BT Means Business

The Cyber Agile Organisation:

UK Market

Transforming security into a platform for growth

business.bt.com

Contents

Foreword		3-4
About the study		5
The cyber agility scoring system		6
Part 1:	The cyber agile advantage	7-8
	Cyber security self-assessment	9
	The importance of being agile	10-11
Part 2:	Becoming cyber agile: Key focus areas for UK businesses	12
	Preparedness: Securing connectivity	13-14
	Performance: Driving innovation	15-16
Conclusion		17
BT's got your back		18

Foreword

The UK is a thriving hub of innovation across a broad spectrum of industries, from manufacturing and retail to professional services. The country is a leader in health research and innovation, while its financial services sector completes millions of transactions every day and is easily the largest in Europe. These industries are fuelled by digital technology, the evolution of which continuously unlocks new opportunities for partnerships, service delivery and growth.

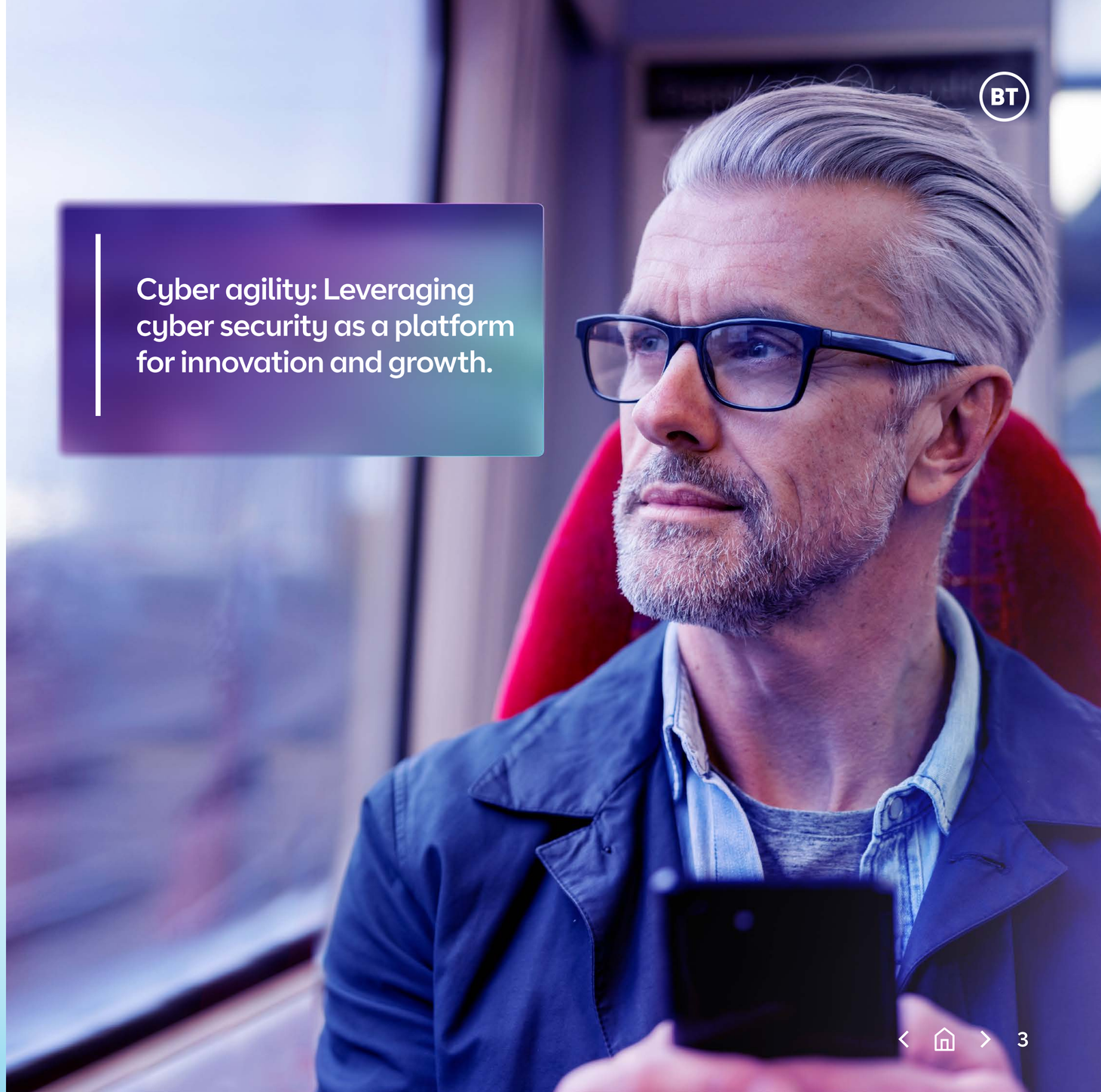
However, as a digitised country with prominent, high-risk and sensitive sectors reliant on information technology and data systems, the UK is an attractive target for cyber criminals and state-sponsored actors alike.

The problem is widespread. Data from BT shows it logs 2,000 cyber attack signals a second, equating to 200 million each day. These attacks target all organisations, including the charity sector and small businesses, but are even more prevalent for larger enterprises – because they are well known, deal with lots of financial transactions and offer a broader attack surface.

The tools and techniques employed by cyber criminals are increasingly sophisticated too, particularly in areas like phishing, ransomware and supply chain vulnerabilities, with criminals using scanning bots to spot weak points in the system. Digital surveillance of UK organisations is growing, with activity by new malicious bots up more than 1,200% between July 2023 and July 2024.

Cyber defence, then, is a national priority, not only to shield UK businesses from the worst impacts of cyber crime, but also to give them the platform they need to grow. Done right, cyber security can be an enabler of innovation and a platform for confident experimentation. Organisations can do deals, commission work and form partnerships, safe in the knowledge that the cyber safety net has been taken care of.

