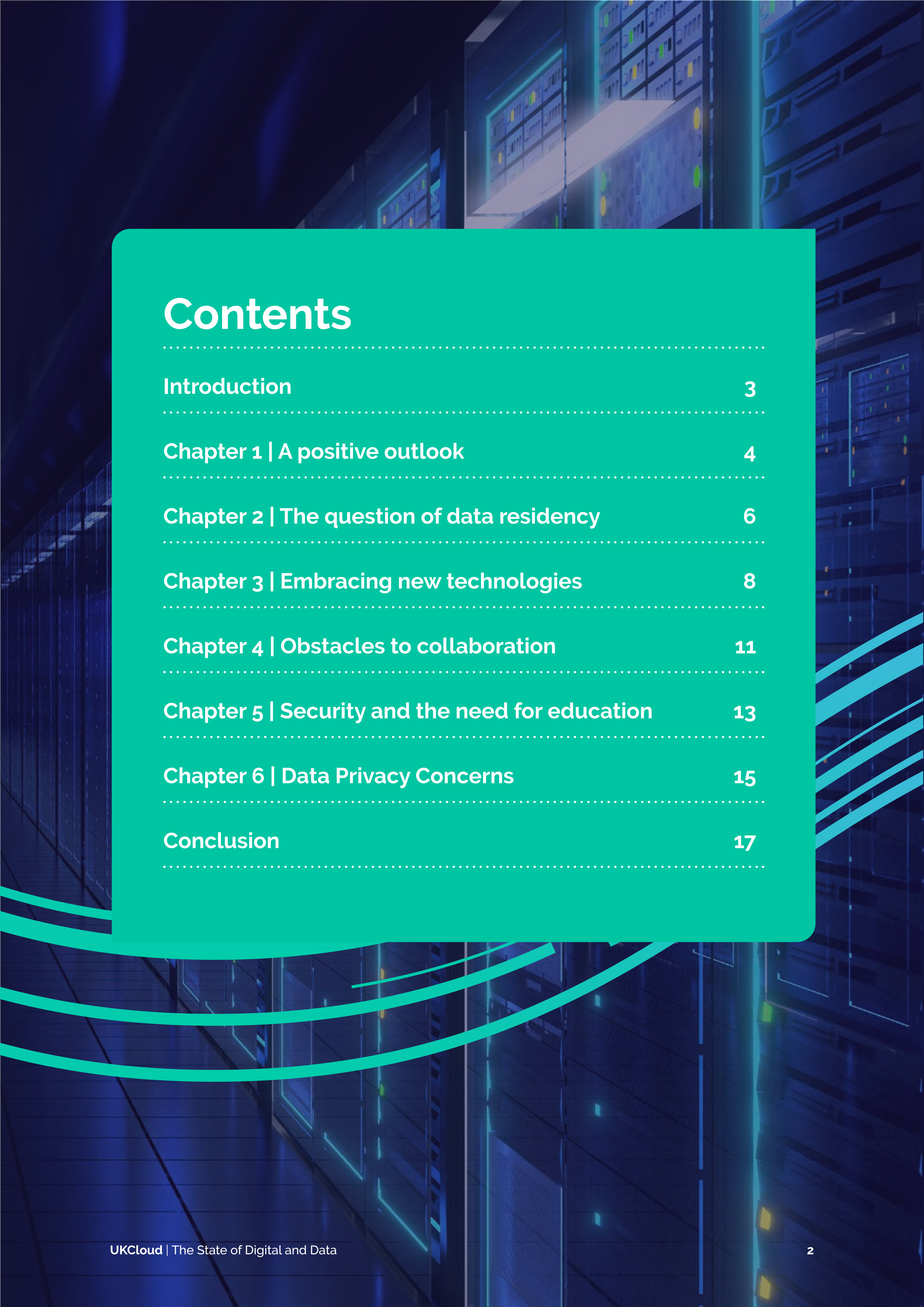
The State of Digital and Data Report

2021

ukcloud

ukcloud health

ukcloud X



Contents

Introduction

In UKCloud's report, The State of Cloud Adoption – UK Public Sector, CEO Simon Hansford stated the data public services held should be treated as a national asset.

