VERITAS™

Data Management in a Multi-Cloud World:

Telecoms and IT Software Edition

Data Management in a Multi-Cloud World
Executive Summary

In recent years, cloud utilisation has grown significantly across all industries, with telecoms and IT software no exception.

This is one of the industries where cloud-based deployments are most crucial, particularly when thinking about the COVID-19 pandemic and how telecoms and IT software organisations have – in part through their cloud deployments – been able to continue to support businesses all over the UK and beyond so readily.

However, despite the benefits, shortcomings do exist within cloud use and the data management and data protection that goes with it. As we will go on to see, many organisations have work to do in this area. There is considerable room for improvement when looking at data backups, visibility, scalability and availability.

It's certainly a challenge for organisations, but not an impossible one to overcome, as we will go on to explore. In many cases, organisations are utilising multiple vendors and solutions within their data management and data protection infrastructure, but this is an area where unification of vendors could be extremely helpful in overcoming issues.

This report focuses on a recent quantitative research study conducted with UK and Ireland IT decision makers (ITDMs), and considers how telecoms and IT software organisations are approaching cloud adoption, where the key challenges exist, and how they can look to overcome these challenges through improving their approaches to data management and data protection.

Data Management in a Multi-Cloud World
Key findings

Click on a key finding to read more

47%

of data in surveyed ITDMs' organisations is stored or managed in the public cloud at present, expected to rise to 76% in five years' time, on average

56%

of respondents say that, since COVID-19, moving more apps/ data to the cloud is a top three priority for their organisation – higher than any other priority

66%

identify at least one application or data source that their organisation is unlikely to move to public cloud – security concerns (62%) are the most likely reason for this

---

Risk of downtime (41%) and difficulty defending against cyber attacks (40%) are amongst respondents' greatest concerns relating to cloud-based deployments in the context of this industry

68%

admit that their organisation could improve in terms of its approaches to dealing with cyber security incidents, highlighting this as a real cause for concern

In the context of data backups, only a minority of surveyed ITDMs state that their organisation already has infrastructure that enables: having a consolidated on-premises and cloud solution (22%), storing backups across different locations (19%), being able to backup all workloads equally effectively (18%), and automatic discovery of workloads and creation of backups (16%)

27%

of respondents' organisations have full visibility with regards to regulatory requirements in relation to unstructured data

83%

highlight that the process of scaling cloud backups and disaster recovery as cloud deployment grows could be easier, while 59% agree that an inability to scale cloud deployments effectively will hold organisations back

72%

utilise multiple different vendors or solutions in unison within their data protection infrastructure

Under half of respondents' organisations ensure automatic failover (42%), eliminate single points of failure (40%), and/or implement geographic redundancy (23%) as ways of ensuring availability for cloud-based applications or services is maintained for customers

The rising utilisation of cloud within telecoms and IT software organisations

Within telecoms and IT software organisations, cloud is now almost inevitably a central part of IT strategy. Surveyed IT decision makers (ITDMs) from this industry estimate that 47% of the data in their organisation is stored or managed in the public cloud at present, on average, a figure that is anticipated to rise substantially over the next five years to 76%. Whether or not this estimation proves to be accurate, one thing is clear: modern organisations are truly embracing cloud deployments.

Average percentage of data stored/managed in the public cloud

47.40%
at present

64.78%
in three years

76.33%
in five years
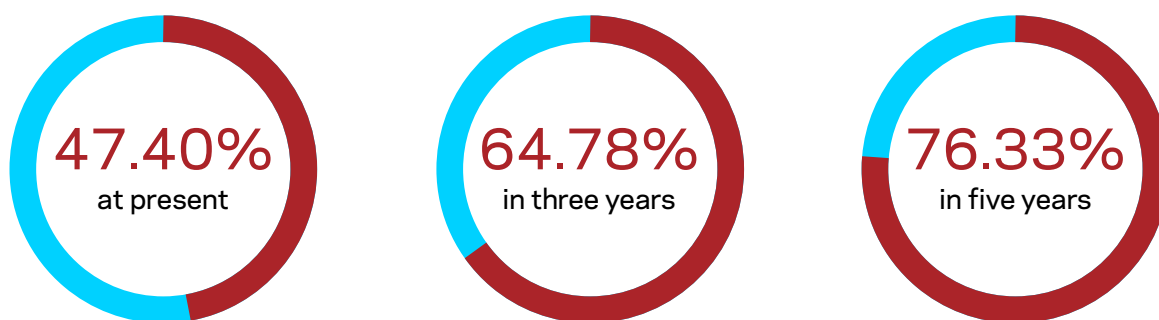
Showing the average percentage of their organisation's data that respondents estimate is stored/managed in the public cloud at present and is expected to be in the future [100]

