BT Means Business

The Cyber Agile Organisation

Transforming security into a platform for growth

business.bt.com

Contents

Foreword

There is a huge opportunity to do more, better and faster in business.

Thanks to game-changing technologies such as artificial intelligence, big data and automation, today's leaders have an almost unlimited array of digital tools at hand to help them achieve their goals. However, to grab their chance, businesses must be not just agile but *cyber* agile.

Cyber security is more than just a defence against the dark arts; it's a strategic advantage. Companies must approach it differently today compared to just a few years ago, such is the wild pace of change.

Cyber Agile Organisations invest in their people, acquire cutting-edge security software, build slick processes, and either assemble expert teams or partner with reliable third-party providers to move forward confidently, free from fear of cyber attacks.

That's not to say innovation, experimentation and change don't come with a measure of risk, they do, but the most agile organisations are prepared for all threats, harnessing security as an enabler – not a blocker – of growth.

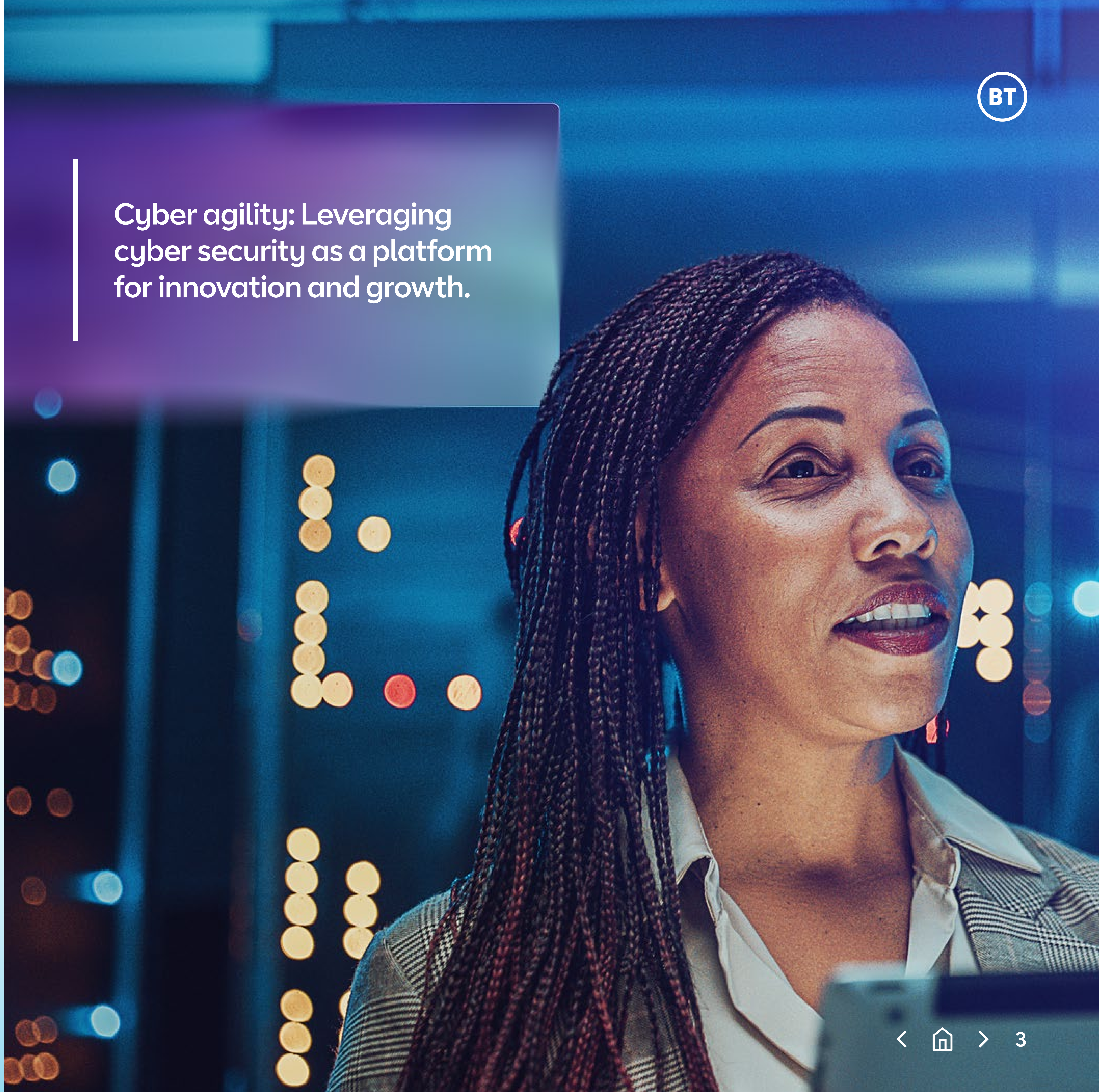
The DNA of a Cyber Agile Organisation

As a trusted leader, we've been protecting ourselves, our customers, and the UK's critical national infrastructure for over 70 years.

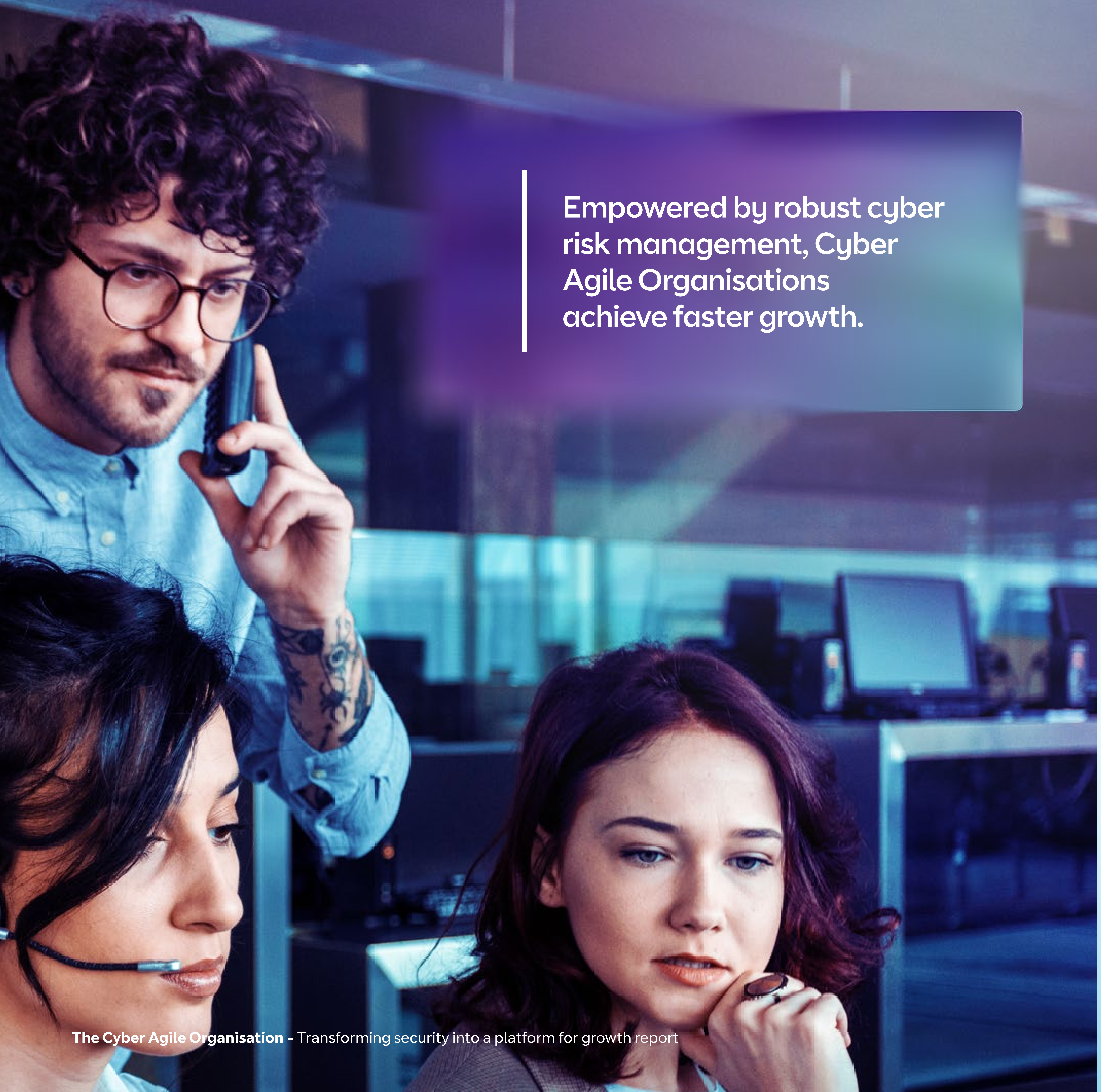
Today, we understand what it takes to be cyber agile, combining processes, technology, and expertise to keep organisations secure.

In this study, we shine a light on these high-performing organisations, weighing their attitudes and approaches to learn what they are doing right.

We assessed a wide range of businesses and public sector organisations, asking how they build resilience against cyber threats and use the resulting operational freedom to experiment, strike deals and build lasting relationships.



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



Empowered by robust cyber risk management, Cyber Agile Organisations achieve faster growth.

Foreword

We scored businesses and public sector bodies across six dimensions of cyber agility. The top performers, the Cyber Agile Organisations, had common threads.

They invest in cutting-edge solutions and train their people, but also keep one step ahead of cyber legislation, blend security strategies into enterprise-level business plans, and gain strategic advantage from their solid, secure and structured approach.

Empowered by robust cyber risk management, Cyber Agile Organisations achieve higher growth rates. They innovate, communicate and collaborate freely and are more likely than other organisations to be meeting their sustainability commitments.