When that report was published in early 2020, we had no idea just how invaluable the data underpinning our digital services would become, as the impact of COVID-19 forced organisations in both the public and private sectors to accelerate their digital transformation efforts.

Since the beginning of the pandemic, we've seen a renewed focus from organisations not only on investing in new technologies, but also in building the digital skills and foundations needed to unlock greater value from their data. Indeed, the Government's National Data Strategy describes how the UK's response to the coronavirus pandemic has powerfully illustrated the potential benefits of data. The picture wouldn't be accurate without recognising the success of the NHS, a national asset in itself, as an exemplar in harnessing data for social good through the intelligent use of its own, to make informed decisions that profoundly impact society.

It's clear the shift to remote working, too, has highlighted the need for secure and efficient data access to ensure teams can continue to collaborate despite the distance between them. The traditional office setting has been left behind in 2020, opening the eyes of many to the benefits of digital. Our latest survey carried out in February 2021 and consisting of more than 300 public sector organisations, large and small, reveals a widespread interest in new technological innovations across the public sector, and an overwhelming confidence from IT leaders that their teams have the skills necessary to unlock the value of their organisation's data in line with the core pillars of the National Data Strategy.

There are still issues, of course. The move to remote working has created its own set of particular challenges, and concerns remain about the security and sovereignty of public sector data, especially when it's held in infrastructure owned by the Big Tech players. What's more, reports from the likes of think-tank The Institute for Government[1] – and even from the UK Government[2] itself – highlight a disconnect between the beliefs of some public sector organisations around the digital skills they think they possess, and what they actually do. All the signs point to a digital skills gap in the UK

Overall, though, it's pleasing to see that 62 percent of our survey respondents recognise that harnessing data to its full value when collaborating is essential to providing better services, and more than a third (35%) are using it to power IoT and AI-driven applications. The survey demonstrates that everyone in the public sector is now thinking about new technologies that will unlock ever greater value from the data they hold – something that UKCloud is eminently qualified to facilitate.

This report presents the key findings from the survey, along with contributions and insights from various experts.

1. Institute for Government: Whitehall Monitor 2021
2. House of Commons Public Accounts Committee: Specialist skills in the civil service