This is the essence of what makes an organisation not just agile, but cyber agile.



Foreword

Cyber agility in the UK

BT forms the backbone of much of the UK's digital infrastructure and protects the country's key assets from a litany of threats. As such, we were interested in the UK landscape for cyber agility and keen to discover what makes organisations perform in this area. In this study, we aim to distil the key elements of what confers cyber agile status upon businesses. This is the who, what, where and how of cyber security, the strategies and the execution that propels them to the head of the pack.

We consider their attitudes, their evaluation of the threat landscape, the maturity of their strategies and the perceived impact of these measures on factors such as client trust, business efficiency and connectivity, all of which pave the way for productive partnerships.

It's an important study for any organisation wanting to understand the DNA of cyber agility in an evolving global economy. It's also your chance to elevate your businesses to the status of a Cyber Agile Organisation and enjoy all the incredible benefits that cyber agility brings.

Tristan Morgan,
Managing Director, Security, BT

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 industries and eight markets (including the UK).

Respondents were split into two groups:

- **1,275 IT C-suite technology leaders** (166 from the UK).
- **1,225 other C-suite leaders**, including Chief Executives, Chief Operating Officers and Chief Compliance Officers (207 from the UK).

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

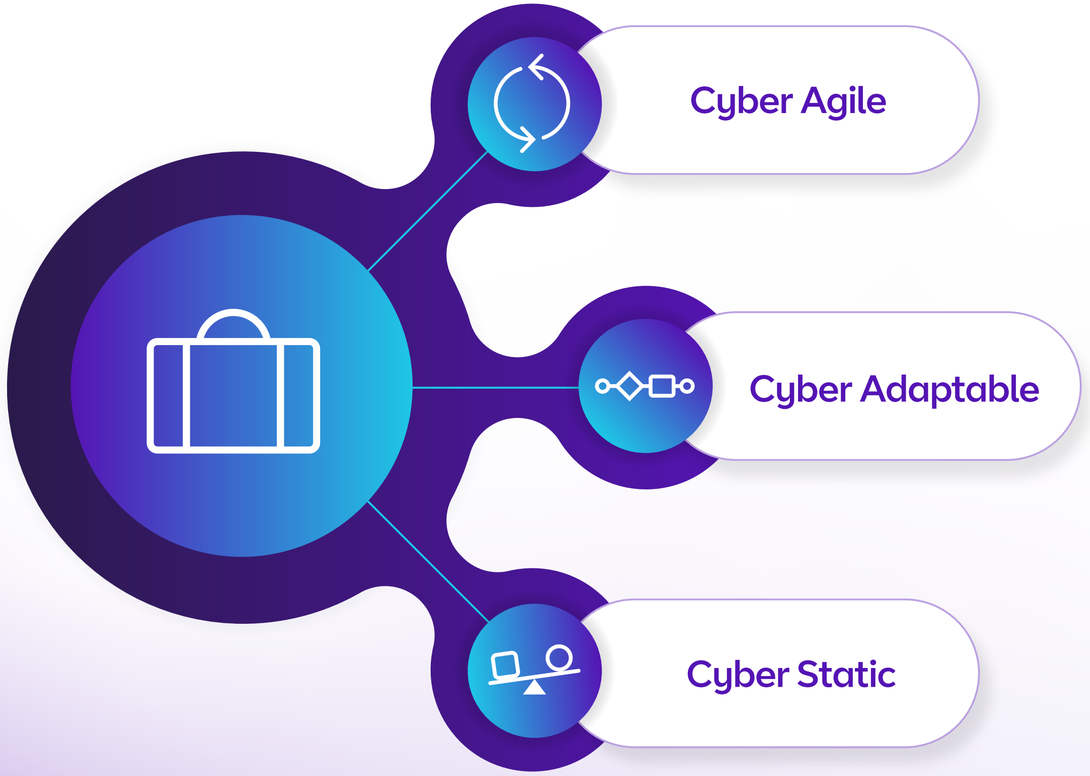
The extent to which cyber security is used as an enabler for innovation and broader organisational transformation.

The cyber agility scoring system

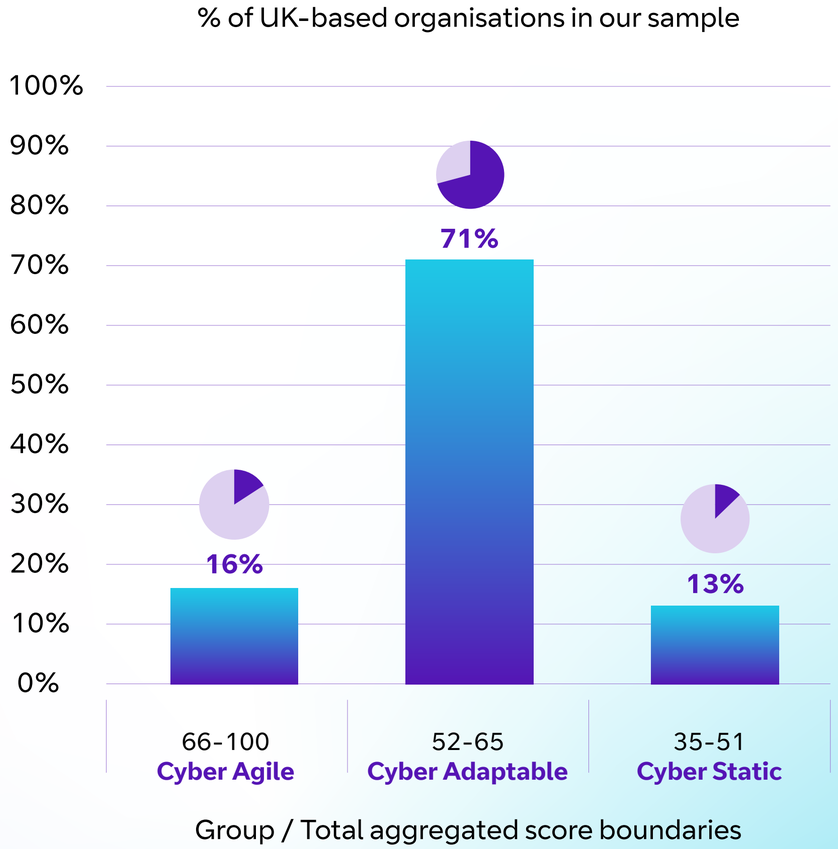
Cyber agility scores were based on performance in the six dimensions: Awareness, Compliance, Connectivity, Strategy, Skills and Innovation. Each dimension comprised a set number of questions from the opinion research which were attributed different weightings. In total, each dimension was valued at 30 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.

