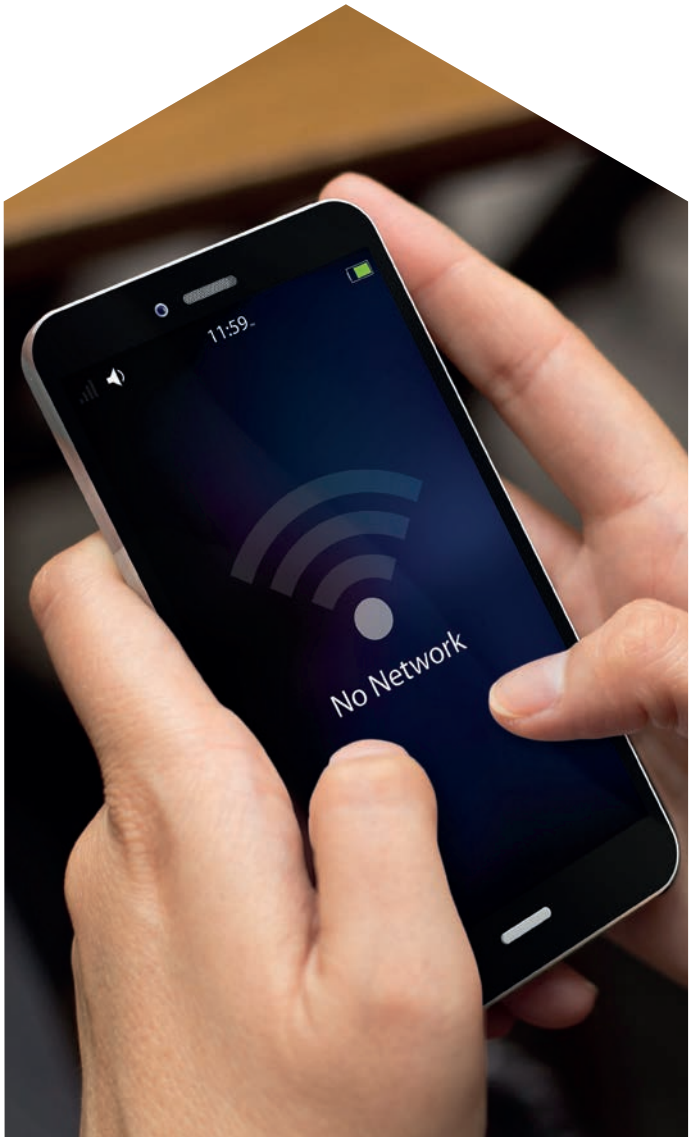


Figure 23. What working environment issues have you encountered when trying to ensure staff can work from home and how much disruption did it cause?

Indeed, whilst many organizations faced significant operational and strategic disruption in 2020 as a result of the pandemic, it did not make them immune to additional disruptions. Although nearly two-thirds (60.2%) reported not having another major incident this year, 22.1% did. Encouragingly, of those organizations which did encounter disruptions this year, 84.2% were able to recovery in line with their Recovery Time Objective (RTO), despite the organization already facing COVID-related headwinds. Just a small minority (4.1%) of those who had a secondary disruption reported that they were severely hampered in the ability to recover as a direct result of COVID-19. For many organizations, it was a lack of onsite IT staff due to COVID-19 which meant recovery options were limited, particularly for those with on premise servers. Although in some situations, remote hosting should have been used as a backup, some organizations reported that their contracted provider were unable to meet Recovery Time Objectives due to a lack of staff availability as a result of COVID-19.



60.1%
We have had no other major incident this year

18.6%
Yes, but we were able to recover in line with our standard Recovery Time Objective (RTO).

1.4%
Yes. It has severely affected the organization and we have yet to fully recover.

1.2%
Yes but we were hampered by our ability to recover in line with RTO due to non-COVID-19 issues (please specify)

0.9%
Yes, but we were hampered by our ability to recover in line with our RTO due to COVID-19 (please specify)

16.0%
Not applicable

1.9%
Other

Figure 24. Has your organization encountered a significant non-COVID related major incident this year and was your organization able to recover?