Chapter 1

A positive outlook

97%

Almost all (97%) public sector organisations are evaluating new technologies

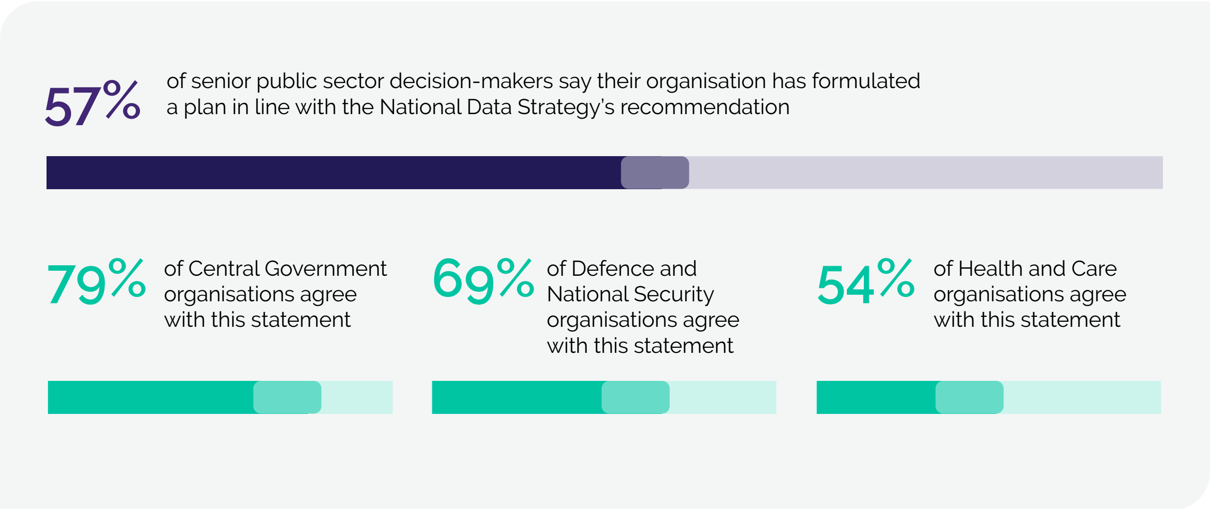
1 | A positive outlook

There is clearly a hunger for new technologies within the public sector. According to the survey, most organisations are, at the very least, evaluating or experimenting with the use of new technologies such as IoT, artificial intelligence (AI), or machine learning, to drive more value from their data. More than a third (35%) are already using such technologies consistently across their organisation, while almost half of those surveyed (47%) use them in specific systems. This is very promising – that fact that public sector organisations are at least thinking about adopting new technologies suggests a desire from the industry to improve the services being delivered to citizens.

This desire is reflected, too, in levels of alignment with the National Data Strategy. Overall, 57 percent of senior public sector decision-makers say their organisation has formulated a plan in line with the Strategy's recommendations, although this alignment does vary from one organisation type to another. Seventy-nine percent of Central Government organisations agree with this statement, for instance, with 69 percent of Defence and National Security, and only 54 percent of Health and Care organisations saying the same.

In accordance with the Strategy's core pillars, almost nine-in-10 (88%) believe that their data is fit for purpose, recorded consistently, and on easily accessible IT systems. A similar number (90%) say they have the skills and experience to unlock the value of their data/use data to drive efficiency; 87 percent agree their staff and partners can access all the data they need, when they need it, from wherever the need it; and 85 percent are confident that data is used responsibly, in a way that is lawful, secure, fair, and ethical.

Finally, in a market dominated by Big Tech, it was encouraging to see over half of those surveyed (55%) say that their organisation recognised the social value benefits of using specialist British partners to help it safely adopt new digital technologies.



57% of senior public sector decision-makers say their organisation has formulated a plan in line with the National Data Strategy's recommendation

79% of Central Government organisations agree with this statement

69% of Defence and National Security organisations agree with this statement

54% of Health and Care organisations agree with this statement

Chapter 2

The question of data residency

Many public sector organisations (40%) lack confidence in their ability to understand where their data is and how it is used

2 | The question of data residency

The survey revealed a wide spectrum when it comes to where data is stored across public sector organisations.

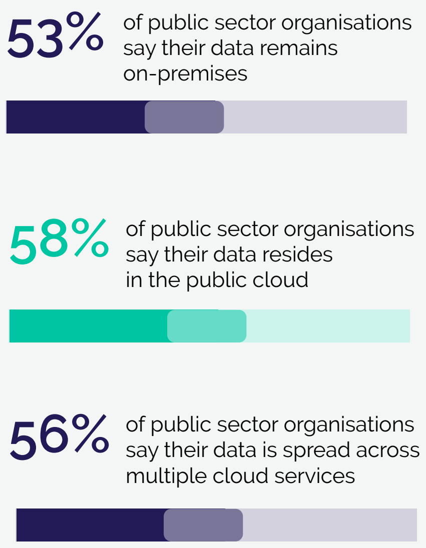
While just over half (53%) say their data remains on-premises – rising to 71 percent within Central Government – 58 percent say their data resides in the public cloud and more in Police and Justice (62%) and Central Government (68%) organisations. 56 percent of respondents (65% within Central Government) told us their organisation's data is spread across multiple cloud services, using different locations for different workloads.

However, there's confusion visible in the responses, suggesting a lack of understanding – organisations don't actually know where their data is, they just think they do. It's impossible for the majority of an organisation's data to reside across public, private and multiple cloud services, which highlights an overall lack of certainty. Public sector organisations are sleep walking into a state where data is actually spread across multiple places and it's been partly driven by a lack of visibility into what is stored on legacy technology, alongside the convenience of Big Tech deployments.