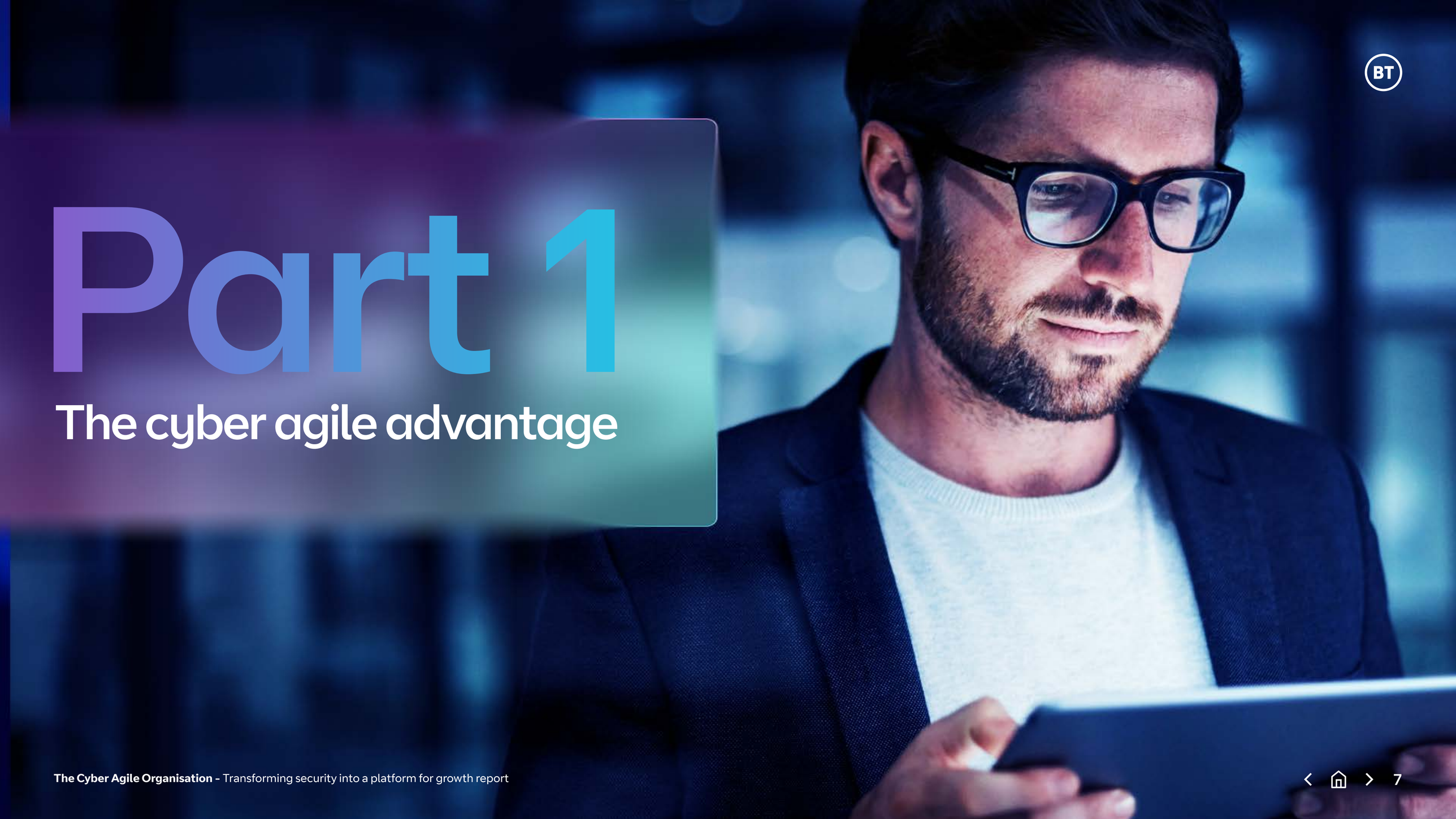
Organisations were divided into three groups, based on their aggregated scores:



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



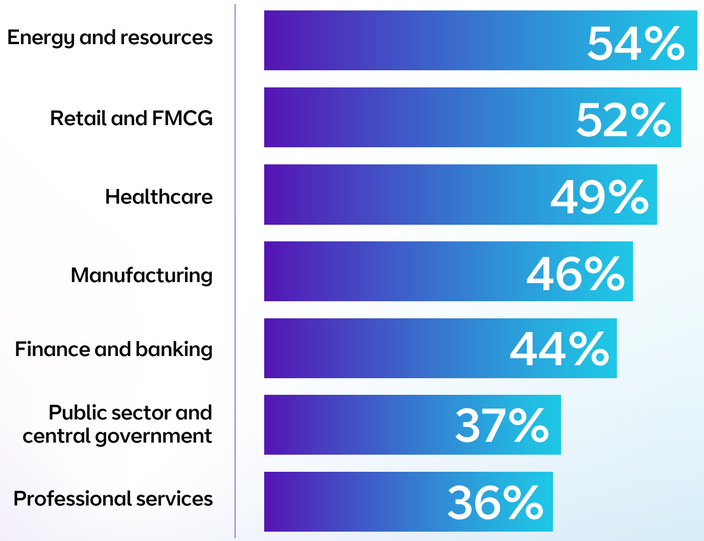
Part 1

The cyber agile advantage

The cyber agile advantage

The UK is a hotbed of cyber activity, both positive and negative. More than a third (34%) of UK-based organisations in our study say they are currently experiencing either 'high' or 'very high' cyber attack severity. The threat is likely to worsen in the near future, with 46% of respondents anticipating that they will experience this level of attack severity in the next three years.

This rising threat is causing sleepless nights for UK business leaders, with **62%** believing that a major cyber attack is the main existential threat to their organisation.



% of organisations that anticipate 'high' or 'very high' levels of attack severity in the next three years

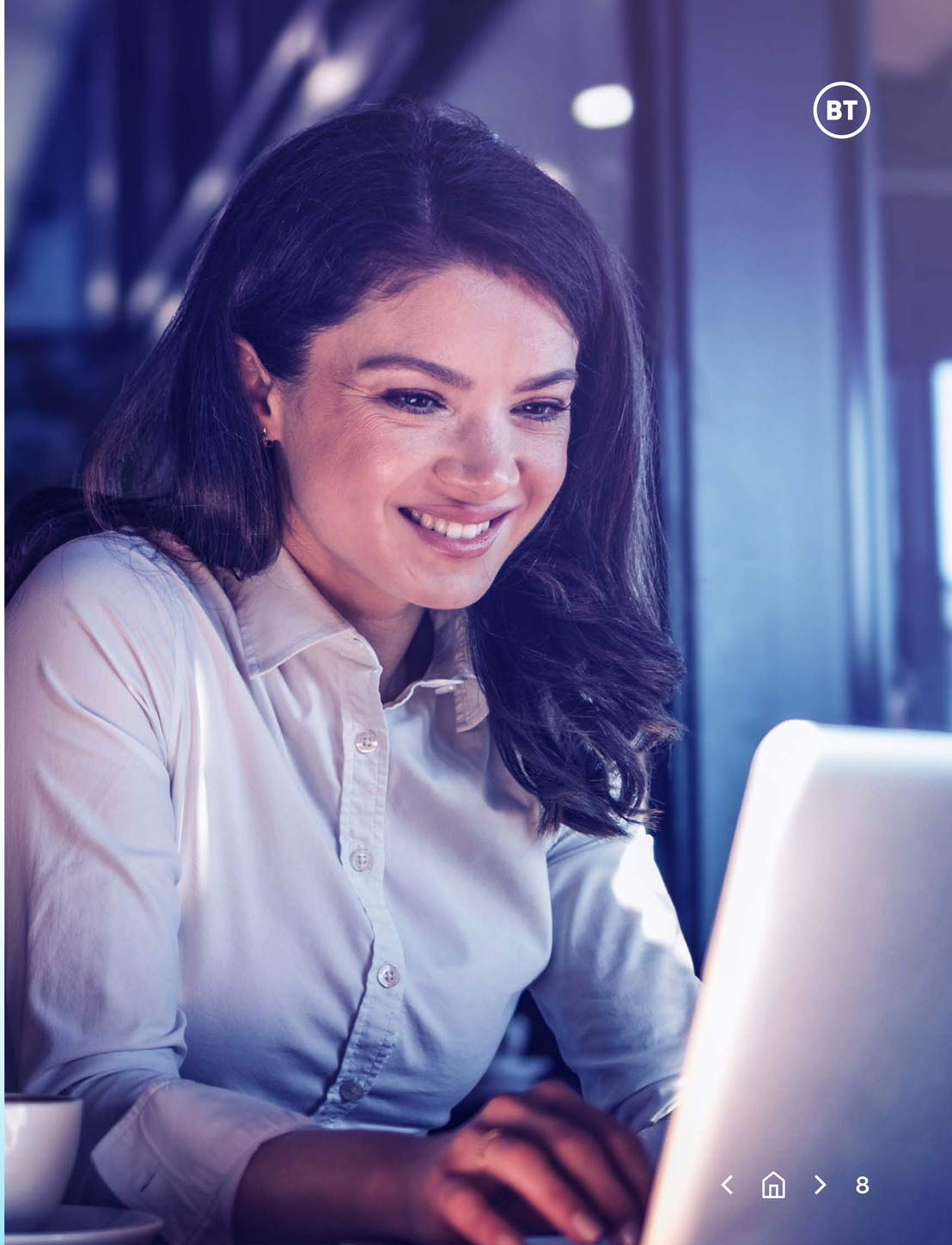
Prepared to protect

While prevention is better than cure, organisations must prepare for the worst. That means not just mitigating threats, but also putting plans in place to get back up and running fast in the case of a successful attack.

Our study indicates that the majority of UK organisations are getting the balance right, with **57%** claiming to be either 'very' or 'extremely' prepared to deal with cyber attacks and **71%** arguing they will be very or extremely prepared within the next three years.

This focus on cyber resilience feeds into fundamental business principles for many, with more than two-thirds **(67%)** of leaders in UK-based organisations considering a secure network to be a prerequisite for doing business.

62% believe that a major cyber attack is the main existential threat to their organisation.