In short, they are better at finding success and hitting targets now and in the future. What's clear from the research is this: companies that commit to becoming cyber agile perform better on average than those that don't.

Want to understand more about these advanced organisations and emulate their success? Then read on.

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 split into two groups:

- **1,275 IT C-suite leaders,** with job titles including Chief Security Officer (CSO), Chief Technology Officer (CTO) and Chief Information Officer (CIO).
- **1,225 other C-suite leaders,** including Chief Executive Officers (CEOs), Chief Operating Officers (COOs) and Chief Compliance Officers (CCOs).

Respondents represented organisations across eight industries: energy and resources, finance and banking, FMCG, healthcare, manufacturing, professional services, public sector including central government, and retail.

The sample also covered eight geographical markets: the UK, US, Benelux (Belgium, The Netherlands and Luxembourg), France, Germany, Spain, Australia and Singapore.

Economic model

We partnered with Capital Economics to build an economic model that estimated the potential macroeconomic benefits of improving the cyber agility of the businesses within each of the eight markets within this study. **See p44 for the detailed methodology.**

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

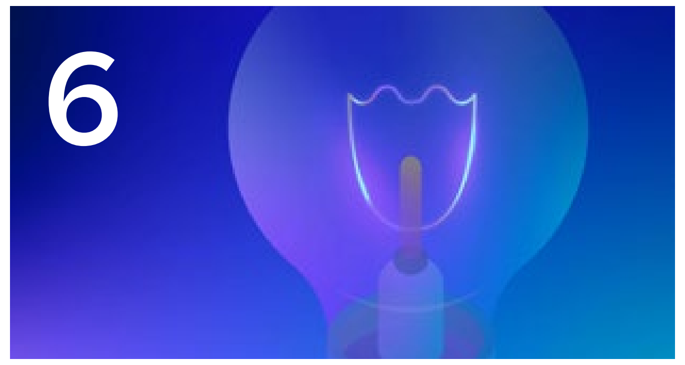
An organisation's visibility and understanding of its IT infrastructure and network, and the safeguards in place to ensure its security.

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.



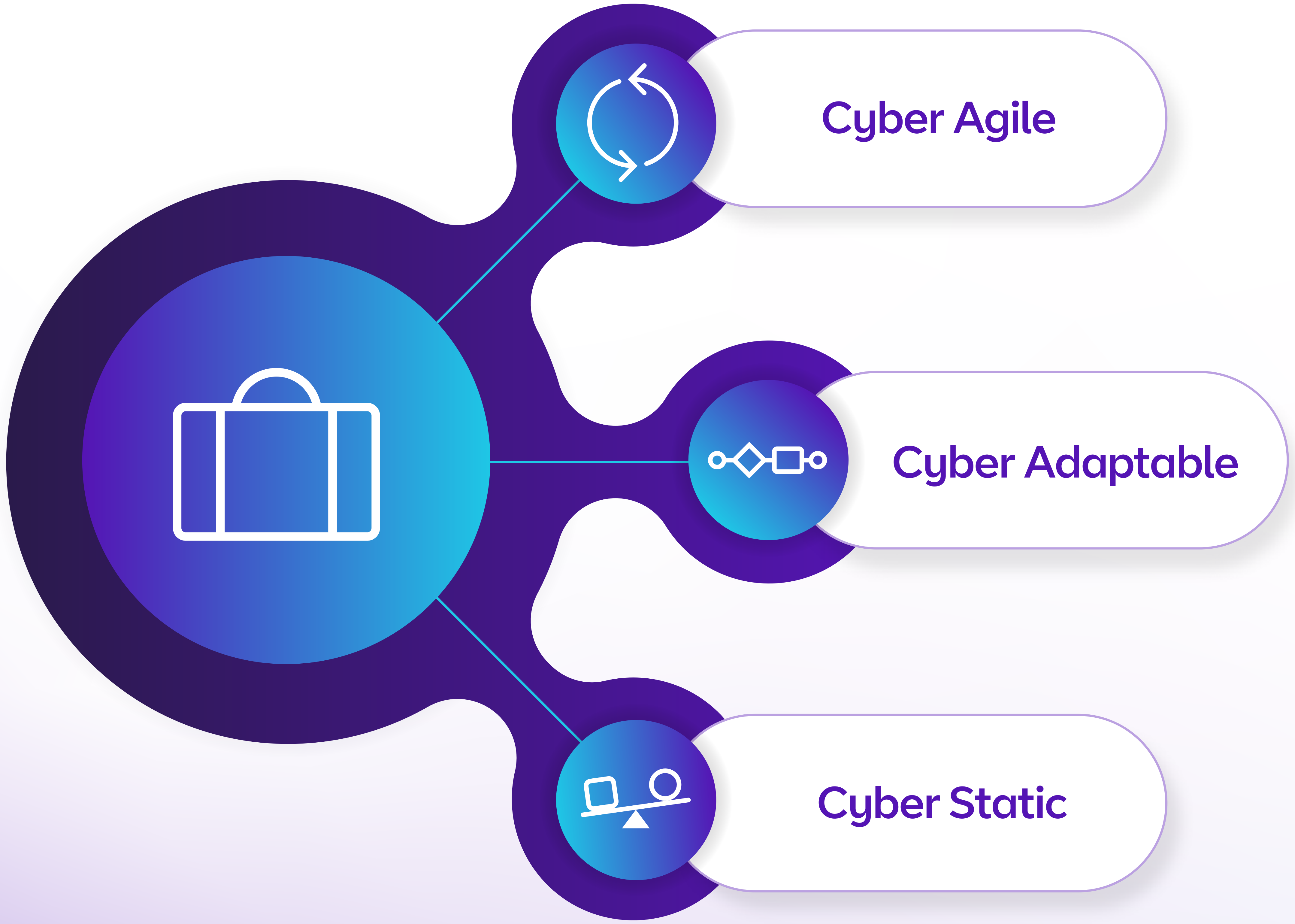
Innovation

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

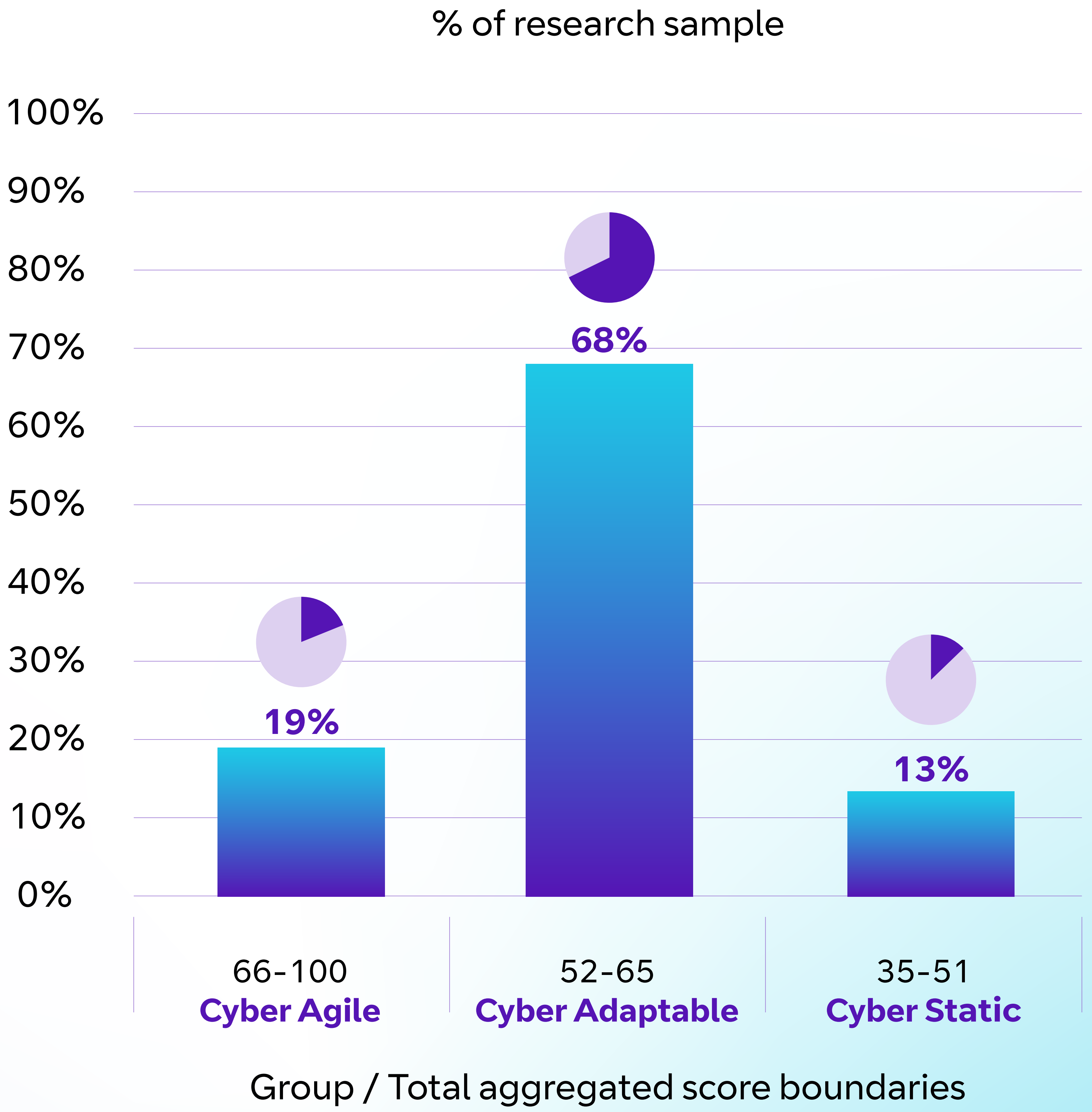
The cyber agility scoring system

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. **See p43 of the detailed methodology for the weightings by dimension.**

