BT Means Business

The Cyber Agile Organisation: Public Sector

Transforming security into a platform for resilience and innovation

business.bt.com

Contents

Foreword

Public sector organisations are navigating incalculable opportunities driven by technological advancements. But, they face challenges too. Technical debt is slowing down processes and draining vital resources, while siloed and unstructured data can complicate efficient data access and integration. Additionally, the public sector must compete with the private sector to attract and retain top IT talent.

All this adds to cyber risk in an era when bad actors are upping their game and widening their net to target an ever-greater number of organisations with ever-more sophisticated viruses and scams. Not to mention the very real risk of cyber compromises at the hands of honest and unsuspecting members of the team, who, without proper and regular training can cause security breaches by mistake.

While larger centralised government departments benefit from mature cyber postures and better resources, devolved governments and smaller public sector bodies must rely on agility and innovation to keep pace.

At BT we think it's the perfect time to study and assess organisations that are not only secure, prepared and resilient in the face of cyber attacks, but use this cyber maturity as a bedrock for innovation in service provision. We call these bodies Cyber Agile Organisations.

With money tight across the public sector, there's never been a better time to take a fresh look at approaches to cyber security. It's a process with the potential to answer the riddle of how it's possible to do more with less.

The purpose of our study is to shed light on the key attributes of a Cyber Agile Organisation. By doing so, we aim to provide public sector organisations that have not yet achieved this status with a clear target to strive for, as well as insight into which aspects of their infrastructure, personnel and processes might need improvements.

At BT, our mission is to help public sector partners to innovate with confidence, ensuring their systems are secure, connected and resilient. Want to understand how your organisation can become cyber agile? Then read on.

Tristan Morgan,
Managing Director,
Security, BT

Cyber agility: Leveraging cyber security as a platform for innovation and growth

About the study

The Cyber Agile Organisation is based on an independent opinion research study conducted among 2,500 C-suite leaders across organisations with a minimum turnover of $500 million. Respondents were from organisations across eight markets and eight industries (including the public sector).

Respondents were split into two groups:

- **1,275 IT C-suite technology leaders** (112 from the public sector).
- **1,225 other C-suite leaders,** including Chief Executive Officers, Chief Operating Officers and Chief Compliance Officers (108 from the public sector).

Defining cyber agility

Organisations were scored according to their responses across six dimensions of cyber agility.

The six dimensions of cyber agility:

Awareness

An organisation's understanding of its cyber risk profile, and the various strategies and mitigation measures in place to respond to attacks.

Compliance

An organisation's capacity to comply with cyber security regulations, plus its adoption of voluntary accreditations and standards.

Connectivity

An organisation's visibility and understanding of its IT infrastructure and network, and the safeguards in place to ensure its security.

Strategy

The maturity of an organisation's cyber security strategy and its alignment with broader business goals.

Skills

The security skill sets – both general and specialist – that exist within an organisation, and the approach to organisation-wide cyber security training.

Innovation

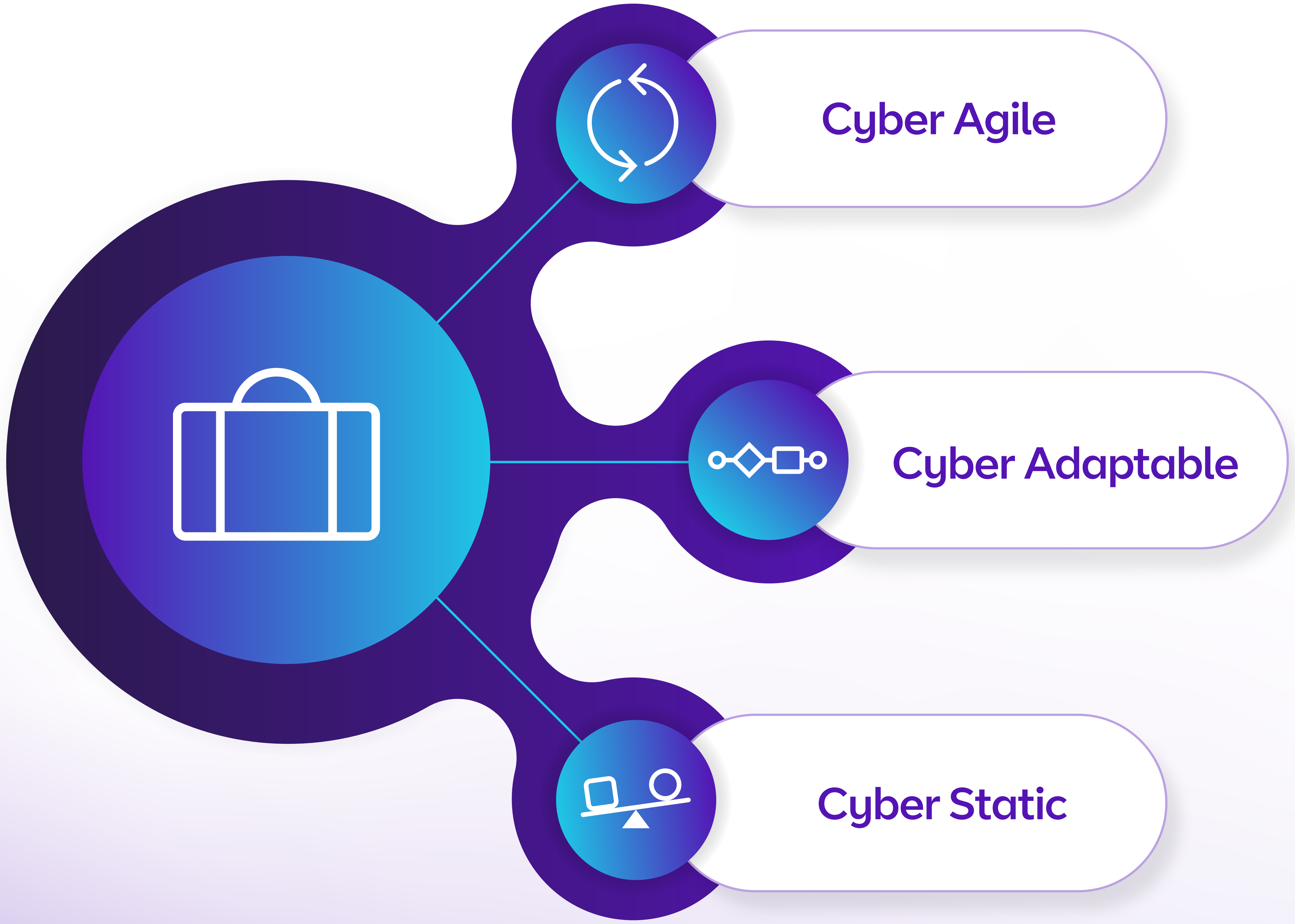
The extent to which cyber security is used as an enabler for innovation and broader organisational transformation.