This sentiment is echoed when looking at organisations' greatest business priorities prior to and in the wake of the COVID-19 pandemic. When thinking prior to COVID-19, over half (56%) of respondents placed moving more apps and data to the cloud as one of the top three business priorities for their organisation, higher even than reducing downtime for mission-critical apps (46%), making cost savings (41%) or increasing resilience to ransomware (31%).

Thinking since COVID-19 and the impact it has had on businesses, this figure remains unchanged – 56% of respondents place moving more apps and data to the cloud within their top three business priorities, a higher percentage than any other priority. Meanwhile, over half (53%) now place making cost savings within their top three – a considerable rise.

Organisations' top three priorities prior to and since COVID-19
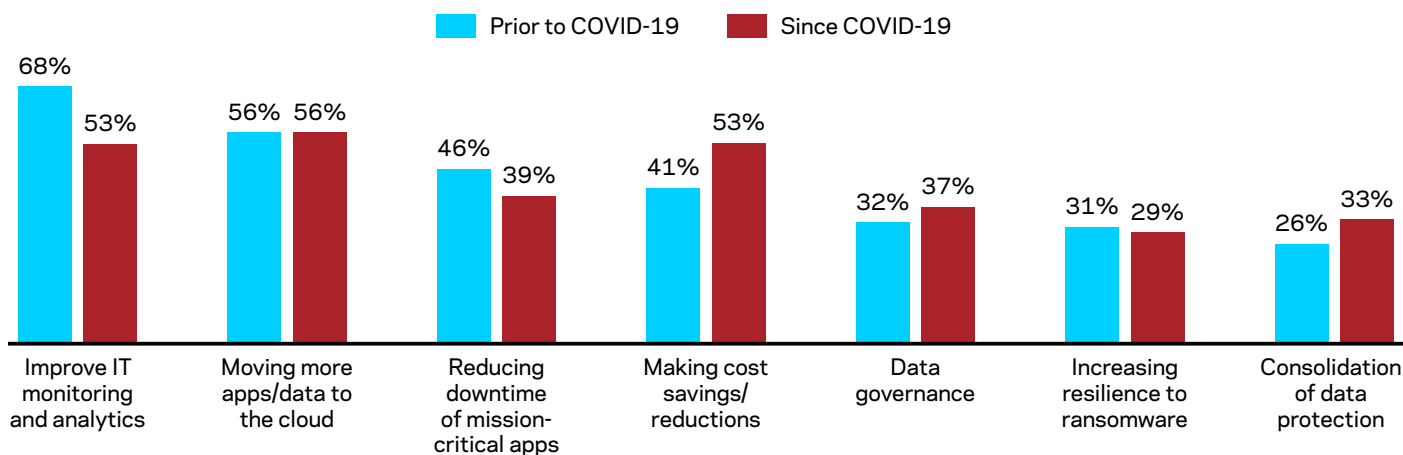
Showing the proportion of respondents that place the above in the top three priorities for their organisation when thinking prior to COVID-19 and since COVID-19 [100]
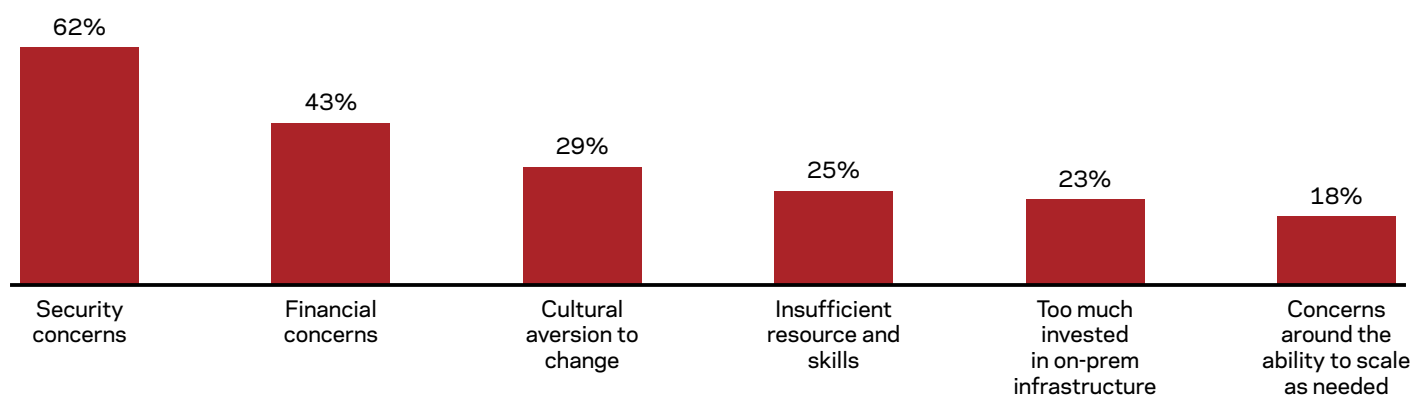
While cost savings will inevitably always be a high priority for organisations, it's no surprise to see this being far more front and centre within business priorities post-pandemic, at a time when many organisations and economies are in financial disarray. However, the fact that moving more apps and data to the cloud is still coming out on top speaks volumes about the importance that organisations are attaching to cloud deployments at this time. For many organisations, cloud utilisation has enabled them to continue operating through 2020 despite unprecedented levels of business disruption.