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



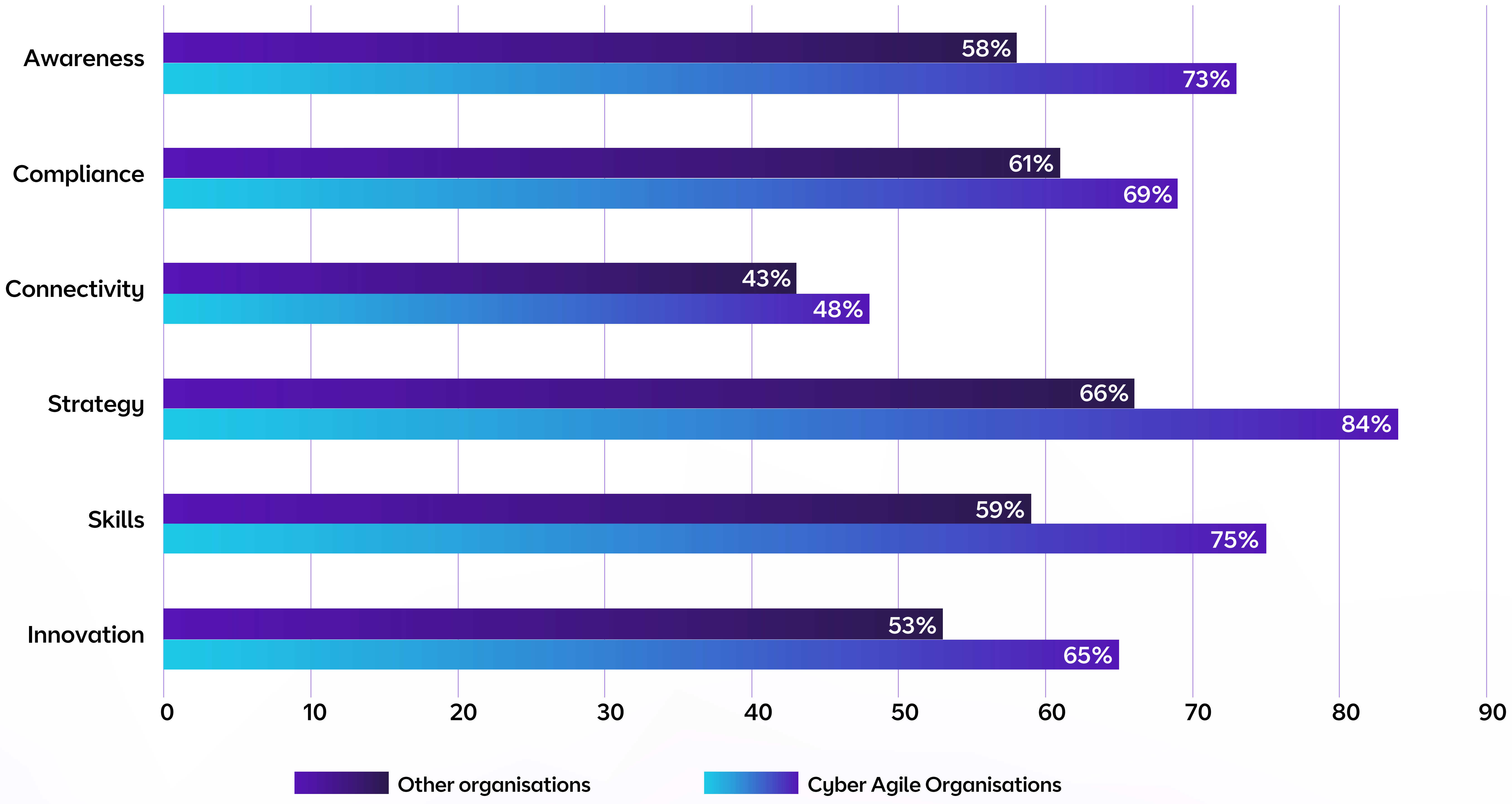
To qualify as a Cyber Agile Organisation, businesses and public sector bodies had to rank in the top-performing segment for aggregated scores across the six dimensions.

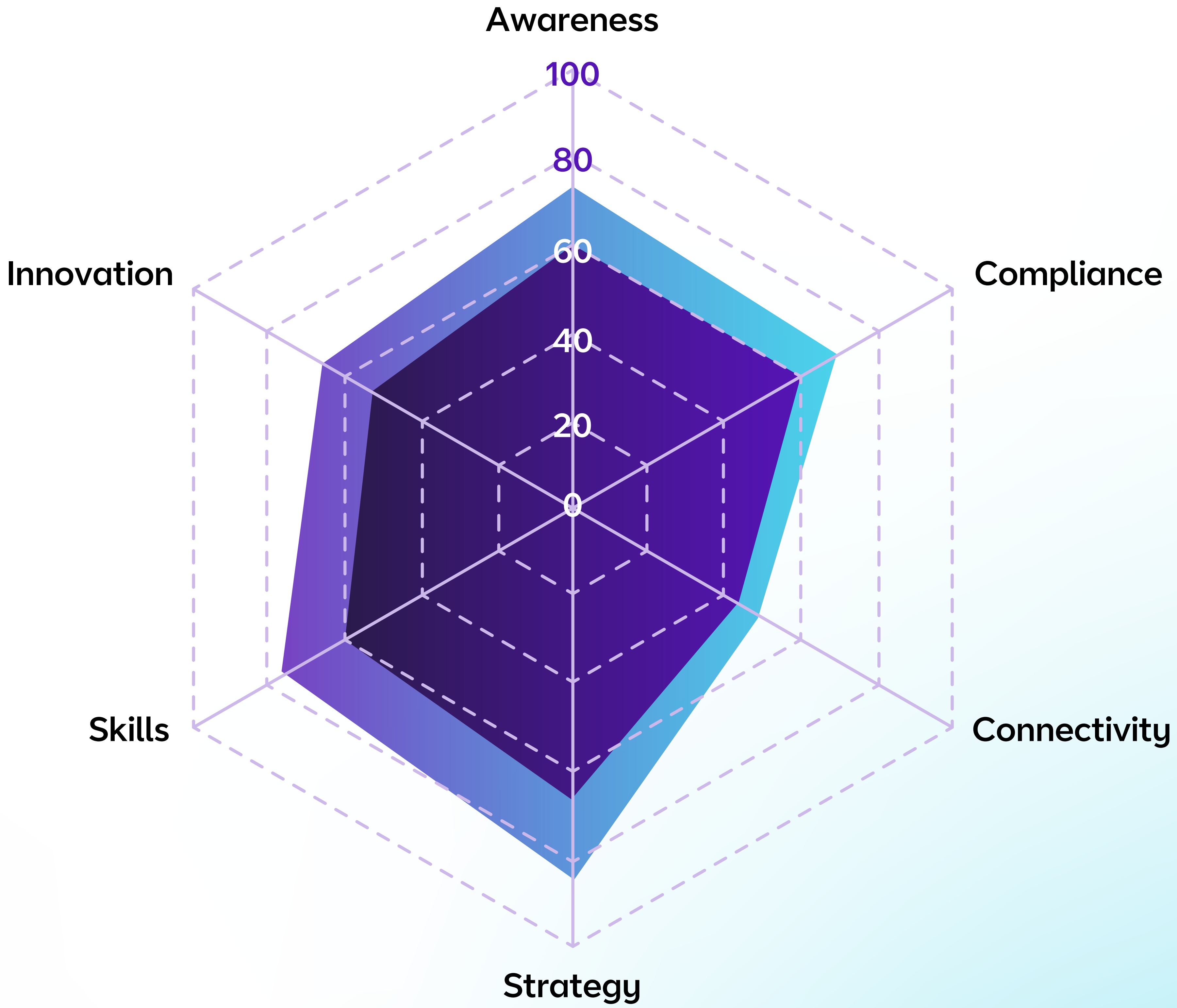


Graph: The cyber agility scoring system

Executive summary

Average cyber agility scores for Cyber Agile Organisations and other organisations





Cyber Agile Organisations excel across the six dimensions of cyber agility.

The gap between Cyber Agile Organisations and other organisations is starkest within the Awareness, Strategy and Skills dimensions, with the biggest gap seen within Strategy.

Connectivity is a critical area of focus.

The Connectivity dimension sees the lowest scores across all organisations, with only a small gap between Cyber Agile Organisations and others. As network infrastructure continuously evolves, leaders must focus on enhancing visibility and adapting safeguards to keep their ecosystems secure.