The cyber agility scoring system

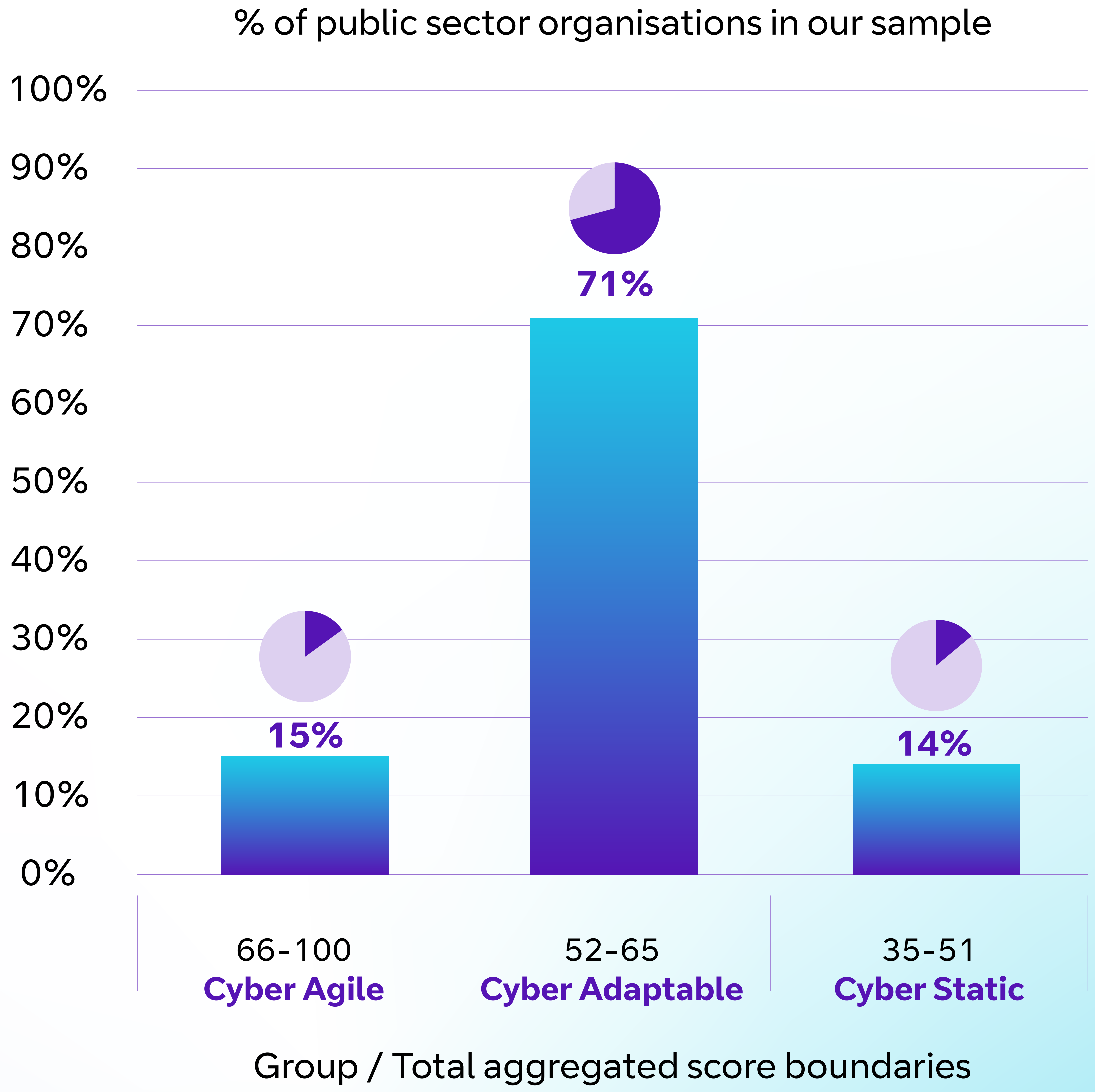
Cyber agility scores were based on performance in the six dimensions: Awareness, Compliance, Connectivity, Strategy, Skills and Innovation. Each dimension comprised a set number of questions from the opinion research which were attributed different weightings. In total, each dimension was valued at 30 points, making 180 the best possible score. These figures were then recalibrated to return final scores out of 100.

More information about The Cyber Agile Organisation methodology can be found here.

Organisations were divided into three groups, based on their aggregated scores:



To qualify as a Cyber Agile Organisation, businesses and public sector bodies had to rank in the top-performing segment for aggregated scores across the six dimensions.



