People, Data and Technology: Unlocking 'Digital Advantage' in Government

Digital Intelligence

BAE SYSTEMS

Introduction

Chapter One: The importance of public trust

Organisations of all shapes, sizes and sectors now see the effective use of digital technologies as a critical driver of innovation, productivity and efficacy. However, those in "high-trust" industries like government have an added challenge: they must be responsible custodians of citizens' data even as they look for innovative new ways to use it to advance society and the economy.

As our Digital Strategy Director James Hatch says: "These organisations cannot risk failing in the way a start-up can; the cost would be too great, impacting security at both a national and international level. Society fundamentally needs, and expects, to be able to trust these organisations."

This is no mean feat. Our research reveals that 85% of digital transformation decision makers across government believe it's "critical" or "very important" that they are trusted by society.[i] Yet, they also handle some of the country's most sensitive and secret data to deliver critical services and safeguard democracy. The stakes couldn't be higher for ensuring that this data is handled securely, legally and ethically – because any digital initiative which fails to gain public support could end up wasting increasingly limited public funds and in turn, damage trust.

Under lock and key

Exactly what kind of data are we talking about? All (100%) respondents to our survey say they work with:

Official data – including information that is sensitive and must not be shared freely

Official sensitive data – where loss or disclosure would have damaging consequences for the government, or cause significant distress for an individual or group of people

Secret and top-secret data – highly sensitive information relating to defence, diplomacy or national security

It's clear that such information would be a valuable commodity for financially motivated cybercrime groups and state actors alike. Accidental leaks such as a Cabinet Office breach of the New Year's Honours List recipients' addresses[ii] do nothing to reassure the public that their personal data is in safe hands. In fact, nearly two-thirds (61%) of Europeans are concerned that their personal information may not be securely stored by public sector authorities.[iii]

Some 59% of government respondents believe data breaches are the biggest current threat facing their organisation. So having a strong data security strategy in place would seem to be key to cementing public trust in digital transformation initiatives – especially as digital investments such as cloud migration add complexity and expand the potential cyber-attack surface.

Chapter Two: Digital transformation is a priority, but strategy concerns persist

The government is committed to driving digital advantage. Some 80% of respondents claim it's "crucial" or "very important" to their organisation. Among other things, they see it as a way to drive efficiency, improve citizen services and enable easy access to such services through digital channels.

The need to accelerate such initiatives has become even more critical due to global factors such as climate change (63%), COVID (52%) and Brexit (46%). In a world characterised by rising costs, flatlining growth, increasing uncertainty, and a need for health and energy security, governments must be nimble and resourceful in how they use digital systems and data.

Fail in these efforts, and digital experts believe that the government will be unable to solve key challenges within society (54%) and unable to share data-driven insights effectively and securely across the organisation or other sectors (65%). Worse, they warn of disconnected services (59%), slower innovation (54%) and an increased threat from adversaries (52%).

Looking for the right strategy

The British Government released an updated National Data Strategy in December 2020, promising an "unashamedly pro-tech" approach to drive digital advantage.[iv] However, over two-fifths (41%) of the government decision makers we spoke to maintain that the biggest barrier to gaining such an advantage is the lack of a clear digital transformation strategy. Budget constraints (48%) and slow adoption of new technologies (43%) are also cited as challenges.

A parliamentary report issued in December 2021 echoes some of these sentiments.[v] It argues that too few government leaders have sufficient knowledge to drive projects, that there's no clear plan to modernise legacy systems and that many departments fail to understand "real digital transformation." This might explain why only 11% of the government digital leaders we surveyed claim to be "completely mature" in making full use of digital technology and data.

Chapter Three: Data, trust and delivering innovation

Innovation is a frequently cited goal of digital transformation. But it is also one that's often misunderstood by those hoping to achieve it. Nearly all (96%) of the government digital decision makers we spoke to say they believe that either a complete overhaul (33%) or some kind of improvement (63%) is needed to deliver an innovation-centric organisation.

The seemingly rapid advances made in the metaverse, blockchain and quantum computing technologies might make it appear to government stakeholders like true innovation is way out of reach. But the reality is that transformative change rarely happens overnight. What we're actually seeing is a huge amount of incremental change, happening all over the technology landscape. The most important thing is that any new tech adoption is standards-based and interoperable, so it can "talk" to anything that comes after.

However, it's also true that government has an innovation problem.

The Government Digital Service (GDS) is to be commended for its work in helping to break down these barriers. Collaboration with agile start-ups – for which the UK is now a hotbed – with strategic management, can deliver greater innovation much faster across the breadth of government.