Cloud-based deployments are still viewed with some apprehension

Yet, despite the clear upward trend in cloud utilisation within telecoms and IT software organisations and the invaluable role that cloud deployments have played for so many of these organisations during the pandemic, apprehensions are still commonplace. Around two thirds (66%) of respondents admit that there is at least one application or data source that their organisation would be reluctant about moving to public cloud.

In terms of why respondents are saying this, the most likely reason – perhaps unsurprisingly – relates to security concerns (62%). Since cloud's inception, many IT decision makers across the UK and the world have held the belief that, despite its many benefits, it can carry additional security risks. And in a time when things such as data breaches or regulatory slip-ups can bring with them such vast consequences for organisations, it is understandable that the hesitations still exist.

Factors preventing moving certain apps and data to public cloud

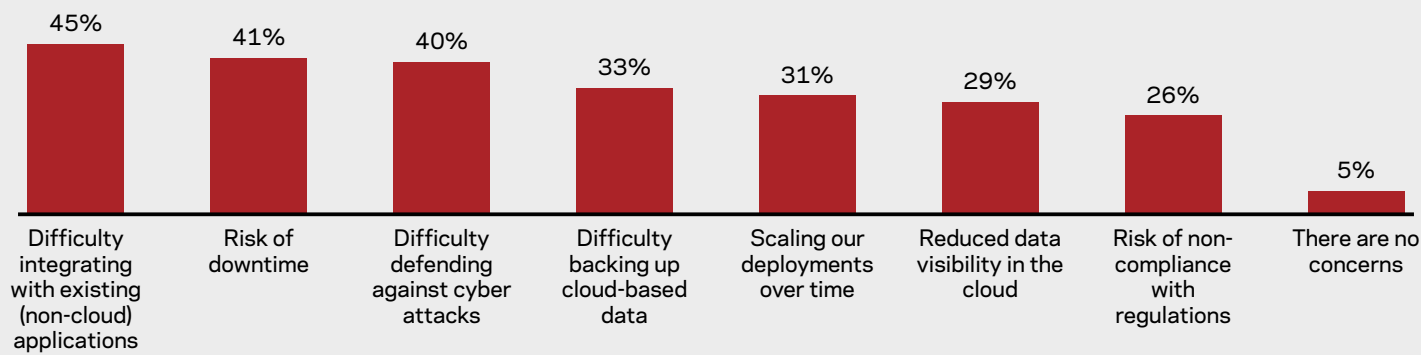| Security concerns	Financial concerns	Cultural aversion to change	Insufficient resource and skills	Too much invested in on-prem infrastructure	Concerns around the ability to scale as needed
62%	43%	29%	25%	23%	18%

What factors prevent your organisation from moving certain applications and data sources to public cloud? [67] Asked to respondents whose organisation would be unlikely to move certain applications or data sources to public cloud

Elsewhere, for those that are using public cloud, over three quarters (77%) note at least one area in which it has failed to meet expectations so far, with speed (32%), flexibility (28%) and security (27%) being the most likely areas for respondents to feel underwhelmed.