Graph: The cyber agility scoring system

Part 1

The cyber agile advantage

The cyber agile advantage

The first port of call for any organisation is the threat landscape: the who, what, where and why of cyber activity and how it could create a negative impact in a worst-case scenario. For public sector organisations involved in our study, the evidence is strong.

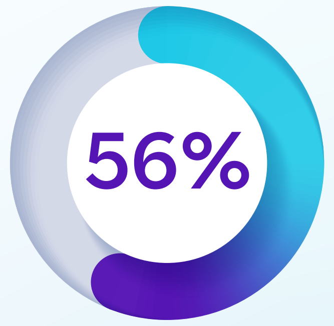
About a third (**33%**) of these bodies say they are experiencing either 'high' or 'very high' cyber attack severity. It seems the situation is set to deteriorate in the near future, with nearly half (**49%**) expecting high or very high severity in the next three years.

These numbers are brought into sharper clarity with the additional finding that **57%** of public sector entities believe a major cyber attack represents the main existential threat to their organisation. In this context, public sector organisations need to find an answer to the question: 'how can we operate with confidence?'.

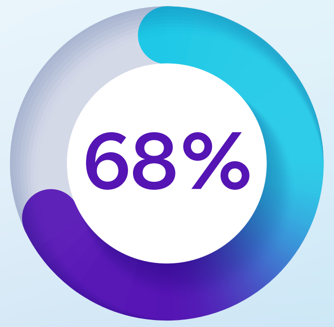
Prepared to protect

With so much activity and the stakes so high, preparation is key. More than half (**56%**) of public sector bodies say they are currently either 'very prepared' or 'extremely prepared' to deal with cyber attacks. And defences are set to strengthen, with more than two-thirds (**68%**) of respondents estimating they will be very or extremely prepared in the next three years.

Of course, this leaves a third (**32%**) of respondents who do not believe they'll reach this level of preparedness in the short- or medium-term future, which is a cause for concern.



56% say they are currently either 'very prepared' or 'extremely prepared' to deal with cyber attacks.



68% estimating they will be very or extremely prepared in the next three years.

Cyber security maturity self-assessment for public sector bodies

Maturity level

Initial implementation

7%

We are in the early stages of developing and implementing a cyber security strategy, with our efforts focused on addressing immediate risks and building foundational security practices.

Enhanced strategy

41%

We have moved past basic implementation and are developing a more structured and proactive cyber security strategy. There is a growing awareness of the importance of cyber security across the organisation.