Potential economic benefits of cyber agility

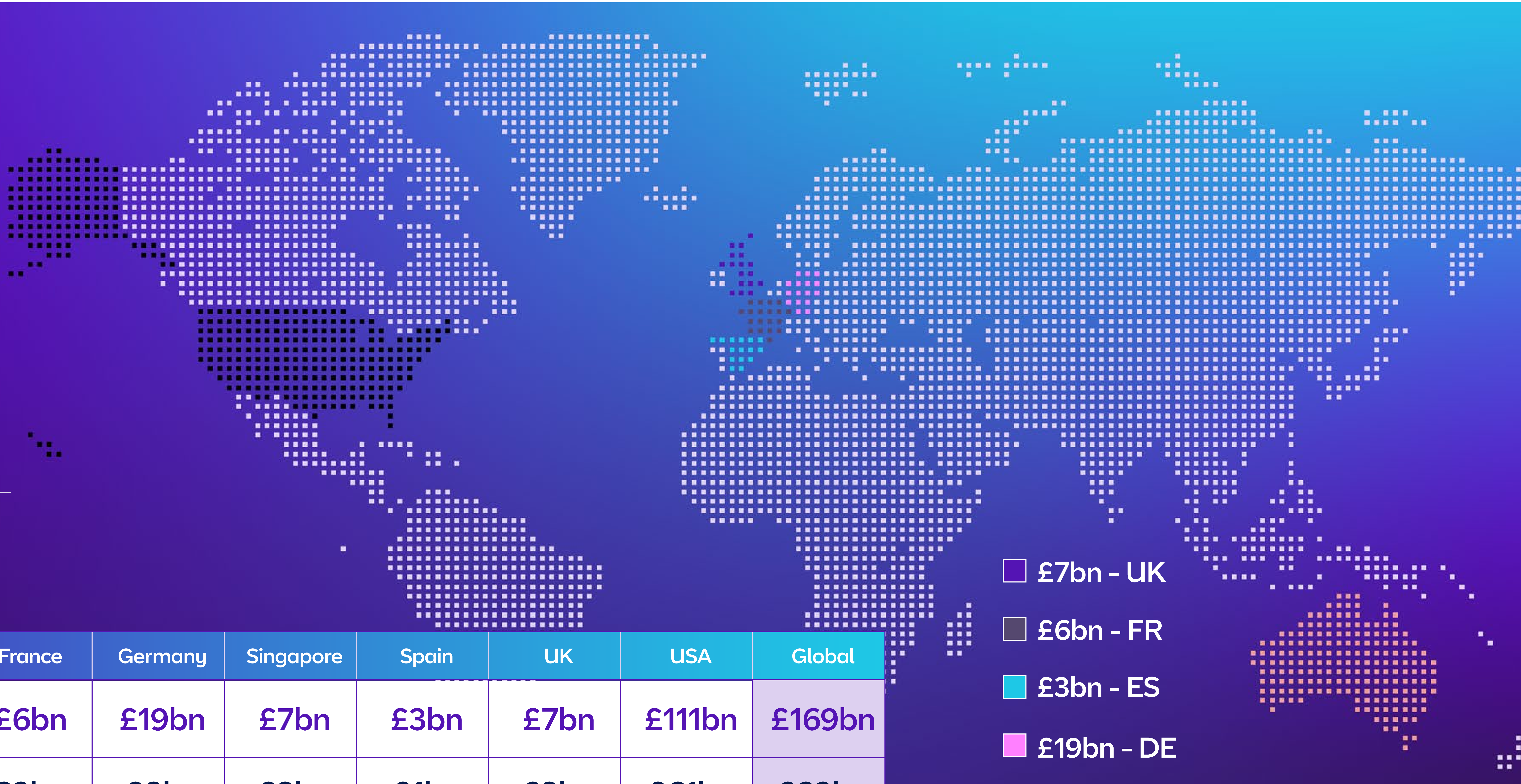
Cyber Agile Organisations are growing faster, representing a huge untapped economic opportunity.

Over the past three years, Cyber Agile Organisations achieved **20% higher growth rates** than other organisations in our study.

Extrapolating, if all other businesses across the eight markets covered in the study matched this growth rate by improving their cyber agility, this could unlock an additional **£169 billion in revenue** and **£83 billion in gross value added (GVA)**[1].

See p44 for the detailed methodology of how the figures were calculated.

[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.



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 1

The cyber agile advantage

The cyber agile advantage

As cyber crime evolves into a sophisticated global enterprise, the scope of criminal activity is deepening and expanding. BT's own data identifies more than 2,000 signals of a potential cyber attack take place every second – over 200 million per day.

Learn more

Bad actors are leveraging novel technologies, notably those stemming from artificial intelligence and big data, to broaden the attack surface, increase the pace of infiltrations and amplify the level of damage caused.

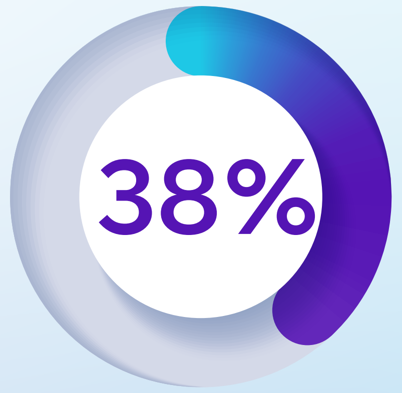
One in three (33%) business leaders in our study state they are currently experiencing 'high' or 'very high' cyber attack severity. The figure increases to 48% for those who anticipate this level of severity within the next three years.

1 in 3
Business leaders experience very high cyber attacks

This finding is brought into particularly sharp focus given that six in 10 business leaders say that a major cyber attack is the main existential threat to their organisation. For 55% of leaders, meanwhile, the risk of a cyber attack is enough to keep them awake at night.

42% report an 'enhanced strategy' for cyber security.

When assessing their organisation's cyber security maturity level, the majority of leaders report either an 'enhanced strategy' (42%) or an 'integrated and proactive' approach (38%). However, just 14% of leaders currently assess their cyber security as 'strategic and agile'.



38% report an 'integrated and proactive' for cyber security.

Cyber security self-assessment

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

42%

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%

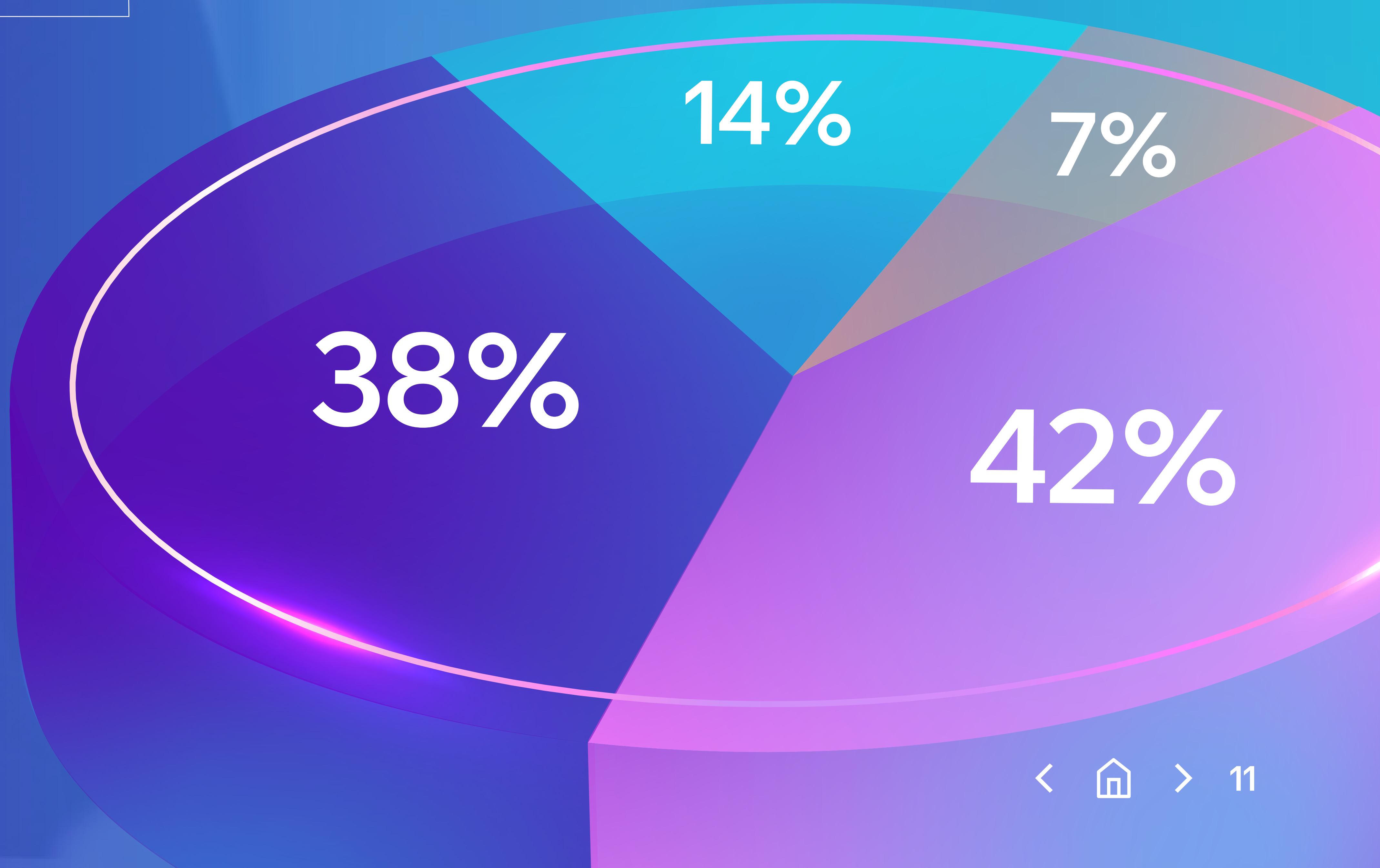
Cyber security is fully integrated into the way we build our products, services and processes within our organisation's operations, with proactive measures in place to prevent, detect and respond to threats.

Strategic and agile

14%

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.

Pie chart: Maturity level - % of organisations



What is cyber agility?

Tackling evolving cyber threats is an ongoing challenge – one that cannot be effectively addressed by security teams working in isolation.

Building cyber resilience requires an organisation-wide response, with accountability in every department and at every level of seniority. With a comprehensive, systemic and agile approach, businesses and public sector bodies stand a better chance of staying one step ahead of threats. And, when they do experience an attack, they are better equipped to contain it and resolve it quickly to minimise the impact.

The Cyber Agile Organisations in our study see cyber security as the cornerstone of their technology matrix; in fact, **89%** of them say it is the foundation of their IT system. So it is unsurprising that they are confident in their ability to manage cyber attacks, if and when they occur. Three-quarters of Cyber Agile Organisations report that they are currently either 'very prepared' or 'extremely prepared' to deal with cyber attacks, compared with half (**51%**) of other organisations.

But, being cyber agile goes beyond simply fending off threats; it involves leveraging a secure IT ecosystem to boost overall business performance. A cyber agile mindset underpins the quick, confident action that fuels fast, sustainable growth.