There are also a handful of cloud-based challenges which are more specific to the telecoms and IT software industries. For example, over four in ten respondents point towards difficulty integrating with existing non-cloud applications (45%), risk of downtime (41%) and/or difficulty defending against cyber attacks (40%).

Challenges to cloud deployment

45%	41%	40%	33%	31%	29%	26%	5%
Difficulty integrating with existing (non-cloud) applications	Risk of downtime	Difficulty defending against cyber attacks	Difficulty backing up cloud-based data	Scaling our deployments over time	Reduced data visibility in the cloud	Risk of non-compliance with regulations	There are no concerns

In the context of your industry, which of the following do you see as being the greatest challenges/concerns that exist in relation to cloud-based deployments? [100]

For telecoms and IT software organisations more than most, availability and uptime are essential, and form a central part of exactly what these organisations offer to their customers and end-users. An unreliable telecoms company or IT software provider simply cannot hope to remain competitive in today's market. As such, it's completely understandable that the threat of things such as downtime or a disruptive cyber attack are especially daunting in this industry context.

Part of the reason that this is so important to consider is that cyber attacks are far from uncommon in this industry. Around two fifths (39%) of respondents state that their organisation has been targeted by a cyber attack in the last 12 months – a figure that could quite feasibly be higher in reality. Adding to this, over two in three (68%) surveyed ITDMs admit that their approaches to dealing with such incidents could be improved.

39%
state that their organisation has been targeted by a cyber attack in the last 12 months

68%
admit that their approaches to dealing with such incidents could be improved

This notion is highly troubling. If this is the case, and if availability and uptime are so crucial for this industry, it's surely a must have that organisations have the very best data protection and data management in place. That way, even if they do suffer from some form of downtime or attack, they can get back on their feet and fully recovered as quickly as possible. But is that always the case?

Where organisations can improve in terms of data protection and data management

For many telecoms and IT software organisations, the simple answer is "no" – they do not have sufficient infrastructure in place as far as their data protection and data management is concerned. And that's a real problem.

Data backups

There is a very clear recognition amongst surveyed ITDMs of the value that data backups hold. While almost all respondents acknowledge backups as being at least somewhat important, many go much further.

The vast majority state that it is absolutely essential or very important that their organisation can backup all types of workload (mission critical or otherwise) equally effectively (93%), have automatic creation of backups (85%), have a consolidated solution that backs up across on-premises and cloud (82%), and store backups across different locations (78%). It sounds a lot, but this is the standard that backups must achieve if they are to be considered truly valuable for organisations.

Areas considered essential or very important for data backups

93%
Being able to backup all types of workloads equally effectively

85%
Workloads being discovered and backups being created automatically

82%
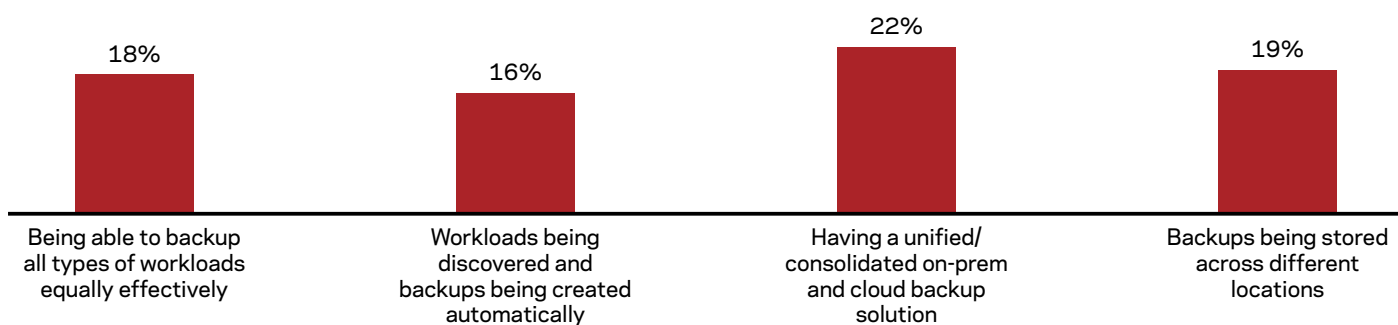Having a unified/ consolidated on-prem and cloud backup solution