Tending to be cheap and easy to set up, Big Tech deployments bring an allure of convenience and for time-poor teams the idea of a painless transaction frequently wins. Organisations will often prioritise price and ease without giving much consideration to concerns around data sovereignty and security, which leads to an unconscious flow of data out of the nation and into other jurisdictions. What's more, the potential for vendor lock-in is high as such services can be tough to get out of. Think about how difficult it can be to cancel a gym membership or other subscription service, and now consider that it's citizen data which is caught up in the middle. The actual cost of Big Tech deployments to public sector organisations is far greater than the figure displayed in the financials.

To further compound issues, the survey also revealed a lack of knowledge and tools, which could be impacting the delivery of services. With the pandemic requiring people to work from home where possible, 41 percent say their organisation is unable to access all the data it needs to provide the best service. A similar number (40%) admit their teams don't possess the capabilities to understand where their data is held, and how it's currently being used.

Given the damage that a data breach can cause – especially to sectors such as Healthcare and Police and Justice – these findings are concerning. Data should be treated as a national asset. When organisations – and those within them charged with managing that data – aren't sure where it resides, its security is in question and its value to an organisation significantly diminished. Harnessing data to its full potential, and delivering the best possible services to citizens, depends on organisations knowing where that data is, and how it's being used at any given time.



53% of public sector organisations say their data remains on-premises

58% of public sector organisations say their data resides in the public cloud

56% of public sector organisations say their data is spread across multiple cloud services

Chapter 3

Embracing new technologies

The past 12 months have put enormous strain on the delivery of public services. With the outlook for funding more challenging than ever, identifying better ways to allocate scarce resources and improve outcomes is critical.

Thankfully, public sector organisations are owners of a vast, untapped resource – data. The survey highlights a growing realisation of data's potential and the role cloud and tools like AI have in realising value. Visionary leaders recognise that using sovereign data does not mean compromising personal information. Not all data is equal and often just understanding when and how resources are allocated can lead to cost saving and improved outcomes.

With improvements in digital connectivity and new technology, the public sector has an opportunity to be more proactive in the collection and utilisation of data. Digital Reef are working with local authorities to implement a data-first strategy– implementing digital and physical infrastructure and analytics tools to ensure future service delivery can be informed by data insight.

The past 12 months have highlighted the fragility and inefficiency in our system. At the same time, citizens are increasingly aware of the value of data, making more considered decisions in what they share. If the public sector can demonstrate that data can be used in a socially responsible way, we can all look forward to a more prosperous future.

Adam Poole
Asset & Development Associate Director, Digital Reef

DIGITAL REEF

97%

The majority of public sector organisations (97%) believe in the potential of digital technology to unlock data

3 | Embracing new technologies

The fact that most public sector organisations (97%) are at least evaluating the use of new technologies is incredibly promising. And with six-in-10 (60%) of those surveyed expressing a desire for all their data to run in the cloud, allowing them to benefit from tools like AI, as well as from greater collaboration, security, and resilience, there's clearly an appetite for innovation – something that has been hindered by legacy technology for too long.

Feeding that appetite requires organisations to have the right tools and skills – effectively creating the digital foundation – which they can build upon to increase their knowledge and usage of those technologies. Sixty percent of respondents would agree, believing that improving timely access to better data and AI will enable their organisation to use it more effectively and drive better outcomes.

As it stands, there appears to be some way to go before this can become a reality. Only just over half (52%) of respondents say they have the resources necessary to understand and drive efficiencies from the data they own, meaning they can't determine its true value. And two-thirds (67%) of organisations currently allocate no more than a few days each month for employees to innovate and research ways to unlock more value from data, with 89% of leaders admitting they dedicate only 20% of their time to innovating ways to unlock data. This suggests there just isn't enough time for them to discover new ways of working and as a result, they remain tied to legacy systems and processes.