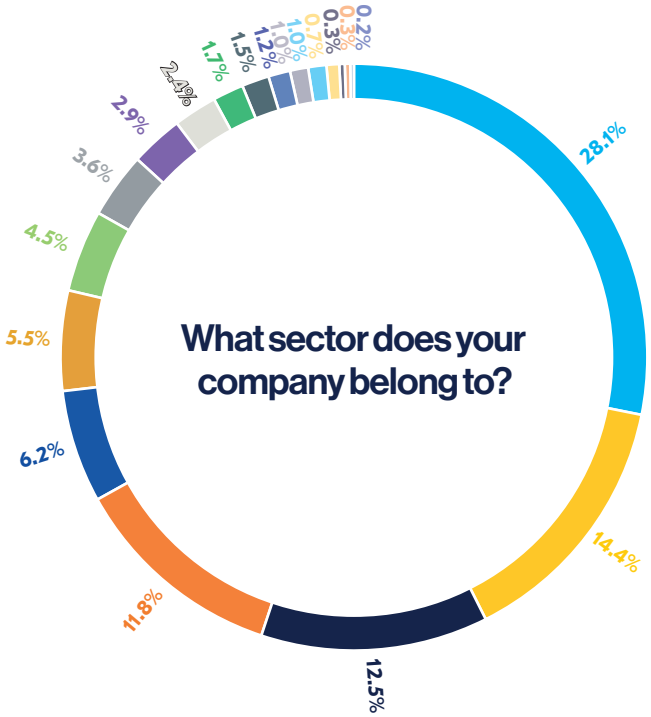
Annex

583
Respondents

80
Countries

20
Sectors

10
Respondent Interviews



28.1% Banking and finance

14.4% Information technology

12.5% Public services, government and administration

11.8% Professional services

6.2% Healthcare

5.5% Energy and utilities

4.5% Manufacturing

3.6% Education and training

2.9% Transport and logistics

2.4% Charity/Not for profit

1.7% Retail and wholesale

1.5% Emergency services

1.2% Engineering and infrastructure

1.0% Leisure and hospitality

1.0% Real estate and construction

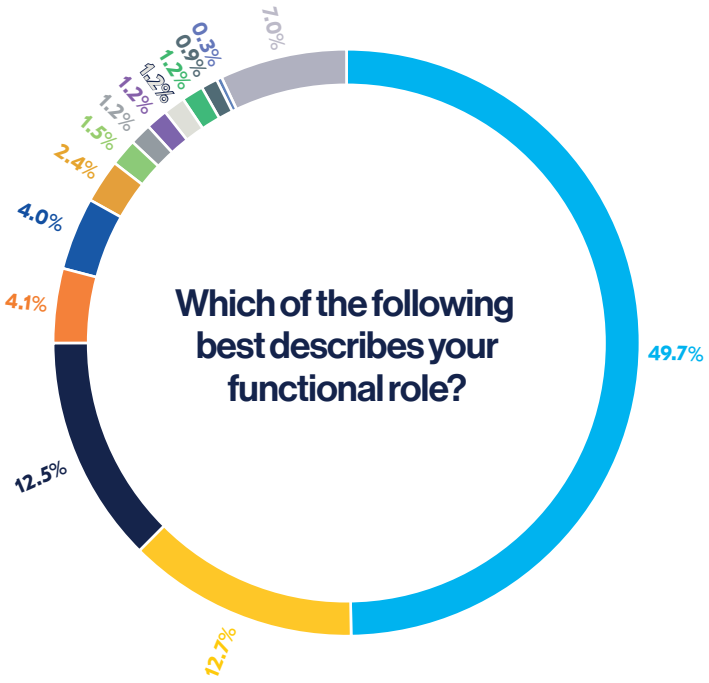
0.7% Creative industries

0.3% Law enforcement and security

0.3% Science and pharmaceuticals

0.2% Environment and agriculture

Figure 25. What sector does your company belong to?