Integrated and proactive

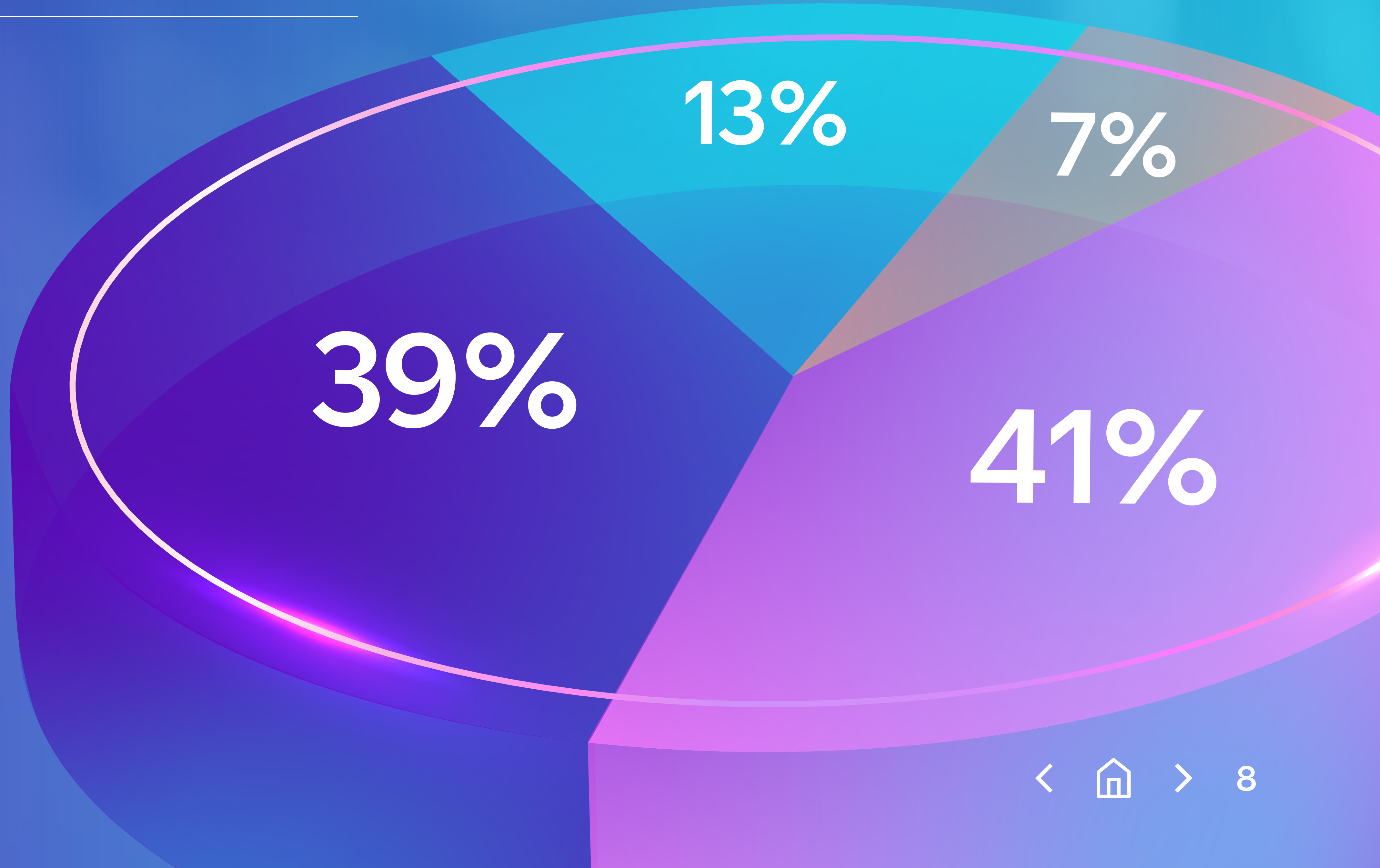
39%

Cyber security is fully integrated into the way we build our products, services and processes within our organisation's operations, with proactive measures in place to prevent, detect and respond to threats.

Strategic and agile

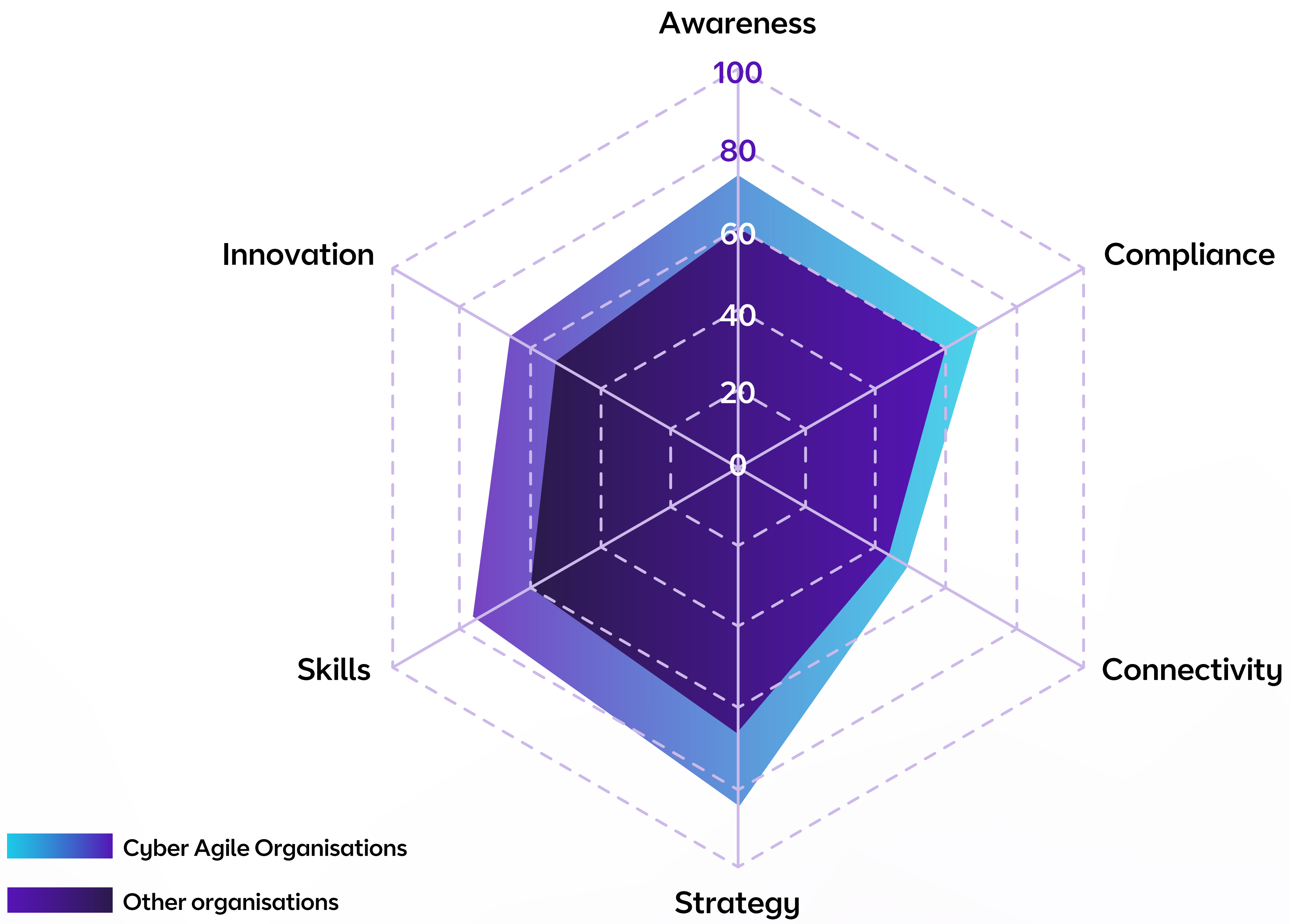
13%

We have a highly mature approach to cyber security that not only safeguards our assets but also drives long-term resilience, cyber agility and supports value creation across the organisation.



The importance of being agile

Average cyber agility scores for public sector bodies.