> Comprehensive cyber resilience ensures proactive threat management.

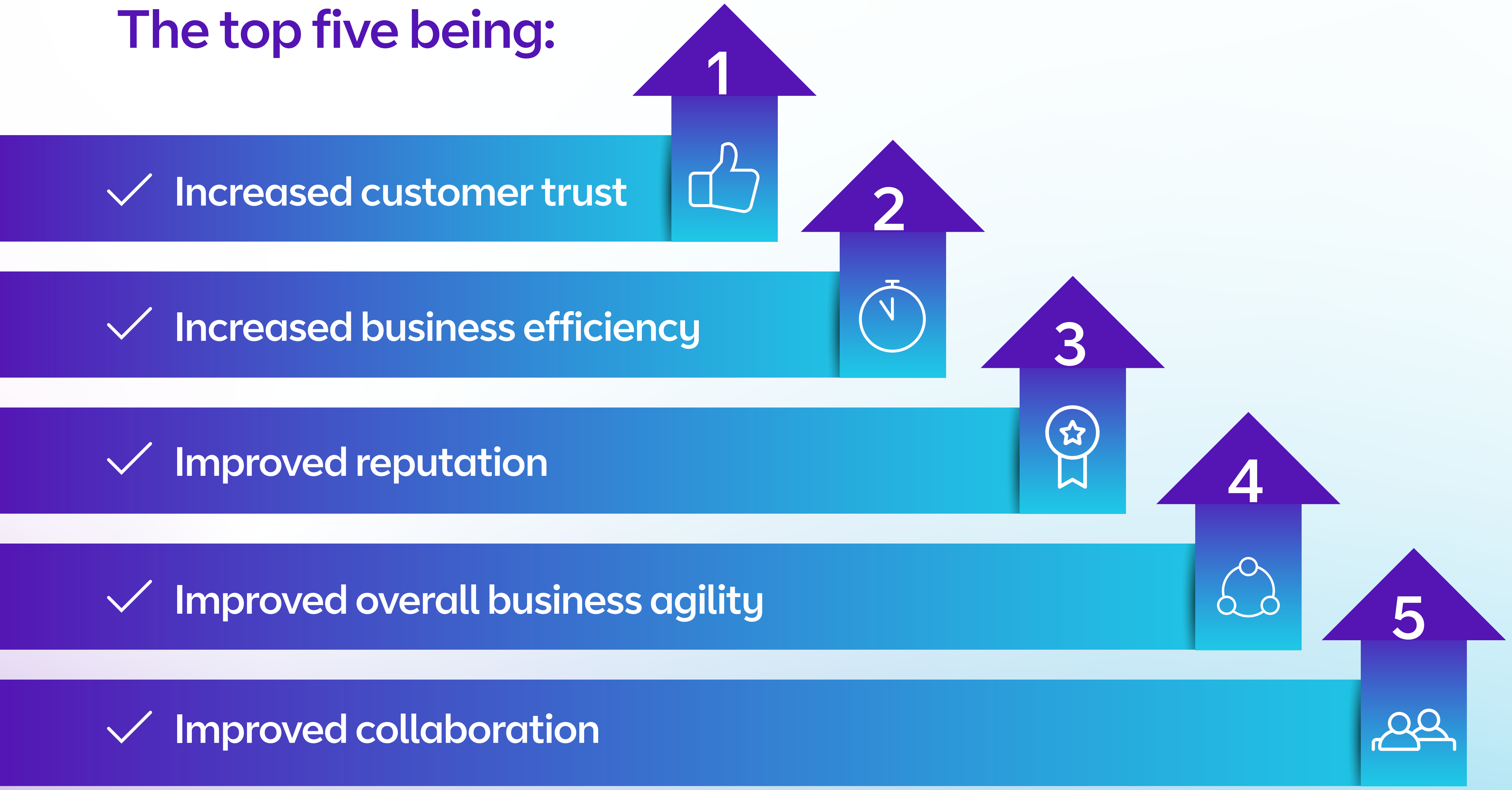
The importance of being agile

Two-thirds (67%) of all leaders in our study believe a secure IT system is a prerequisite for doing business. However, implementing robust systems, along with a cyber-aware workforce and efficient processes, offers a range of business benefits far beyond the server room.

Our research also highlights the link between cyber agility and sustainability. Cyber Agile Organisations are more likely than other organisations to have achieved net zero, but also to have net-zero targets approved by the Science Based Targets initiative (SBTi).

Business leaders recognise several significant benefits that improved cyber agility would bring to their organisations.

The top five being:



✓ Increased customer trust

✓ Increased business efficiency

✓ Improved reputation

✓ Improved overall business agility

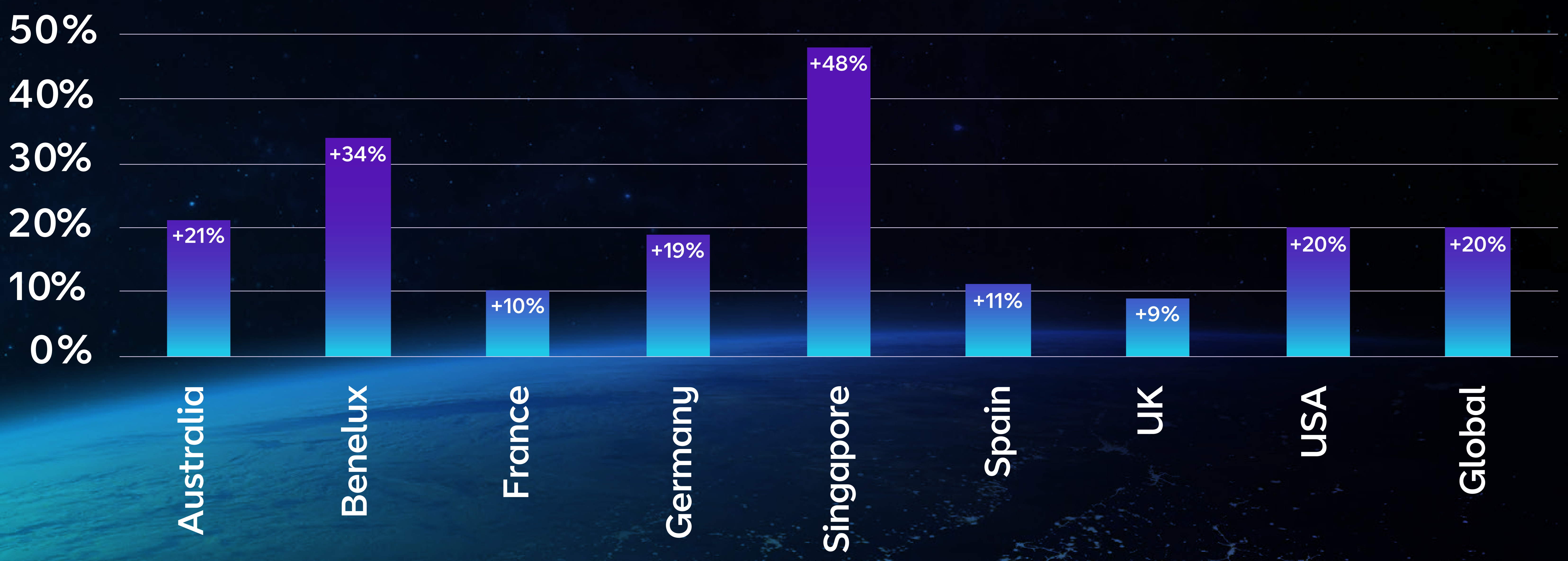
✓ Improved collaboration

Cyber agility builds businesses

Over the past three years, Cyber Agile Organisations achieved 20% higher growth rates than other organisations in our study. Extrapolating, if all other businesses across the eight markets covered in the study matched this growth rate by improving their cyber agility, this could unlock an additional £169 billion in revenue and £83 billion in gross value added (GVA)[2].

[2] 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

The six dimensions of cyber agility

Preparedness

Cyber Agile Organisations follow cyber security regulations, adopt best practices and keep a sharp watch over their IT systems.