78%
Backups being stored across different locations

Showing the proportion of respondents that consider the above to be "Absolutely essential" or "Very important" in terms of data backups [100]

The issue is, however, that it is only around one in five respondents that have confidence in their existing infrastructure – across any number of vendors or solutions that may be being utilised in unison – to be able to deliver on these backup elements. For example, only 22% agree that their organisation has a consolidated backup solution for both on-premises and cloud backups.

"No improvements needed - our current infrastructure already enables this"

18%	16%	22%	19%
Being able to backup all types of workloads equally effectively	Workloads being discovered and backups being created automatically	Having a unified/ consolidated on-prem and cloud backup solution	Backups being stored across different locations

Showing the proportion of respondents that believe their organisation does not need to improve and can already achieve the above with their existing data backup infrastructure [100]

Meanwhile, there's also work to do in terms of organisations' approaches to backups for cloud-based critical workloads. Around one in ten (9%) still use a manual process (e.g. manually copying backups to their data centre) as part of this, which could mean trouble both from an operational efficiency standpoint as well as a data management and security standpoint.

Elsewhere, approaching half (44%) state that their cloud service provider is left to arrange backups for these workloads without any form of intervention. While this is fine in theory, the reality for many organisations is that they could be making a sizable assumption here – do they know for certain that their cloud provider is in fact ensuring that backups take place? There's a degree of risk that goes with this approach which organisations should not be taking. If disaster strikes and organisations are left without appropriate backups for important workloads, it's the organisation that will face the consequences, not the cloud provider.

Organisations should make sure that they are backing up their data in a way that is comprehensive, automated and workable for both on-premises and cloud-based deployments. Doing this will help enable fast and effective recovery if a disruptive incident occurs.

Visibility

Another area where many telecoms and IT software organisations must improve is visibility. With their existing tools and processes in mind, only around one in four (27%) respondents would consider their organisation to have full visibility over their unstructured data. For those without complete visibility, they face a clear and concerning risk to their regulatory compliance. The time, money and effort involved in ensuring a high level of visibility will be more than worthwhile if it means that organisations can avoid significant disciplinary fines, particularly in a time when budgets are so stretched.

Only 27%
believe that their organisation has full visibility with regards to compliance and regulatory requirements of their unstructured data

Organisations must explore ways to achieve full and thorough visibility of their data, with unification of data management and data protection vendors being a clear way that they can better achieve this.

Scalability

Another key area for improvement – and one which applies particularly pertinently to this industry – is scalability. We know that there is a steady upward trend expected in terms of organisations' cloud utilisation in the coming years, while it is also common knowledge that the volume of data being managed by organisations in general is increasing over time. Within this, telecoms and IT software organisations will regularly be faced with fluctuations in demand and usage by their customers and end-users by nature of the services that they provide.

However, while almost all (98%) respondents say that their organisation is able to scale cloud backups and disaster recovery along with growing cloud deployments, over eight in ten (83%) highlight that this could be easier for their organisation. In addition, around two thirds (65%) recognise scaling of data protection and data management solutions as a big challenge for the next five years, while a similar proportion (59%) acknowledge that an inability to scale cloud deployments effectively is something that will hold an organisation back.

65%

believe that scaling their data protection/management solutions is a big challenge for the next five years

59%

agree that an inability to scale cloud deployments effectively will hold organisations back

Scaling something as vital as backups or cloud deployments should not need to be a difficult task for organisations' IT departments. However, as it stands, it seemingly is in many cases.