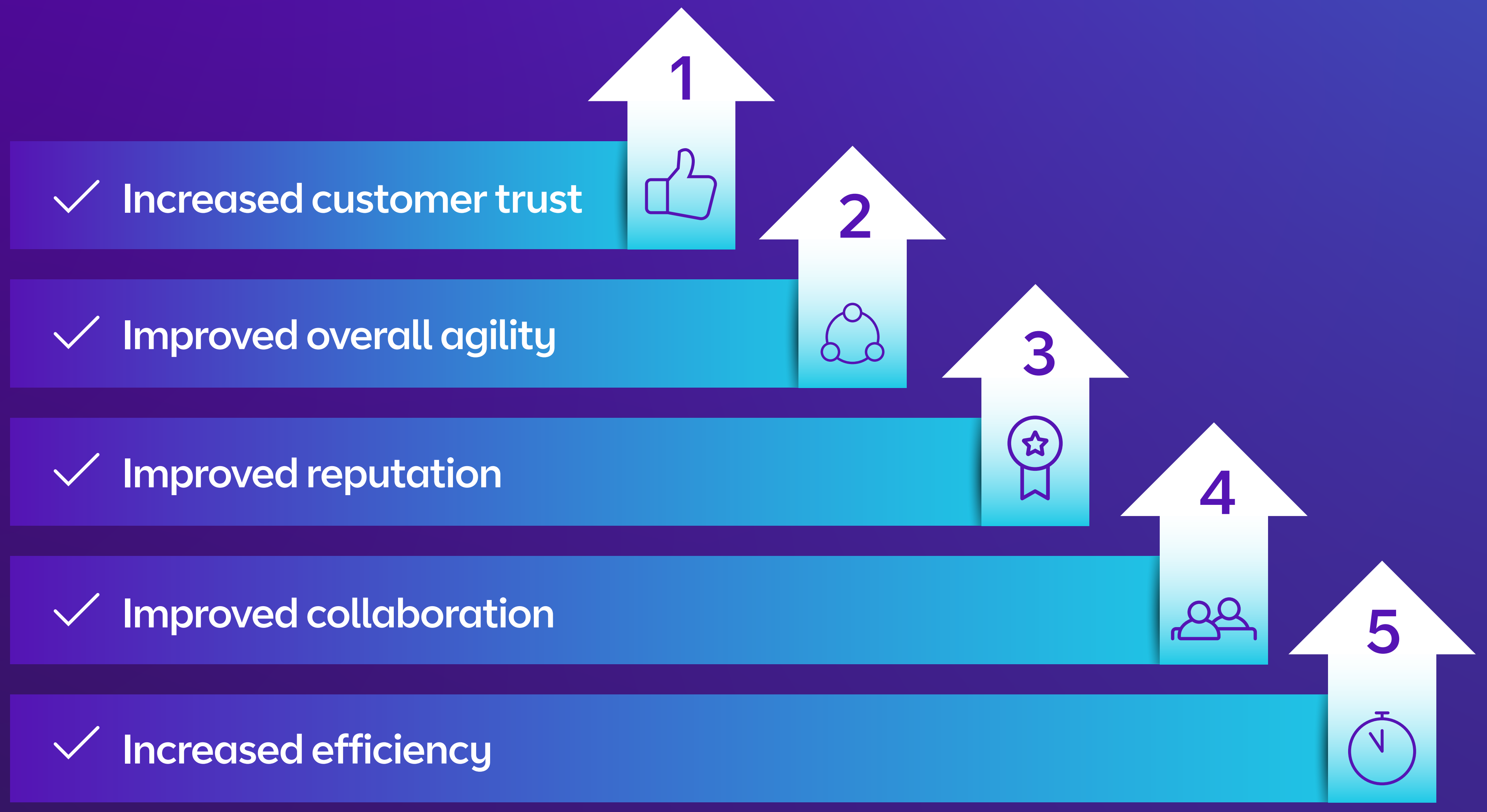
Dimension	Cyber Agile Organisations	Other organisations
Awareness	76	58
Compliance	69	60
Connectivity	48	43
Strategy	81	65
Skills	78	57
Innovation	63	55

Public Sector Cyber Agility: Significant Skills Gap Identified

Of the public sector bodies included in our study, **15%** qualify as Cyber Agile Organisations. The gaps are clear between sector leaders in this field and the rest, particularly within the Awareness, Strategy and Skills dimensions – with the biggest divergence seen in the Skills dimension.

The rewards of cyber agile transcend simply holding back the tide of the hacking community and data breaches. Public sector leaders recognise several significant benefits that improved cyber agility would bring to their organisations, the top five being:

> "For the public sector bodies in our study, rising geopolitical tensions and increasingly sophisticated attack methods make the prospect of a breach a constant concern for Chief Information Security Officers and politicians alike. Building world-class cyber resilience is essential to safeguarding our nation and keeping ahead of our adversaries. This requires the right partnerships and investment, which should be a priority for our government at this time of heightened treats."
>
> **Ed Stainton,**
> Managing Director, Public Sector