Cyber security self-assessment

Maturity level for UK-based organisations

Initial implementation

5%

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

45%

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

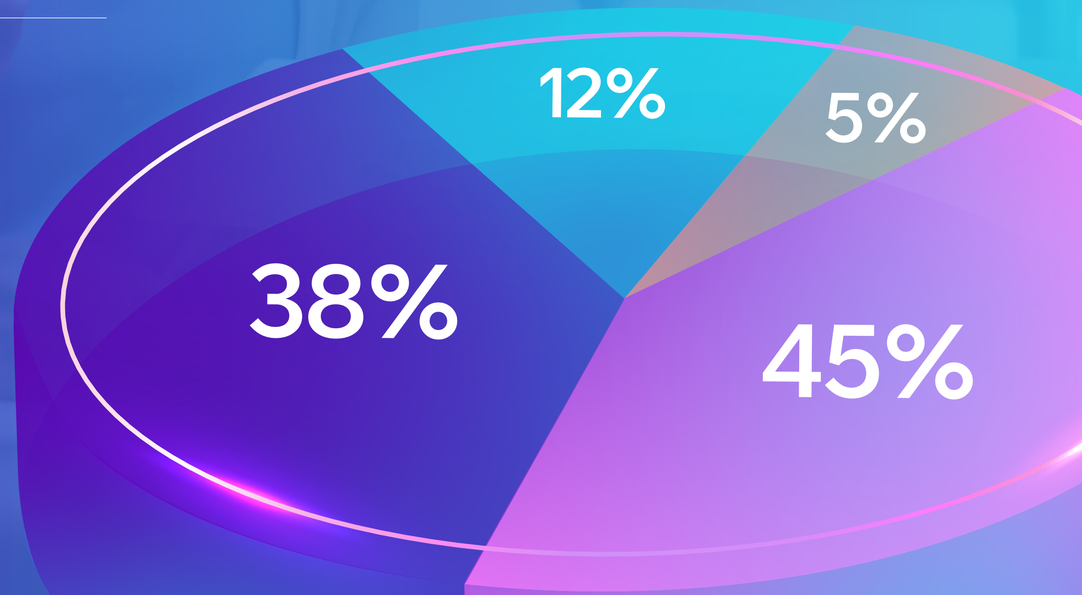
38%

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

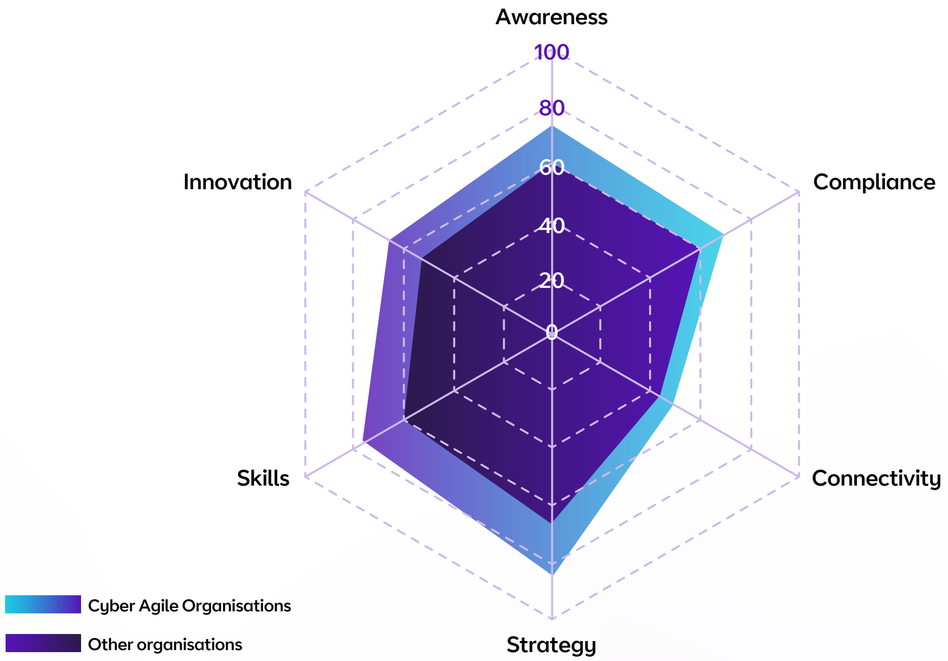
12%

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 UK-based organisations.



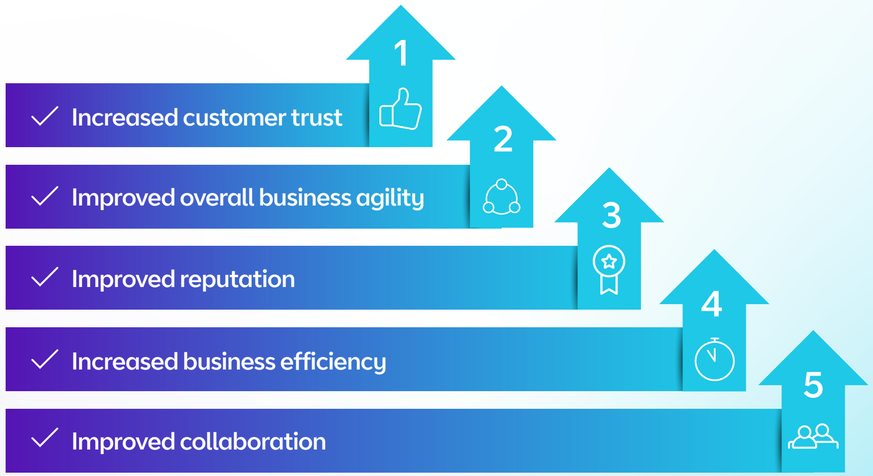
Dimension	Cyber Agile Organisations	Other organisations
Awareness	75	59
Compliance	67	61
Connectivity	48	43
Strategy	89	66
Skills	75	61
Innovation	62	51

Of the UK-based businesses in our study, around one in six **(16%)** qualify as Cyber Agile Organisations. Performance gaps are visible between these organisations and others in the market, particularly within the Awareness, Strategy and Skills dimensions. The biggest gap between the two groups appears in Strategy.