For those that are able to experiment, there is a tendency to leverage large public Cloud Service Providers (CSPs) to support technology adoption. Whilst large, global public CSPs deliver a scalable environment for testing and adopting new technologies, new challenges arise regarding data sovereignty, security, and compliance that can negate any initial benefits they offer.

Moreover, while Big Tech deployments claim to provide a good environment for collaborating on new technology, they can have the adverse effect and see it siloed. Proof of concepts may be prevented from turning into organisation-wide solutions due to a number of reasons, including a lack of connectivity to secure networks, the inability to provide security classification levels, as well as fuelling a concern of spiralling costs due to cloud sprawl that can come with unmanaged cloud usage.

Such an issue raises the question of build vs buy. It's promising that so many public sector organisations are looking to implement innovative technology, but it must be supported by the right environments and expertise to ensure it can ultimately add value and enhance citizen services.

52% of respondents say they have the resources necessary to understand and drive efficiencies from the data they own

67% of organisations currently allocate no more than a few days each month for employees to innovate and research ways to unlock more value from data

89% of leaders admit they dedicate only 20% of their time to innovating ways to unlock data

In the short- to medium-term, for the public sector to more widely – and safely – embrace new technologies, vendors need to shift from simply being software providers to becoming trusted service providers and do some of the heavy lifting themselves. This requires them to take on the responsibility for security, availability, and performance by delivering their specialist software as-a-service, rather than as a stand-alone offering. Then, confident that their providers can manage these aspects on their behalf, public sector organisations will be more able to safely adopt new technologies and begin unlocking the value in their data.

Looking longer term, for organisations to build and evolve their own solutions, they must consider the value of investing in people with the right skills and the best cloud setup to match what's being developed and the data it will process. With an increasing digital skills gap and the urgent agenda to build digital knowledge into communities, organisations should be turning their focus to the social value and innovation that can be achieved from upskilling existing staff.

Chapter 4

Obstacles to collaboration

"Within the field of Artificial Intelligence, the technique of Federated Learning is being used to great effect in regulated industries including Financial Services and Health & Life Sciences, and provides a powerful example of the future of data sharing backed by strong data security & control, and the application of leading edge technologies to provide it.

Federated Learning provides a mechanism for multiple parties to collaborate on the training of a common AI model, in a way that data is kept private from the other contributors. An aggregator node shares a common model with members of a trusted network, whereupon each member re-trains the model using their own private data. Once re-training is complete, any resulting updates to the model parameters are transmitted back to the aggregator where they are combined with updates from the other members of the network, to form a new and improved model for re-distribution.

Cloud provides an ideal and scalable platform to link dispersed collaborating parties, and whilst the private data is not shared between them, it is still necessary to protect the transmitted model parameters against leakage or tampering. To help to achieve this protection, Trusted Execution Environments (TEE) are created using hardware technologies including Intel® Software Guard Extensions (SGX), which uses processor instructions to create enclaves – areas of system memory which are designed to be protected from operating system, virtual machine or hardware-based attack – thus providing confidence in the integrity of the newly optimized model.

Other Intel silicon-level security features support security use cases including Platform Integrity, Data Sovereignty, Threat Detection and more. Talk to your cloud service provider about how these capabilities can help secure your data."

Chris Feltham,
Industry Technical Specialist, Intel

Many public sector organisations (45%) aren't confident they're able to share data for collaboration

4 | Obstacles to collaboration

The third pillar of the National Data Strategy concerns data availability, arguing that for it have the most effective impact, there needs to be "better coordination, access to and sharing of data of appropriate quality between organisations in the public, private and third sectors."

With many of the services delivered by the public sector interconnected in some way, their effectiveness could be enhanced through the sharing of more data both internally and externally. The benefits of "joined up" policing across a nationwide data layer for example, would improve overall oversight and help solve significantly more cases. Greater collaboration between different regional forces and with Home Office databases would significantly increase efficiencies and improve criminal profiling. Healthcare services could benefit too, if they had better access to education or social services data, not to mention patient records held by service providers in other Trusts. Health Minister Matt Hancock has hinted towards plans of a more unified approach – the introduction of a consistent cloud data platform – intended to enhance health service connectivity.