1 ✓ Increased customer trust

2 ✓ Improved overall agility

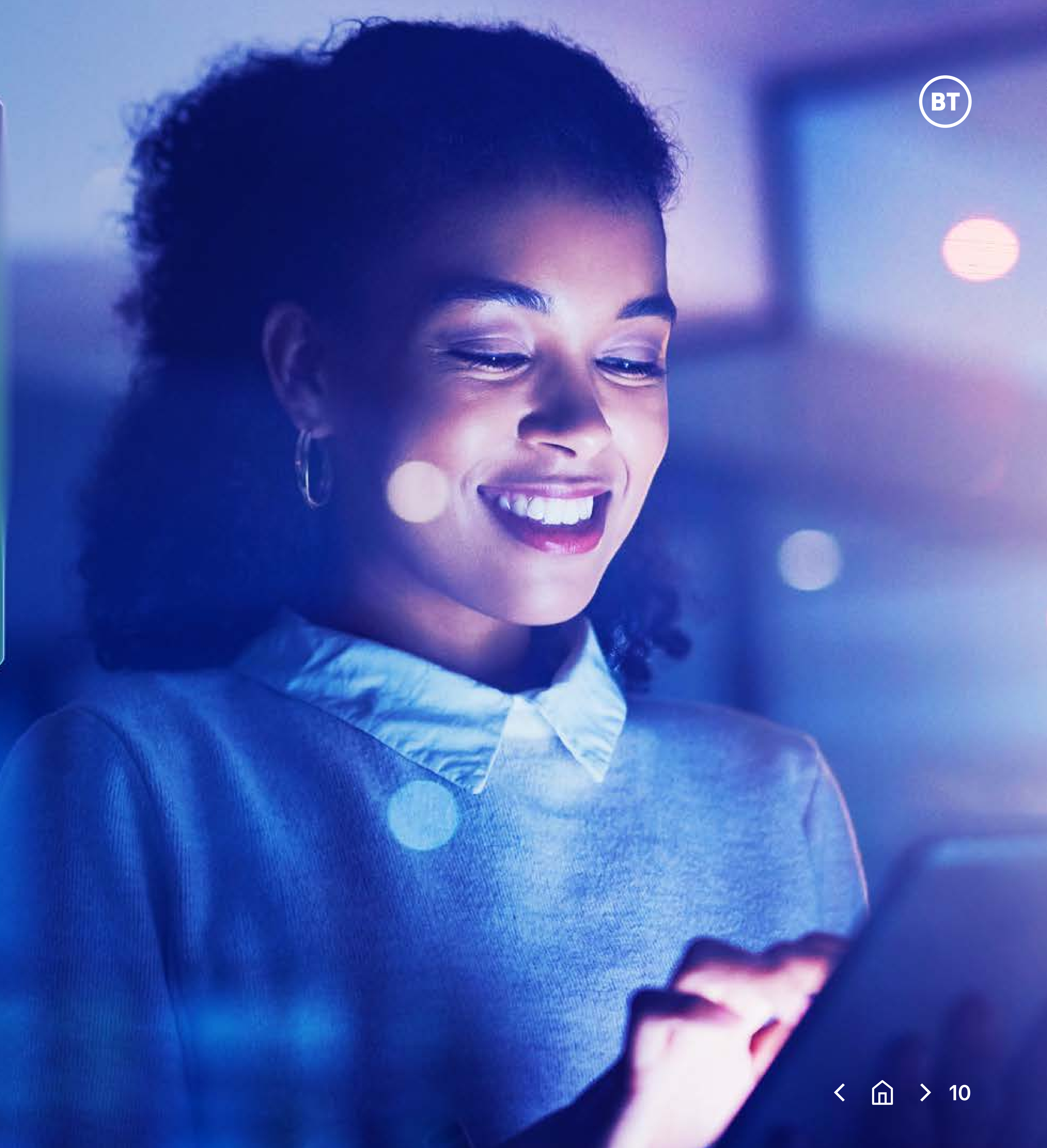
3 ✓ Improved reputation

4 ✓ Improved collaboration

5 ✓ Increased efficiency

Part 2

Becoming cyber agile: Key focus areas for the public sector



Efficient spending and investment challenges in the public sector

With operational funds coming principally from central government, plus government agency grants and local taxes, public sector organisations have a responsibility to spend efficiently, producing a return on investment in the form of brilliant service provision to communities. It's often the case that investing for the long term produces savings later on, but budgetary cycles mean this can be hard to plan for.

Rising cyber security budgets and strategic investment in the public sector

The majority of public sector bodies expect their cyber security budgets to increase in the next three years by an average of 13%. In this sector, perhaps more than any other, organisations need to demonstrate they're allocating investment to the areas that help facilitate service delivery. But they must also ensure to keep on top of evolving cyber security challenges and stay in tune with the fast-paced threat landscape.

Protection:
Driving awareness

As public sector bodies increasingly adopt digital technologies and services, the attack surface for cyber threats is expanding. The growing use of cloud services, the surge in IoT and other connected devices and the prevalence of remote working setups all introduce new vulnerabilities.

Furthermore, as geopolitical tensions spill into cyberspace, individuals and organisations interacting with public sector bodies are increasingly aware of their data within the supply chain. This is making data sovereignty a major factor. CISOs and procurement professionals are scrutinising their suppliers' supply chains more than ever before, with a focus on identifying any single points of failure.

While all the Cyber Agile Organisations in the public sector claim they have 'complete' or 'high' visibility over their supplier base, only **68%** of other organisations say the same, opening the latter group up to potential risks.

Cyber Agile Organisations in the public sector are also faring better overall regarding the resiliency of their IT ecosystem. Some **91%** believe their partners are 'extremely' or 'very' resilient, compared to 68% of other public sector organisations, while their on-premises software is also more likely to be resilient (91% versus 72%).