49.7% Business Continuity

12.7% IT Disaster Recovery/ IT Service Continuity

12.5% Risk Management

4.1% Top management

4.0% Cyber/information security

2.4% Emergency Planning

1.5% Quality/Business Improvement

1.2% Internal Audit

1.2% Line of Business/ Service Directorate

1.2% Security (physical)

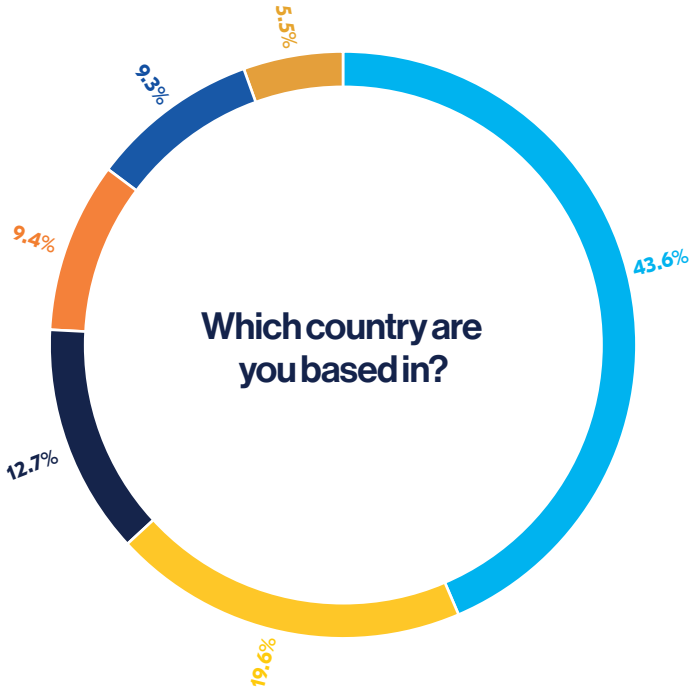
1.2% Crisis management

0.9% Health & Safety management

0.3% Supply chain/logistics/ procurement/purchasing

7.0% Other (please specify)

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



43.6% Europe

19.6% North America

12.7% Middle East and Africa

9.4% Australasia

9.3% Asia

5.5% Latin America

Figure 27. Which country are you based in?

7.6% 1-10

1.9% 11-20

2.4% 21-50

1.2% 51-100

4.8% 101-250

6.0% 251 - 500

7.7% 501 - 1,000

19.7% 1,001 - 5,000

12.0% 5,001 - 10,000

19.4% 10,001 - 50,000

8.1% 50,001 - 100,000

9.3% More than 100,000

Figure 28. Approximately how many employees are there in your organization globally?

10.1% Less than €1 million

5.8% €1-10 million

2.4% €11-25 million

2.6% €26-50 million

4.3% €51-100 million

3.8% €101-250 million

4.8% €251-500 million

7.9% €501 million-€1 billion

11.0% €1-10 billion

5.7% €11-50 billion

6.0% Greater than €50 billion

35.7% I don't know

Figure 29. What is the approximate global annual turnover of your organization?

About the Author

Rachael Elliott (Head of Thought Leadership)

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

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

About the BCI

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

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

Contact the BCI

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

About Sungard

Sungard Availability Services (Sungard AS) is a leading provider of cloud connected infrastructure solutions serving enterprise customers from 75 hardened data centres and workplace recovery facilities in nine countries. Sungard AS has a 40-year track record of delivering resilient and highly available hybrid IT solutions. Backed by high performance networks, Sungard AS modernizes customers' end-to-end IT across connected infrastructure, cloud, recovery and workplace solutions. Working with customers to understand their business objectives, Sungard AS identifies gaps in customers' current environments and tailors a solution to achieve their desired business outcomes.

Correct as of October 2020

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

bci@thebci.org / www.thebci.org