But, while 62 percent of respondents agree that being able to use data to its full value when collaborating internally and externally is essential to providing better services, and 87 percent agree that their organisation is in line with the NDS pillar on availability, other responses suggest a disconnect between what's needed to align on paper and how organisations are actually able to use data for better collaboration.

Forty-five percent of organisations say they're not confident that they can safely and easily share data to effectively collaborate with partners and other agencies, while half say that sharing and collaboration is made difficult by compliance and security restrictions.

The issue is complicated by the fact that living and working under COVID-19 has made collaboration something of a buzzword. Video calling and collaboration apps have become pervasive and the "new normal" for remote working. However, organisations must ensure that these new technologies adhere to the security and regulations required of their industry. Given the sudden nature of the COVID-19 pandemic, organisations were thrust into quick-fixes to support remote workers. However, its crucial to understand the underlying infrastructure.

Once again, it comes down to the issues of data residency and security. As we've seen, there's a concerning lack of awareness about exactly where this data is being held. And when you consider the sensitivity of data that might be shared by public sector organisations, ensuring its security should be of paramount importance.

62% of respondents agree that being able to use data to its full value when collaborating internally and externally is essential to providing better services

87% of respondents agree that their organisation is in line with the NDS pillar on availability

45% of organisations say they're not confident that they can safely and easily share data to effectively collaborate with partners and other agencies

Chapter 5

Security and the need for education

> The past year has driven unimaginable change across the public sector. The pandemic has been an unexpected positive force, accelerating public sector digitisation and driving changes in attitudes and behaviours that many would never have thought possible.
>
> What the survey highlights however is the continued tension that exists between cloud adoption and the perception that such adoption leads to an increase in cyber risk. In reality though, these two factors are not inextricably linked. Cloud adoption can positively reduce risk as many of the controls that are baked into a modern cloud platform are more comprehensive and better managed than those in on-premise equivalents. Proportionality is critical as not all data is created equal and risk and impact needs to be seen through this lens as well.
>
> Like it or not, the pandemic has driven employees to be creative in their use of unsanctioned digital technology to get their work done. Public sector organisations must evaluate shadow IT usage post-pandemic and put in place the necessary visibility and control to protect sensitive data, but must do so in a way that ensures that employee workflow is not impacted.
>
> Attitudes towards cloud and cyber security are at in inflexion point in this post pandemic world and maintaining the benefits many have observed in the past 12 months means it is time for organisations to 'lean in' such that these benefits can be sustained and extended in the future.

Mark Jackson,
UK&I National Cybersecurity Officer, Cisco

55%

Not enough organisations (55%) believe public sector data should be protected to a higher standard than commercial data

5 | Security and the need for education

Our reporting findings show that there is a desire from public sector organisations for greater collaboration, but strict data privacy regulation is forcing many to work in silos, unable to share data with other agencies or third parties. As revealed in our 2020 report, Building the Digital Foundations, security concerns mean most public sector workloads take place on-premises rather than in the cloud. So, it's perhaps unsurprising that almost half of the respondents (48%) to our latest survey suggest that concerns around compliance and security risks are hindering their use of digital technologies to derive the best value from data.

There also remains uncertainty around the use of shadow IT and, in particular, the risk it poses. Concerningly, only just over half (54%) acknowledge that an organisation's cyber risk is increased due to the use of unauthorised IT tools, such as out of policy applications, web apps, and messaging tools, suggesting that the use of shadow IT is rife and sensitive data is regularly vulnerable.

The challenge is, employees use the cloud and cloud-based software in their daily lives, so they know how it can benefit not just them in their work lives, but also as citizens through better services. As such, organisations must give them the environment to use them at work, or they increase the likelihood of them getting used without the relevant approvals. Employees don't see the decision as safe versus not safe, but quick versus slow, and it's that lack of security awareness that means even the most sensitive of data will probably be placed at risk.