Strong performance across these six dimensions offers business advantages that extend far beyond the server room. Business leaders recognise a range of significant benefits that improved cyber agility would bring to their organisation.

> "Cyber agility isn't just about fending off threats; it's about leveraging a secure IT ecosystem to supercharge business performance. A cyber agile mindset drives quick, confident actions that fuel fast, sustainable growth."
>
> Yasemin Mustafa,
> Cyber Security Product Director, BT

Top five benefits of improved cyber agility.

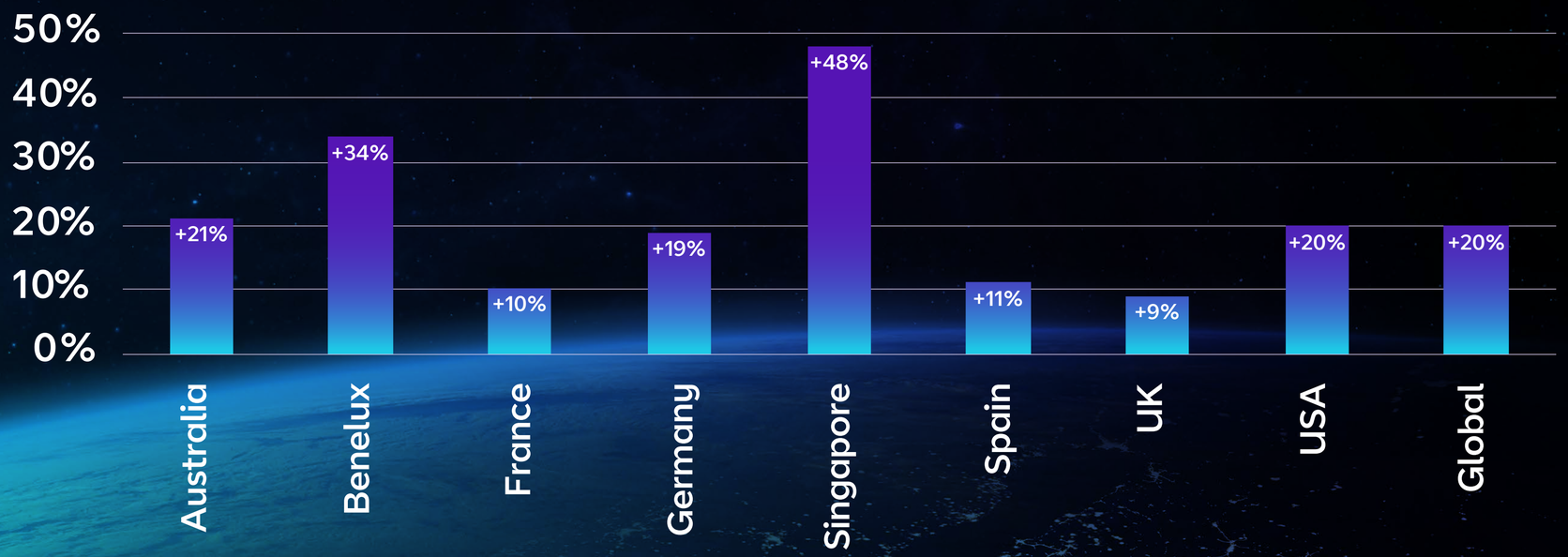


Cyber agility builds businesses

Our research demonstrates the link between cyber agility and business performance. Over the last three years, UK-based Cyber Agile Organisations achieved 9% higher growth rates than other organisations. While this is the smallest growth gap seen among the markets studied, if all other UK businesses matched this growth rate by improving their cyber agility, this could unlock an additional £7 billion in revenue and £3 billion in gross value added (GVA).[1]

[1]Gross value added (GVA) is a measure of economic output calculated as the value that has been added to the goods and services that have been purchased.

Difference in growth rate between Cyber Agile Organisations and other organisations 2021-2023



Graph: Potential economic benefits of cyber agility

Geography	Australia	Benelux	France	Germany	Singapore	Spain	UK	USA	Global
Potential additional revenue (+)	£6bn	£11bn	£6bn	£19bn	£7bn	£3bn	£7bn	£111bn	£169bn
Gross value added	£2bn	£4bn	£3bn	£8bn	£2bn	£1bn	£3bn	£61bn	£83bn

Part 2

Becoming cyber agile: Key focus areas for UK businesses

Cyber Agile Organisations excel in different areas of cyber security best practice, from clear visibility of the technology estate to awareness-building across all levels of the business. Here's how organisations in the UK fared in our study.