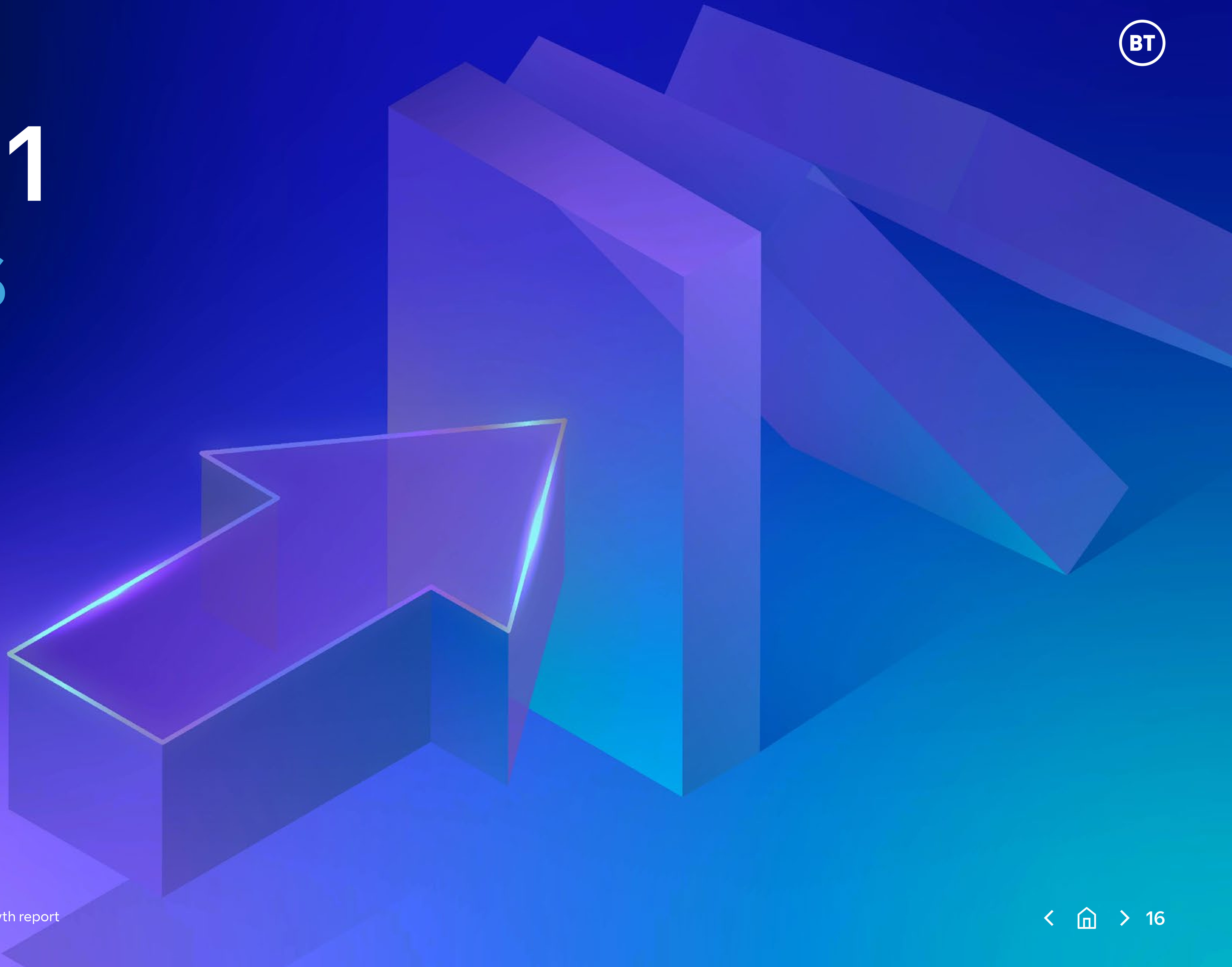
1. **Awareness**
2. **Compliance**
3. **Connectivity**

Performance

Cyber Agile Organisations align cyber security with business goals through mature strategies, skilled talent and innovative approaches.

4. **Strategy**
5. **Skills**
6. **Innovation**

Dimension 1 Awareness

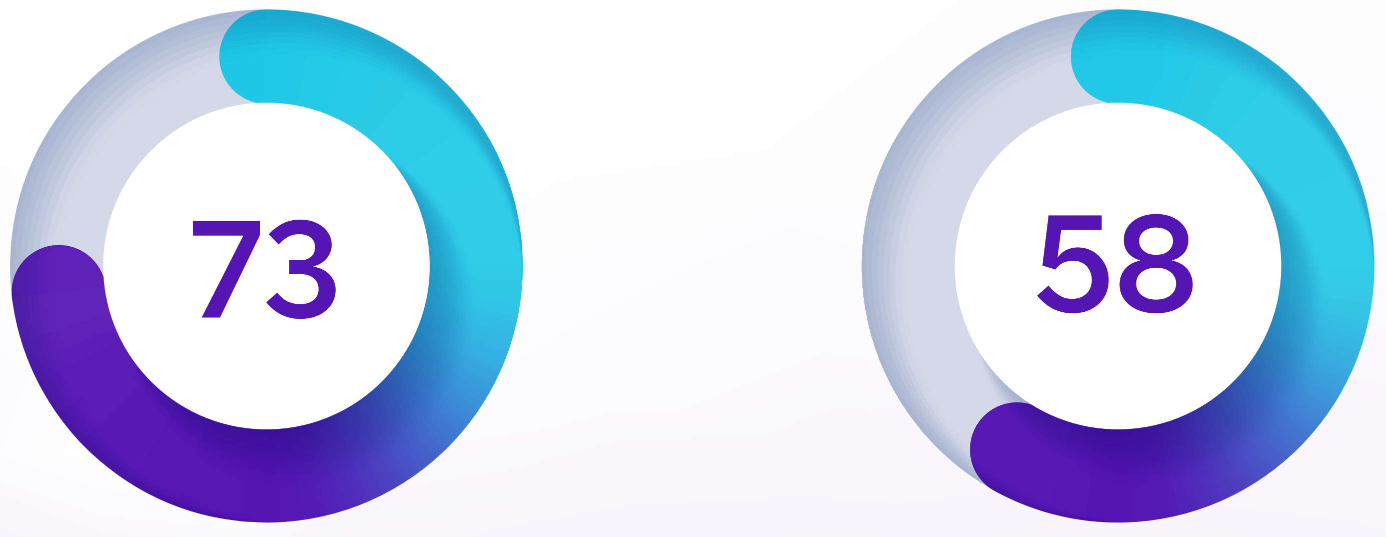


Dimension 1
Awareness

Cyber criminals are constantly updating their strategies and tactics in a bid to wrong-foot organisations. Encompassing clear visibility and proactive mitigation measures, awareness is the bedrock upon which cyber agility rests.

It equips organisations with both the foresight to spot threats and anticipate malign activity, as well as the proactive tools to stop cyber-criminals in their tracks. In the case of a successful attack, awareness also gives organisations a better chance of spotting malign activity in the network and taking steps to contain the threat.

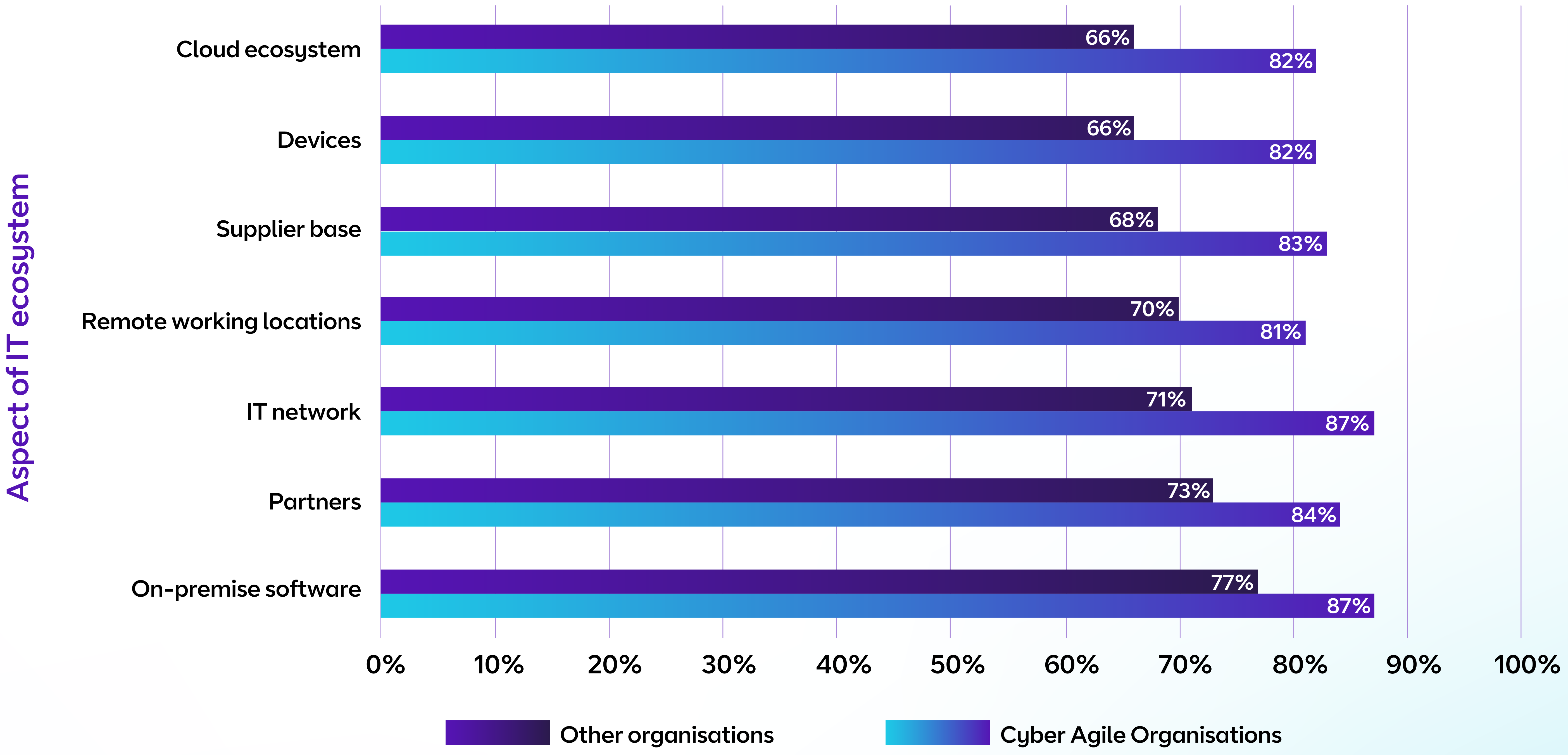
Average Awareness scores



Cyber Agile Organisations

Other organisations

Organisations that have 'complete' or 'high' visibility across their IT ecosystem



Visibility powers cyber resilience

You can't guard what you can't see. With businesses increasingly managing multi-cloud and multi-vendor ecosystems, having full visibility of the IT footprint and a comprehensive understanding of its operations allows organisations to better map potential threats and develop strategies to mitigate them.

Our research reveals that **87%** of Cyber Agile Organisations have 'high' or 'complete' visibility of their on-premise software (compared to **77%** of other organisations), and **82%** have 'high' or 'complete' visibility of their cloud ecosystem (compared to **66%** of other organisations).

Cyber criminals look for weaknesses across the attack surface, eyeing potential fragilities beyond organisations' core security infrastructure. The organisations in our study – including Cyber Agile Organisations – report lower awareness levels when it comes to devices and remote working.