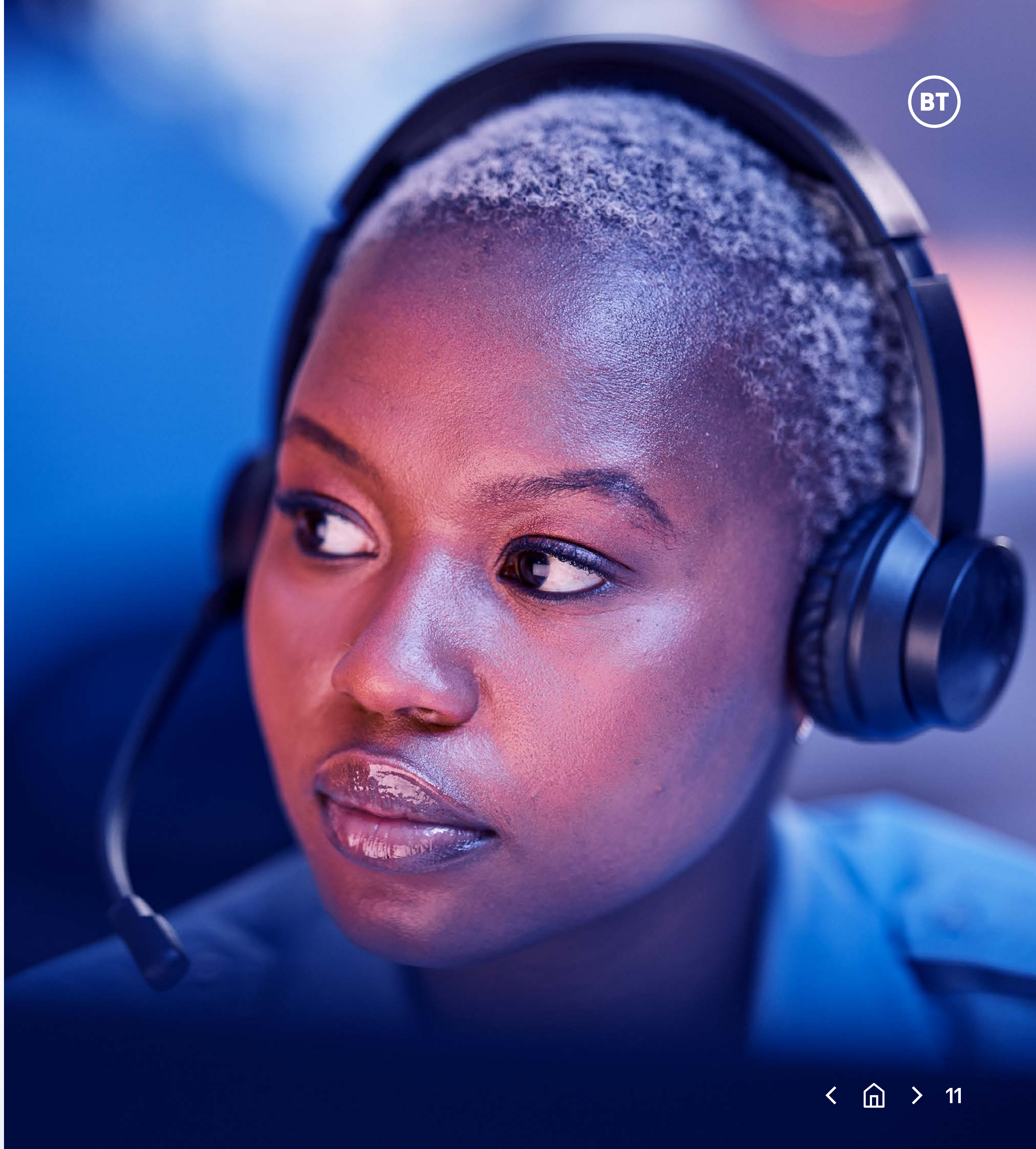
How often organisations review and update their cyber security policies

Cyber Agile Organisations in the Public Sector:

Every 5 Months

Other organisations in the Public Sector:

Every 6 Months



Steps to cyber agility in the Awareness, Compliance and Connectivity dimensions

1

Actionable threat intelligence

Knowing where your data resides and who has access to it along your supply chain is fundamental for identifying and addressing vulnerabilities. This assessment should also encompass cyber security trends beyond your network. Recent regulation has placed an emphasis on securing supply chains and strengthening response processes, both of which require a comprehensive baseline understanding to address effectively.

2

A different view of how your organisation connects

In a world of cloud capability, hybrid working and perimeterless networks, the integrity and confidentiality of your connectivity enables businesses to operate, change and grow. Cyber security approaches and technologies like Zero Trust, endpoint detection and response (EDR), and secure access service edge (SASE) must be deployed, relevant processes layered on top, and all brought together by trained people who can underpin the agile organisation.

3

Blend physical and digital security

Criminals are taking advantage of weaknesses in physical security, such as premises entrance points, to gain access to information which could prove useful in cyber attacks, such as passwords and user data. As a result, security strategies must combine solutions to both physical and digital threats. Companies can start by conducting a comprehensive security audit that evaluates physical access points and digital vulnerabilities and establishing a 'live' threat analysis that tracks key areas of risk.

Performance: Enhancing skills

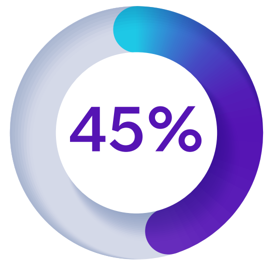
Demonstrating cyber agility goes beyond secure networks, endpoints and compliance; it involves empowering your workforce to defend against cyber threats. The development, retention and incentivisation of skills are critical issues for the public sector, which often struggles to compete with the wider market in the cyber field, frequently losing top talent to the private sector. More than two-thirds (**67%**) of public sector leaders in our study believe human error is the biggest threat to their organisation's cyber security.

Employees are the first line of defence against cyber attacks, so it makes sense that **82%** of Cyber Agile Organisations in the public sector report that they are actively building a cyber security culture, compared to **63%** of other organisations. And **79%** of Cyber Agile Organisations say that every employee within their organisation knows they are responsible for IT security, compared to **59%** of other organisations.

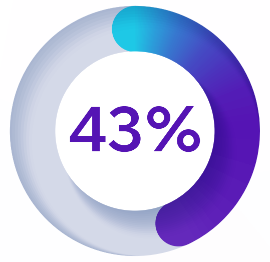
On average, the public sector bodies in our study invested $3.8 million in cyber security training for employees over the last 12 months.

Half of public sector bodies mandate regular cybersecurity training for all employees as part of their professional development. Additionally, **43%** provide role-specific cyber security training for key departments, such as IT and finance. However, only **16%** encourage security teams to acquire professional qualifications and participate in industry events – the lowest proportion across the industries in our study.