"Governments have traditionally struggled with a lack of digital agility and a large amount of bureaucratic processes that slow down innovation,"

"Disjointed procurement has been another challenge, whereby different departments speak to different people and use different technology which not only slows down innovation, but can also lead to cybersecurity issues."

Sneha Dawda
Research Fellow in Cybersecurity and Cyber Threats
RUSI

Building on a secure foundation

Perhaps one of the biggest hidden barriers to innovation-centric digital transformation is security. Over half (52%) of respondents to our survey claim it's harder to reach digital maturity because the data they are handling is more sensitive than that in commercially focused sectors. This is certainly true in many cases, and as we've discussed, public trust is essential if any projects are to stand a chance of success.

Getting this right will involve not only technology investment and security policy changes, but also a more challenging endeavour: cultural change. All of the government digital leaders we spoke to believe either a "complete overhaul" (24%) or some improvement (76%) is needed to make their organisation more security savvy. Ensuring personal and sensitive information is handled and stored securely and in compliance with strict regulations like the GDPR is a cornerstone of the government's data ethics framework.[vi]

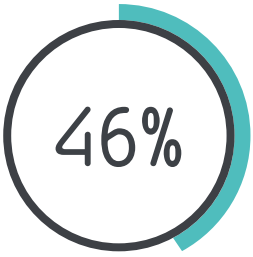
Chapter Four: The skills challenge looms large

It's easy to think of digital transformation as a technology challenge. But even "self-learning" and highly automated AI systems need to be trained and their output interpreted by experienced analysts. In short, government organisations won't be able to gain a digital advantage unless they solve the growing skills shortage.

Our research found the following:

Nearly half of respondents say the government is struggling to become more digitally mature because it's harder to find people with the right skill sets

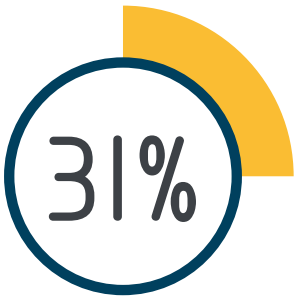
Over two-fifths agree there's a lack of skills to handle official data securely



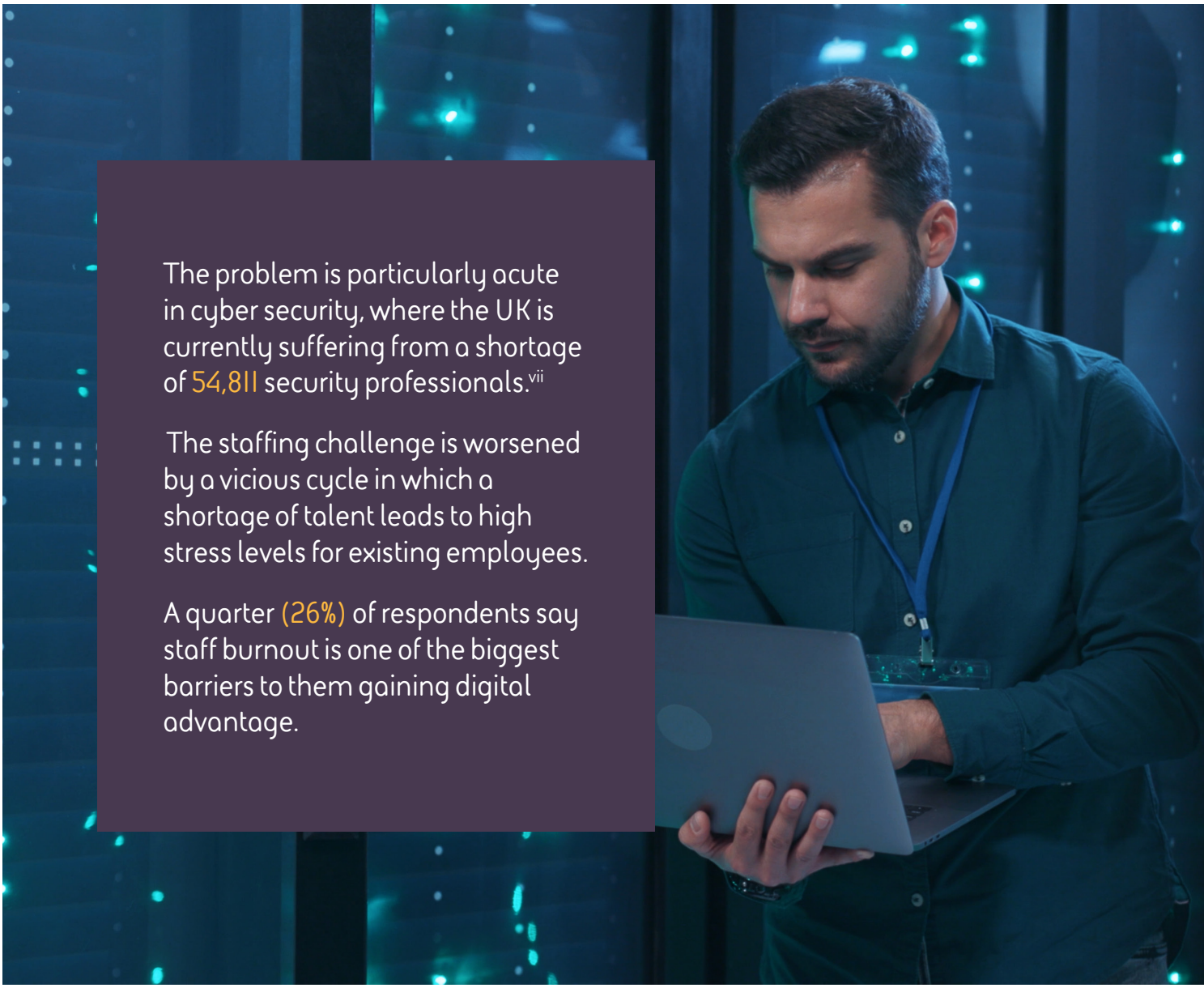
Almost half say they don't have the expertise to undertake and manage data through change