First, though, there needs to be a change in mindset around the value of the citizen data held within the public sector. The majority (55%) of those surveyed say they believe public sector data should be nurtured and protected to a higher degree than commercial data, but it's a figure that should really be much higher. Also, 43 percent aren't confident that their organisation's data is stored appropriately for its security classification. Education is clearly necessary on why, as a national asset, it's vital that public sector data is kept safe and close to home where it can be protected under the UK's The Data Protection Act, the nation's version of the EU General Data Protection Regulation (GDPR).

"To make the best use of data, we must have a wealth of data skills to draw on. That means delivering the right skills through our education system, but also ensuring that people can continue to develop their data skills they need throughout their lives." National Data Strategy

48% of respondents suggest that concerns around compliance and security risks are hindering their use of digital technologies to derive the best value from data

55% of respondents say they believe public sector data should be nurtured and protected to a higher degree than commercial data

54% of respondents acknowledge that an organisation's cyber risk is increased due to the use of unauthorised IT tool

43% of respondents aren't confident that their organisation's data is stored appropriately for its security classification

Chapter 6

Data Privacy Concerns

The majority of public sector organisations (53%) are concerned about over-reliance on Big Tech

6 | Data Privacy Concerns

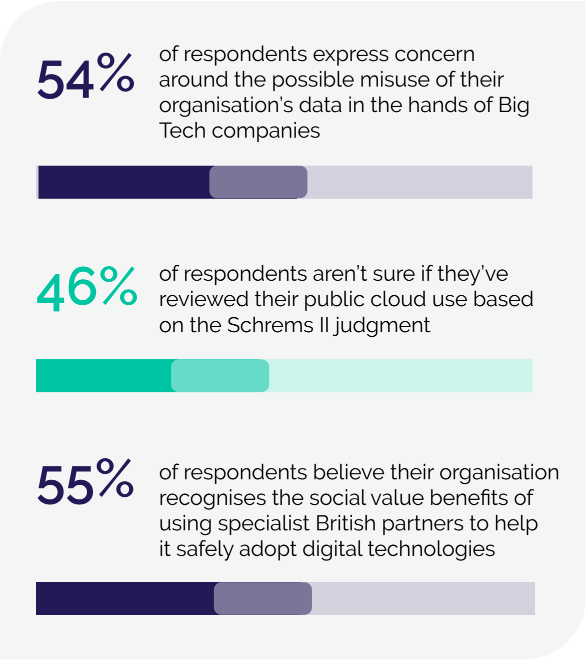
More than half of respondents to the survey (53%) say they have concerns about their organisation's over-reliance on the limited number of global technology providers, rising to 76 percent in Central Government. A similar number (54%) express concern around the possible misuse of their organisation's data. These concerns aren't misplaced. The public repercussions from scandals involving the misuse of data such as Cambridge Analytica have awakened the tech industry and their customers.

What the survey made clear was that there is still a lack of understanding over the amount of data that is reliant on these technology platforms, which is actually a reason for there not being even more concern than what's presented. Some organisations are simply unaware of all the locations where their data may reside.

46 percent of respondents aren't sure if they've reviewed their public cloud use based on the Schrems II judgment. Delivered by the Court of Justice of the European Union (CJEU), it invalidated the EU-US Privacy Shield due to US surveillance programmes. This means that any organisation transferring data to the US can't rely on the shield framework and is responsible for the safeguarding of it. If organisations don't know how much data is going to Big Tech, they're not protecting it.

More education is needed on the implications of using Big Tech infrastructure and the alternatives available. It makes more sense for public sector organisations to seek out and support the many UK-based providers of specialist IaaS, PaaS and SaaS based cloud solutions, with experience of delivering public services, that can offer the right mixture of cloud technology at the right classification level for that organisation, while keeping data on these shores.

Positively, there is movement towards this being the industry approach reflecting policy movement, with over half (55%) believing their organisation recognises the social value benefits of using specialist British partners to help it safely adopt digital technologies, but there is some way to go.