> Most organisations would clearly benefit from a solution which is fully scalable in terms of data protection and management, and they should therefore explore the available data management options which can facilitate this.

Availability

As previously noted, availability of cloud-based applications and services is essential for telecoms and IT software organisations. Downtime or a lack of reliable service can easily turn the most loyal of customers into a frustrated detractor.

And yet, worryingly, only around four in ten respondents' organisations ensure automatic failover (42%) and/or eliminate single points of failure (40%) as part of their availability strategy for cloud-based workloads. Even fewer (23%) implement geographic redundancy. Without improvements in these areas, organisations are missing out on clear opportunities to further shore up their resilience and maximise the availability that can be offered to customers.
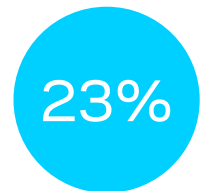
Methods to ensure availabilty of cloud-based software, applications and services for customers
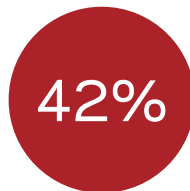
42%
Ensure automatic failover

40%
Eliminate single points of failure

23%
Implement geographic redundancy

How does your organisation ensure that availability for cloud-based software/applications/services offered to your customers is maintained? [100]

Using multiple vendors

Likely to be a key factor causing organisations to need improvement in many of these areas is their use of multiple vendors – something that approaching three in four (72%) are currently doing as part of their data protection infrastructure. In reality, this approach can easily result in a heightened degree of risk and complexity in terms of backing up data, maintaining data visibility, scaling operations and ensuring availability.
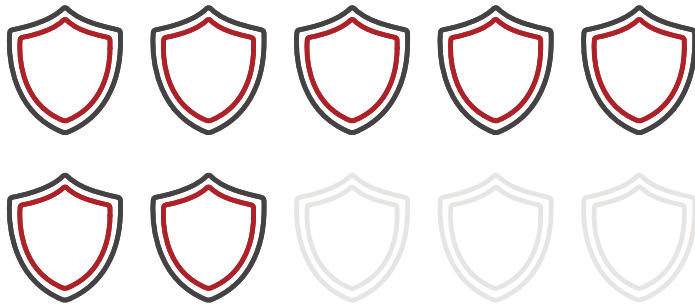
72%

are utilising multiple different vendors or solutions in unison within their data protection infrastructure

Conclusion

While cloud uptake continues to rise, data volumes continue to grow, and the consequences of downtime are more severe than ever before. Telecoms and IT software organisations are up against a huge challenge as they seek to reinforce their data management and data protection.

The opportunities to thrive that cloud deployments provide are plentiful, and wider cloud utilisation can of course bring countless benefits to organisations, despite the ongoing apprehensions that many IT decision makers have about cloud deployments when thinking about things such as security.

Improvements are needed before organisations can truly embrace the benefits of cloud without fear. Backups, visibility, scalability and availability are all crucial areas where – whether in the context of cloud or otherwise – organisations could and should be doing more.

As part of their data protection and data management, the majority of organisations are still utilising multiple vendors and solutions. This is an approach which could quite feasibly be adding to the complexity and bringing further challenges with it.

Organisations that are able to work with a single vendor for their infrastructure where possible will likely be in a stronger position when it comes to simplifying their data protection and management. This will not only enable them to improve in these individual areas in isolation but will help them to strengthen their infrastructure in general. If it's not possible to use a single vendor, they should utilise an application or platform that is able to monitor across their multi-vendor data protection and management infrastructure and report back on this via a single pane of glass .

In doing the above, they will be much better equipped for embracing cloud deployments and the wealth of benefits that they can bring, rather than seeing it as a cause for concern or apprehension.
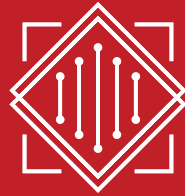
VERITAS™

ENTERPRISE DATA SERVICES
P L A T F O R M

AVAILABILITY   **PROTECTION**   **INSIGHTS**

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds. Learn more at http://www.veritas.com

ABOUT VANSON BOURNE

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

METHODOLOGY

Veritas commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 100 UK and Ireland IT decision makers were interviewed in July and August 2020. Respondents were from **telecoms and IT software** organisations with at least 500 employees. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.