Over a third say attracting STEM talent is a barrier to digital maturity

30% admit that retaining STEM talent is a core challenge



31% say a lack of skills is impacting their ability to implement new technologies like AI, data analytics and security tools



The problem is particularly acute in cyber security, where the UK is currently suffering from a shortage of 54,811 security professionals.[vii]

The staffing challenge is worsened by a vicious cycle in which a shortage of talent leads to high stress levels for existing employees.

A quarter (26%) of respondents say staff burnout is one of the biggest barriers to them gaining digital advantage.

Empower and upskill

Dwindling budgets make it challenging for government recruiters to compete with the private sector for the brightest and best digital talent. Yet, skills gaps can add to critical delays in upgrading legacy systems, while leaving public sector organisations more exposed to cyber risk.

There are two options open to government decision makers: make better use of existing talent, and do more to nurture a long-term pipeline of skilled apprentices and graduates. The second will take years to come to fruition, although there are various schemes underway to help encourage more students into STEM subjects.

In the meantime, government organisations should look at upskilling non-IT employees to help fill strategic gaps. The use of low- and no-code tools could help with this transition, empowering potentially all employees to become "citizen developers".[viii]

Conclusion

Accelerating digital maturity within government

Further investment in hybrid working technology, digital services and improved use of data in the public sector could add £100 billion to UK GDP by 2040, according to one estimate.[ix] It's no wonder respondents to our survey are desperate to accelerate digital maturity. But they also highlight how people, data and technology challenges are proving stubborn roadblocks to progress.

To overcome these, government organisations should focus on several key areas highlighted by respondents:

- Greater cross-sector collaboration with a range of SMEs, to drive innovation and reduce supplier risk
- More intelligent use of data, by breaking down silos across complex ecosystems to improve agility and ultimately benefit society
- Implementing more clearly defined strategies based on making frequent, small changes towards bigger organisational goals – and doing so in a secure and trusted way
- Increased access to STEM talent, by providing a meaningful career path for existing talent and working more closely with the education sector

"Effective use of data is vital for getting digital agility right, which is dependent on providing people with secure access to accurate data in a timely way," concludes James Hatch. "By giving employees visibility into activity across the organisation, they can make informed, data-driven decisions and use intelligence to solve critical problems."

According to our study, 50% of respondents believe their organisation can be "completely mature" in 10 years' time. By putting the right building blocks in place now, they stand a better chance of accelerating that timeframe – in a way that will hopefully benefit the whole of society.

References

[i] https://content.baesystems.com/digital-advantage?

[ii] https://www.theguardian.com/technology/2021/dec/02/cabinet-office-fined-new-year-honours-list-data-breach

[iii] https://www.capgemini.com/wp-content/uploads/2021/10/eGovernment-Benchmark-2021-Insight-Report.pdf

[iv] https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-1-2

[v] https://publications.parliament.uk/pa/cm5802/cmselect/cmpubacc/637/report.html

[vi] https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020#overarching-principles

[vii] https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[viii] https://www.gartner.com/en/information-technology/glossary/citizen-developer

[ix] https://www.virginmediabusiness.co.uk/revolutionise-the-everyday/CEBR-report/

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey, GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey, GU2 7RQ

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/baes_digital

BAE SYSTEMS