54% of respondents express concern around the possible misuse of their organisation's data in the hands of Big Tech companies

46% of respondents aren't sure if they've reviewed their public cloud use based on the Schrems II judgment

55% of respondents believe their organisation recognises the social value benefits of using specialist British partners to help it safely adopt digital technologies

Conclusion

This survey of more than 300 respondents across UK public sector, healthcare and defence, provides much needed insight as to the sector's ability to adopt digital technologies to maximise the value of the rich data that is prevalent across public sector.

It is encouraging that the vast majority of those surveyed report that they are actively evaluating the use of digital technologies. Combine that with the fact that two-thirds of those surveyed believe that better use of their data is key to delivering better services, and there is clear evidence that the sector is keen to respond to the National Data Strategy and similar initiatives (such as Matt Hancock's call for a Consistent Cloud Platform).

These results echo our findings from the 2020 State of Cloud Adoption survey — clear ambition thwarted by a variety of sector specific challenges which UKCloud and other public sector focused solution providers are ideally poised to help organisations with.

More than
300
respondents

1. Strategise

Although 97% of those surveyed are evaluating digital technologies, almost half have not yet formulated a strategy aligned to the National Data Strategy. If your organisation is in this category, your first step is to commission a Data Assessment from UKCloud so that we can help you understand what data you have, where it sits and what you might be able to do with it. We will help you formalise your strategy and ensure that you're addressing each of the aspects highlighted by the National Data Strategy.

2. Mitigate

40% of respondents lack confidence in their ability to understand where their data is, and most of those surveyed have conflicting views as to whether most of their data is on-premises or in the public cloud. It's essential that organisations establish a strong foundation - and that starts with getting the basics right. Part of that is the formalisation of a strategy but it is also important to ensure that you're able to mitigate risks to security (e.g. cyber monitoring), resilience (e.g. disaster recovery), availability (e.g. up-to-date systems) and compliance (e.g. GDPR) - all areas which UKCloud and our specialist partners can help you with. We call this 'Building your Digital Foundation'.

3. Innovate

The survey found that the majority of organisations look at cloud as an enabler to benefit from digital technologies like AI as well as improved collaboration, security and resilience. However, two-thirds of organisations allocate no more than a few days a month for innovation and research. This is a clear challenge that specialist public sector solution providers, like UKCloud, can help with.

We devote most of our resources to continually improving the services we provide and so we make it much easier for public sector to 'buy' into our innovation rather than having to build it themselves. This also has immense social value benefits (job creation, skills development, UK tax receipts) which is formalised by the Crown Commercial Service and recognised by the majority of those surveyed.

4. Collaborate

Almost two-thirds of those surveyed recognise that being able to use data to its full value when collaborating internally and externally is essential to providing better services, but nearly half are not confident that they can safely and easily share data to effectively collaborate. Part of the problem is that some data and systems have not yet been digitised.

UKCloud has more than 300 specialist partners that can help, whether that's digital evidence, electronic patient records or secure collaborative working environments. These partners are able to rapidly demonstrate their value, and can lead you through the transformation from legacy to digital. And for those systems that can't be easily replaced, UKCloud offers a choice of technologies, connected to a variety of networks and available at multiple classification levels that makes it viable for you to simply 'lift-and-shift' systems into our secure cloud.

5. Protect / Educate

Given that just over half of those surveyed believe that public sector data should be protected to a higher standard than commercial data, it is concerning that a significant minority do not share this belief. Indeed, a similar proportion are not aware of the increased cyber risks of using unauthorised 'shadow IT' and a similar proportion again are not confident that their organisation's data is storage appropriately for its security classification. UKCloud uniquely provide cloud platforms at multiple classification levels and connected to secure government networks like HSCN and RLI.

Leighton James
Chief Technology Officer,
UKCloud

ukcloud

Additional information about UKCloud can be found at
www.ukcloud.com or by following us on Twitter at @ukcloudltd

web: www.ukcloud.com | **email:** info@ukcloud.com | **tel:** 01252 303 300