Adaptive cyber policies

With the changeable cyber risk landscape comes the need for organisations to adapt to survive. So, it's no surprise that, on average, Cyber Agile Organisations review and update their security policies every four months, compared with every six months for other organisations.

A third (**32%**) of Cyber Agile Organisations test their cyber security policies at least once a month

22% have an ongoing process to test their policies as part of their regular operations.

This means reviewing and updating policies fluidly and never imagining that the job is complete.

Steps to cyber agility: Boosting awareness

1

Have clear visibility

Ensure comprehensive visibility and monitoring of your entire IT infrastructure, including operational technology and unmanaged devices. Regularly assess cyber security risks and implement robust safeguards to keep your network secure, now and in the future.

2

Actionable threat intelligence

It's important to know who is attacking you and who you are potentially at risk from – this differs from industry to industry. This assessment should include your organisation's data and networks, but also cyber security trends and patterns happening beyond it.

3

Address vulnerabilities

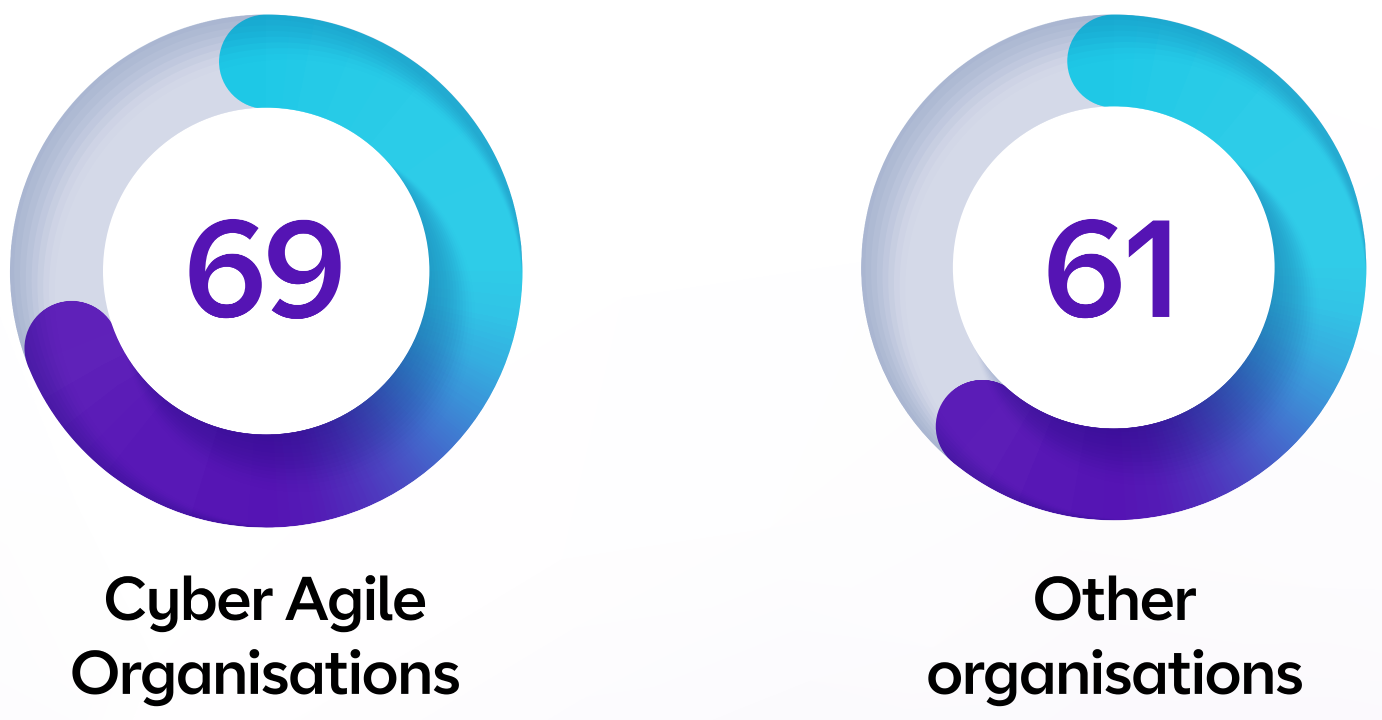
Using a range of reliable information sources, carry out an assessment of your entire IT ecosystem and create a plan to address any problems raised. Know where your vulnerabilities lie and the location of your most important IT assets. It's important to keep a 'live' threat analysis, tracking key areas of risk and highlighting emerging vulnerabilities.

Dimension 2
Compliance

Dimension 2 Compliance

Cyber security is a heavily regulated part of the IT ecosystem, so it's important to stay on the right side of compliance. Keeping pace with evolving rules demonstrates a strong commitment to best practices and helps build stakeholder trust.

Average Compliance scores

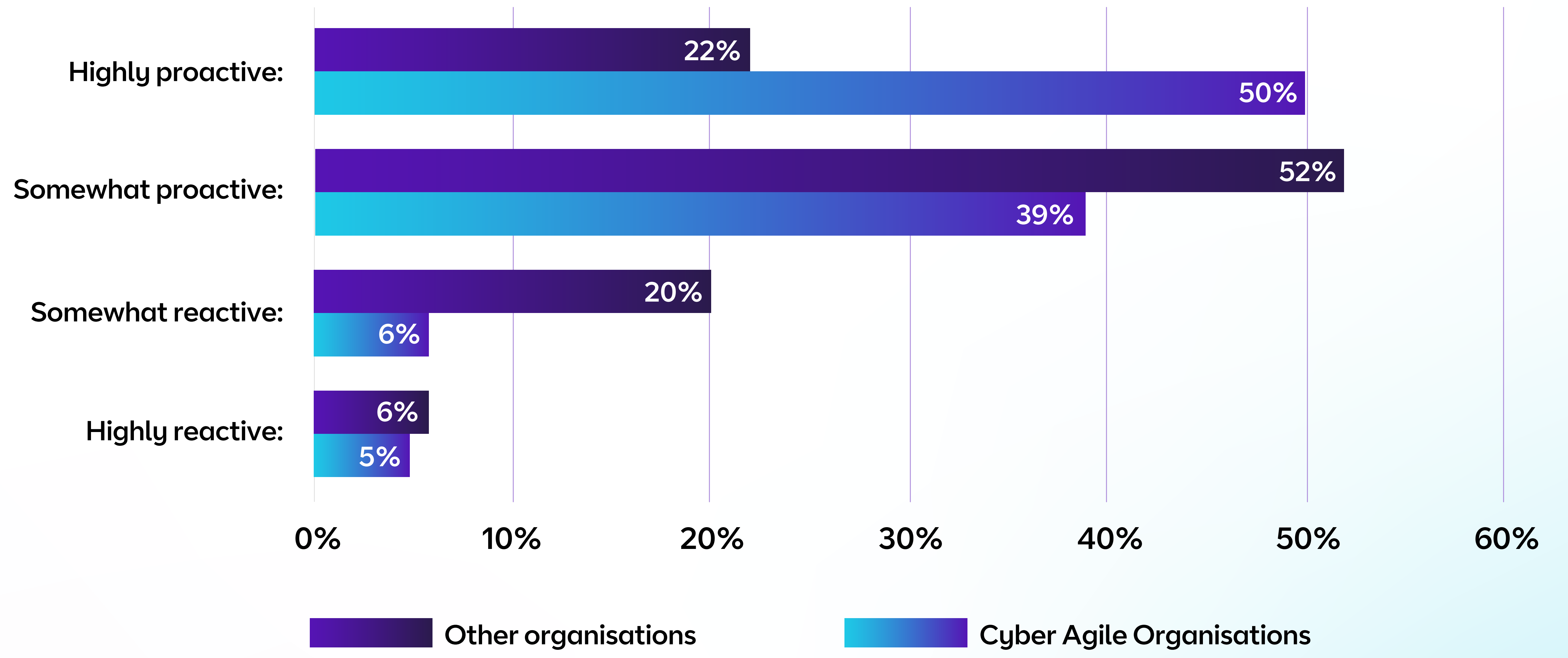


Proactivity pays off

It's good to get ahead of the game and never more so than when you're dealing with complex rules and regulations. According to our research, half of Cyber Agile Organisations take a 'highly proactive' approach to dealing with changes to cyber regulation, contrasting with just over a fifth (**22%**) of other organisations claiming the same.

Organisations are only as secure as their weakest point, so getting every part of the business working in tandem is essential. More than three-quarters (78%) of Cyber Agile Organisations say their global IT team is constantly communicating with local teams to ensure they stay compliant with local regulations.

Approaches to dealing with changes to cyber security regulations



Highly proactive

We constantly monitor, predict and input into upcoming regulation and always put measures in place to manage new regulation before it comes into force.

Somewhat proactive

Most of the time we monitor upcoming regulation and put measures in place before it comes into force, but occasionally this is after regulations are enforced.

Somewhat reactive

Most of the time we wait until regulations are enforced to implement measures, but occasionally we may prepare to implement measures to deal with new regulations before they are enforced.

Highly reactive

We never implement measures to deal with new regulation until it's already come into force.

Steps to cyber agility: Ensuring compliance

The cost of non-compliance

Our research highlights the financial penalties companies face when they fall behind the regulatory curve.

Legal action: In the past 12 months, **39%** of organisations have faced legal action as a result of non-compliance with cyber security regulations.

Lost sales: Moreover, almost half (**46%**) of organisations have seen a loss of sales due to not being able to comply with customer requirements, with **27%** of these seeing losses of more than $1 million.

1

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.

2

Understand your strategy

To ensure regulatory compliance, you need a comprehensive understanding of your cyber security strategy. This means evaluating existing security controls across people, processes and technology, pin-pointing any gaps in your defences, then prioritising areas for improvement.