Preparedness:
Securing connectivity

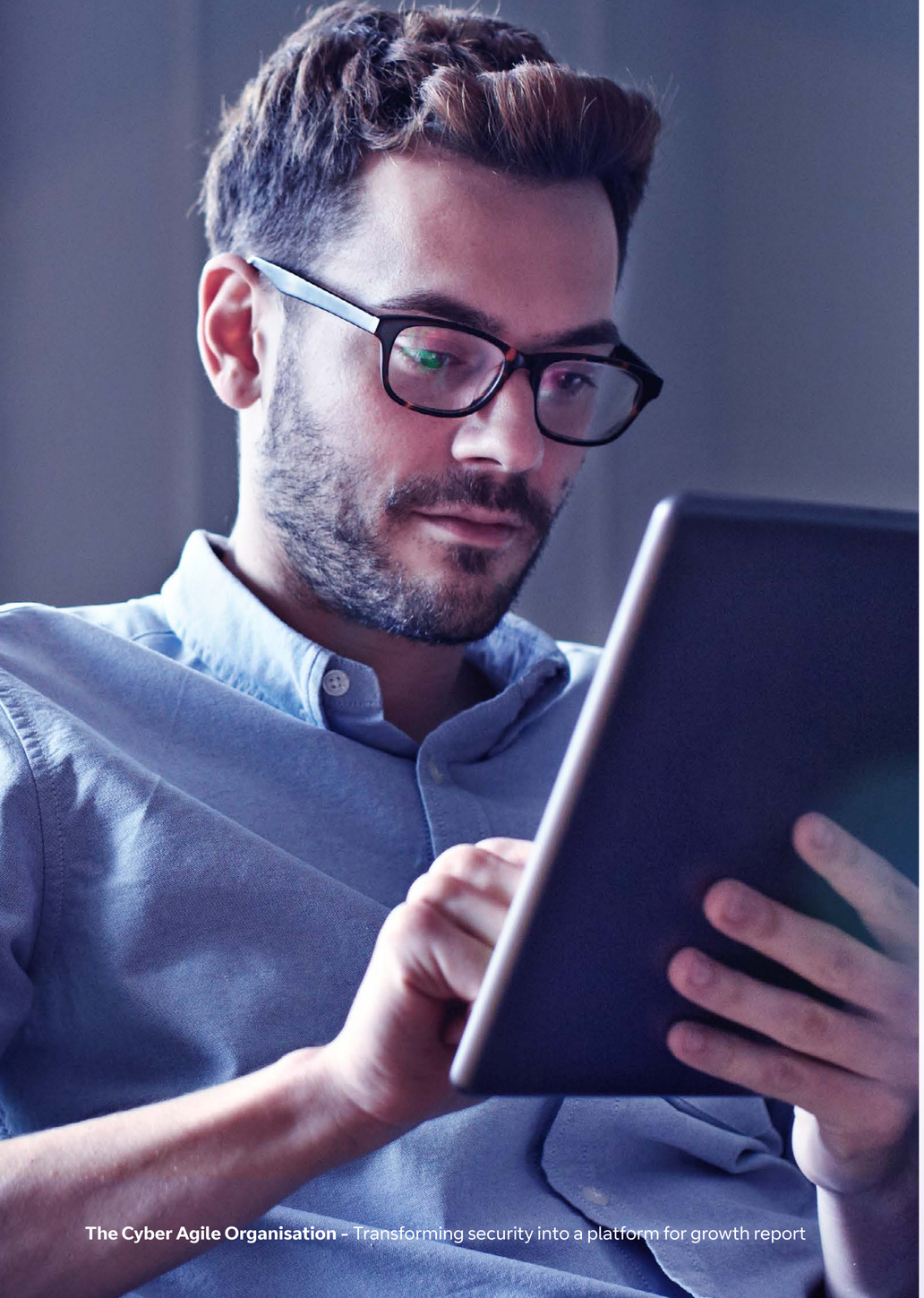
Secure connectivity is pivotal to the efficiency of all business processes, from communication to data management. It grants employees access to the information they need securely and without interruption, enhancing overall productivity.

When it comes to cyber security, information is power. So, it makes sense that nearly three-quarters **(74%)** of Cyber Agile Organisations in the UK market say they have high visibility of their IT infrastructure and network and strong safeguards to keep them secure, compared with just a third **(32%)** of other organisations in the market.

However, the explosion in the number of gadgets feeding into businesses – whether sanctioned or unsanctioned – presents an increasing risk to organisational cyber integrity. And, with more employees working remotely, ensuring the use of secure networks has become increasingly challenging.

Top three connectivity cyber risk factors for UK-based organisations

- Increasing number of devices
- Devices connecting to public wireless networks
- Sanctioned use of personal devices



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

1

Basic cyber hygiene

Ensuring network security involves understanding the personas within your estate (who has access and where) and having a clear inventory of your assets. You should prioritise modern endpoint tooling to make it difficult for threats to move between zones and workloads. Coupled with a systematic approach to threat detection, this strategy will minimise risks and enable faster response times.

2

Strengthen your response

Implement effective incident resolution and recovery processes so that, should the worst happen, your business has a clear plan to get back on track. These processes should not be set in stone; they must be regularly assessed and adapted to mitigate evolving threats.

3

Meet regulatory standards

Keep up to date on the cyber security regulations and frameworks relevant to your industry. Recent regulation has placed an emphasis on securing supply chains and strengthening response processes, both of which require a thorough understanding to address effectively. Staying updated helps ensure compliance and protects against potential breaches.