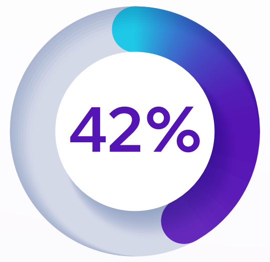
Almost half (48%) of public sector bodies in our study currently have a Chief Information Security Officer in position. And many are actively recruiting for more specialist roles:



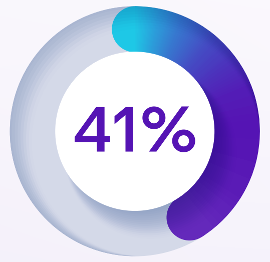
45% are recruiting for a Security Compliance Specialist.



43% are recruiting for a Threat Intelligence Analyst.



42% are recruiting for a Security Operations Centre Analyst.



41% are recruiting for an AI and Machine Learning Security Specialist.

Public sector bodies' five greatest cyber weaknesses

1 Network security practices

2 Device security and safe working

3 Operational technology (OT) security

4 Phishing awareness

5 Incident response procedures

Steps to cyber agility in the Strategy, Skills and Innovation dimensions

1

Communicate clearly

A cyber security strategy can only be strong if it's well communicated. People – especially those outside the IT department – need to understand their part in the strategy. Ensuring clear, concise and accurate communication across all levels of the organisation will help people understand what's expected of them and act accordingly.

2

Sort your legacy tech

Until addressed, legacy tech and technological debt will prohibit an organisation's ability to update systems and adopt agile strategies. Create a transformation plan, revisit, assess and adapt cyber strategies to allow for new and disruptive technology, particularly in fields of artificial intelligence and faster data processing.

3

Enhance flexibility with outsourced solutions

The journey towards cyber agility begins with a skilled security team, but a limited talent pool can make recruitment challenging. Implementing flexible working patterns and launching hiring campaigns targeting a diverse workforce can help address this issue. Additionally, reskilling existing employees and forming industry partnerships will help to build knowledge. Businesses should also consider outsourcing specialist expertise to provide tailored cyber security solutions that can be flexed to meet changing business needs.

UK market spotlight

Three-quarters (**74%**) of UK public sector leaders say their organisation is experiencing more frequent Distributed Denial-of-Service (DDoS) attacks which are increasing IT network downtime. Whether politically motivated or aimed at extortion, these attacks can result in severe disruption to public services, financial costs and theft of highly sensitive data.

Mitigating these increasingly sophisticated attacks will require innovative solutions. Many of the UK public sector entities in our study are implementing cutting-edge solutions to test their network resilience and guard against unauthorised access.

Top three solutions either partially or fully implemented by UK public sector bodies

- Recruiting an ‘ethical’ hacker to test cyber security.
- Identity threat detection and response (ITDR).
- Zero Trust architecture.

However, organisation-wide awareness of and responsibility for cyber security will also be crucial. Just half of UK public sector leaders say that every employee within their organisation knows they are responsible for IT security.

> **‘In this sector, even Cyber Agile Organisations need to pick up the pace and align security strategies to business and governmental objectives, ensuring that cyber and physical security are integrated within the Cyber Agile strategy to address emerging threats’**
>
> **Ed Stainton,**
> Managing Director, Public Sector

UK university and BT

Discover how BT Managed Security Services partnered with a UK university to create a proactive approach to cyber security. By implementing a Security Incident and Event Management Tool (SIEM), the university was able to have insight into its IT environment, enabling protection from potential cyber threats.

Learn more

Conclusion

In a complex world, where opportunities and risks sit side-by-side, cyber agility is the public sector's best defence against bad actors. Cyber Agile Organisations are better prepared for threats; they are increasingly able to fend them off but also to deal with the consequences should an attack prove successful.

Crucially, becoming cyber agile enables public sector bodies to enhance efficiencies and innovate with confidence. When security concerns are minimised and potential risks are well-managed, organisations can optimise people power, deliver on government pledges and improve service delivery across all levels of society.

Now is the time to focus on building cyber resilience and agility within the public sector.

BT's got your back

We have first-hand experience

As one of the most targeted organisations in the world, we understand what it takes to build a resilient business in the face of cyber attacks. Many of the solutions we offer our customers are built with the same technology we use to protect our own organisation. We plough £40m into security innovation each year with our military-grade data security services, trusted to protect nation states, backed by a 3,000-strong dedicated security workforce. And as a national critical infrastructure provider, we're bound by strict government regulations, so you can be sure we have the processes in place to manage governance and compliance.

We're here for you around the clock

BT has over 70 years of experience protecting critical national infrastructure. We are consistently voted as a 'leader' in network and security managed services by Gartner and IDC. We're also a supplier of all the core Crown Commercial Service (CCS) framework agreements, offering you expert support from a dedicated, experienced team.

Our Cyber Security Operations Centres around the globe offer expertise to help customers at every stage of their security journey and ensure they are protected 24/7. Our talented cyber security professionals assess, build and test your defences, to create effective security strategies that are easy to adopt.

We help you unlock the benefits of smarter surveillance

Our end-to-end smart surveillance solutions support national infrastructure, the police, government and local authorities. We keep your people and places secure with digital connectivity, smart cameras, and industrial IoT sensors for comprehensive visualisation and analysis. Working with live data and analysis, we enable more efficient and informed decision making, and better monitor public safety and spaces. AI and data analysis bring better insights, while smart overlays turn your network into a true intelligence provider.

Get the conversation started

Talk to us

Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

© British Telecommunications plc. Registered office: 1 Braham Street, London, E1 8EE.

Registered in England No. 1800000. January 2025.

JN: 1634561879