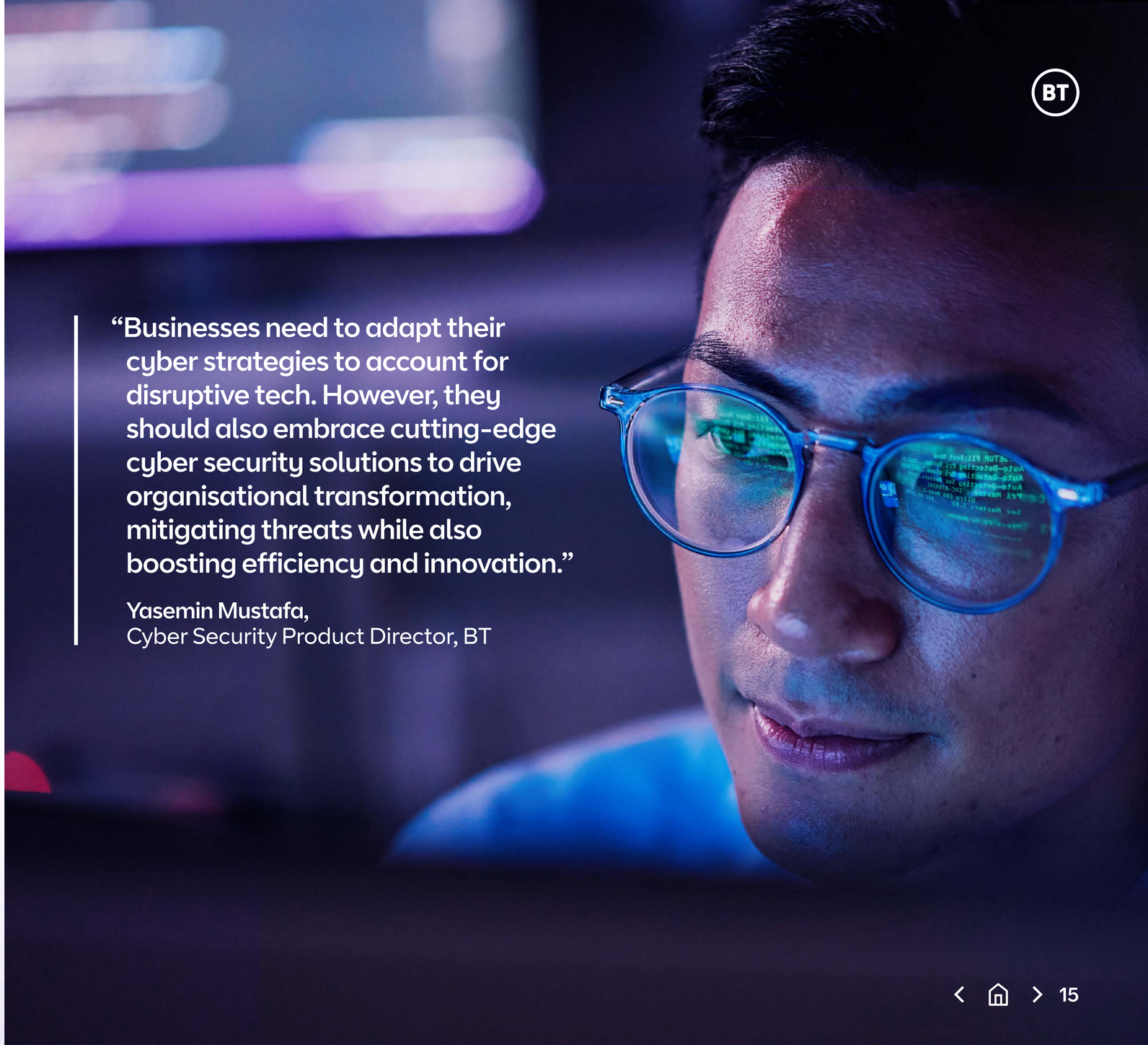
Performance: Driving innovation

Security keeps organisations safe, but it also enables confident experimentation, so it's no surprise that three-quarters of UK-based leaders believe innovating their approach to cyber security helps them to become more innovative overall.

In a cyber agile organisation, security strategies and processes not only keep pace with technological advancements but also power business transformation. AI serves as a prime example. Our research shows that seven in 10 UK business leaders believe the explosion of generative AI and shadow AI in the workplace has made security more important. However, an even greater number have incorporated AI into their cyber security toolkit, with **72%** having either partially or fully implemented AI or machine learning technology for threat detection.

Faced with increasingly sophisticated cyber threats, organisations also need to evolve their incident response processes. Cyber Agile Organisations in the UK are ahead of the curve: **41%** of leaders in these organisations say their incident resolution and recovery process has been extremely useful in mitigating the impact of cyber security threats, ensuring quick recovery and minimal disruption. This compares to only 20% of other organisations in the market.

72% have either partially or fully implemented AI or machine learning technology for threat detection



> "Businesses need to adapt their cyber strategies to account for disruptive tech. However, they should also embrace cutting-edge cyber security solutions to drive organisational transformation, mitigating threats while also boosting efficiency and innovation."

Yasemin Mustafa,
Cyber Security Product Director, BT

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

1

Sync your strategies

Strategies work best when everyone is moving towards a common goal. By aligning individual team strategies with your organisation's 'true north' objectives, you can optimise people power and ensure your organisation is running at its most efficient. Security should be viewed not just as a technical consideration, but as a fundamental business issue. To achieve this, it's important that cyber security has a permanent seat at the boardroom table, ensuring that security considerations are embedded in all strategic decision-making.

2

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.

3

Position security as a catalyst for growth

By integrating cyber security into your innovation strategies and communicating it across the organisation, you can create a culture that prioritises security while driving forward-thinking solutions. So, position security as a catalyst for growth and watch your business take off.

Conclusion

As an advanced, interconnected economy, the UK is a natural target for cyber crime. But companies operating within this market also have a distinct opportunity to push forward with innovative projects and collaborations, thanks to the mature approach to cyber security taken by many of these organisations.

By becoming cyber agile, leaders can take the handbrake off and encourage teams to be both bolder and more ambitious. Knowing that security is taken care of, risks are minimised and attack recovery plans are in place, they're free to strike forward with growth plans and move ahead of the competition.

BT's got your back

We're trusted

We protect the UK's critical national infrastructure. Organisations we all rely on – including the emergency services, armed forces, and NHS – trust our network to keep them connected.

Whatever your business, we've got your back

We've been protecting businesses of all sizes, across all industries, for over 70 years. Our Security Operations Centres around the globe protect your business 24/7, blocking 2,000 cyber attack signals every second.

We partner with world-leading vendors

We work with leading security partners to provide the best solutions and make sure everyone from small businesses to public sector and multi-nationals are protected from end to end.

BT Means Business

Get the conversation started

Talk to us

JN: 1634561879