3

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.

Preparedness

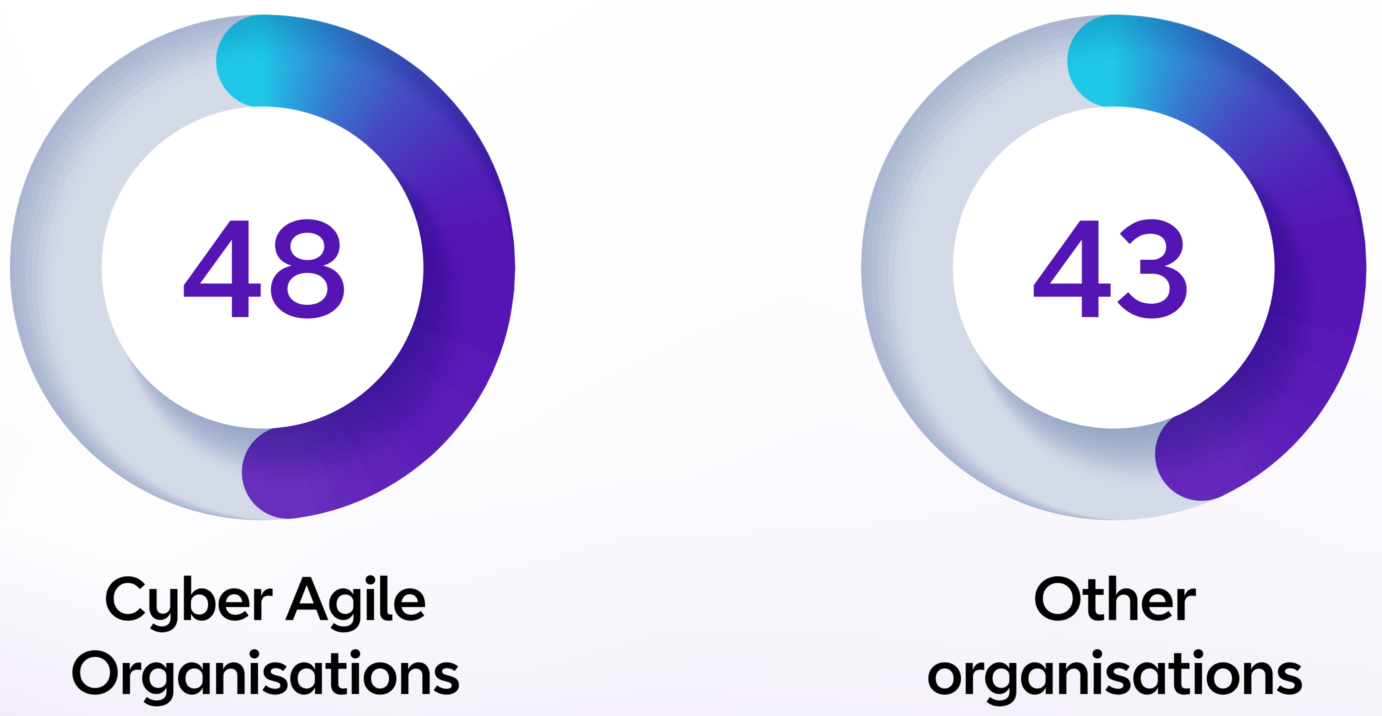
Dimension 3
Connectivity

Dimension 3 Connectivity

Secure connectivity insulates organisations against threats while maintaining network integrity. It protects individuals, safeguards brands and prevents data breaches that erode customer trust.

But it also frees up your people to collaborate, innovate and work across data-heavy apps; the perfect cocktail for fast yet sustainable growth. The Connectivity dimension sees the lowest scores across all organisations, with only a small gap between Cyber Agile Organisations and others.

Average Connectivity scores



Securing the network

An organisation's growth is increasingly reliant on the capacity of its network, but it's important that this growth occurs securely. Securing fixed and mobile networks, data centres and multi-cloud environments is essential for mitigating unauthorised access and large-scale disruptions, ensuring business resilience.

The explosion of connected devices in recent years has blurred the line between IT (information technology) and OT (operational technology) as organisations integrate physical machinery and devices into digital systems. While this transformation is enhancing efficiency and responsiveness, it is also broadening attack surfaces.

As network infrastructure continuously evolves, thriving connectivity depends on continuously evolving security. Two-thirds of Cyber Agile Organisations (**65%**) report that their business has a high visibility of its IT infrastructure and network and strong safeguards to keep them secure, compared to **31%** of other organisations.

Securing the distributed workforce

The rise in remote and hybrid working led to more people conducting company business on their own devices – whether this is authorised by their organisation or not.

This might bring benefits for convenience and cost-cutting, but it presents a serious connectivity conundrum when it comes to network security.

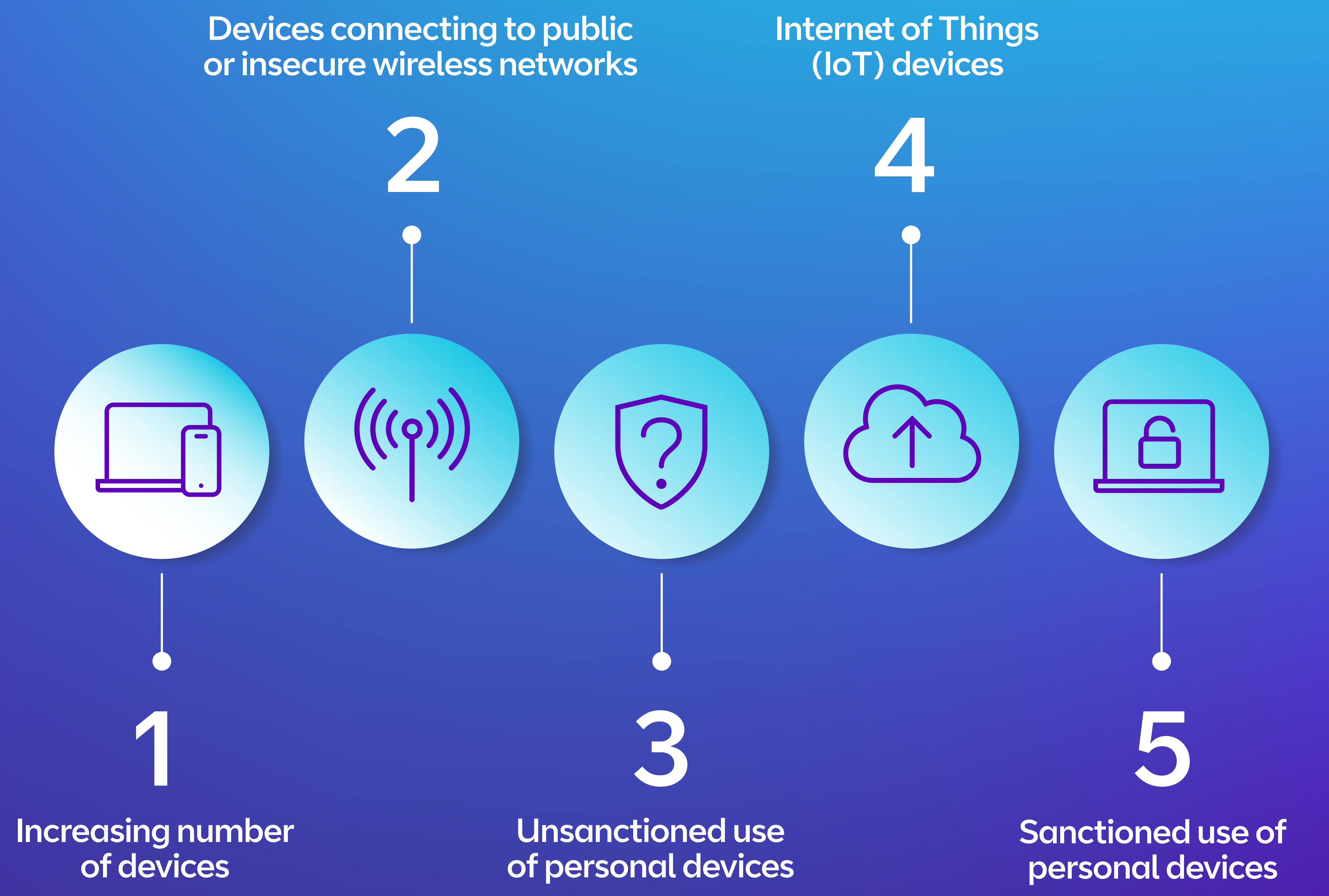
According to the business leaders in our study, the booming number and variety of devices, along with how employees are using them, pose significant risks to their organisations.

Securing the supply chain

The supply chain is a valuable resource for cyber criminals. By targeting weak points in the chain, for example, businesses with legacy systems and outdated security measures, they can gain access to other organisations through the back door.

Cyber Agile Organisations understand this: **84%** of leaders in this group say their organisation won't work with suppliers who can't produce adequate security credentials.

Top 5 cyber risk factors within organisations' networks:



1 Increasing number of devices

2 Devices connecting to public or insecure wireless networks

3 Unsanctioned use of personal devices

4 Internet of Things (IoT) devices

5 Sanctioned use of personal devices

> "Organisations increasingly have access to a universe of transformative digital tools. Only with powerful, stable connectivity will they be able to take full advantage in future."
>
> **Yasemin Mustafa**, Cyber Security Product Director, BT

Steps to cyber agility: Securing connectivity

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 Collaborative data management

Consider how your supply chain impacts the job of protecting your network. Knowing where your data lies, how it moves geographically, and who has access to it is an essential part of maintaining end-to-end visibility.

3 A different view of how your business 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, secure access service edge (SASE) and software-defined wide area network (SDWAN) must be deployed, relevant processes layered on top, and all brought together by trained people who can underpin the agile organisation.

Performance

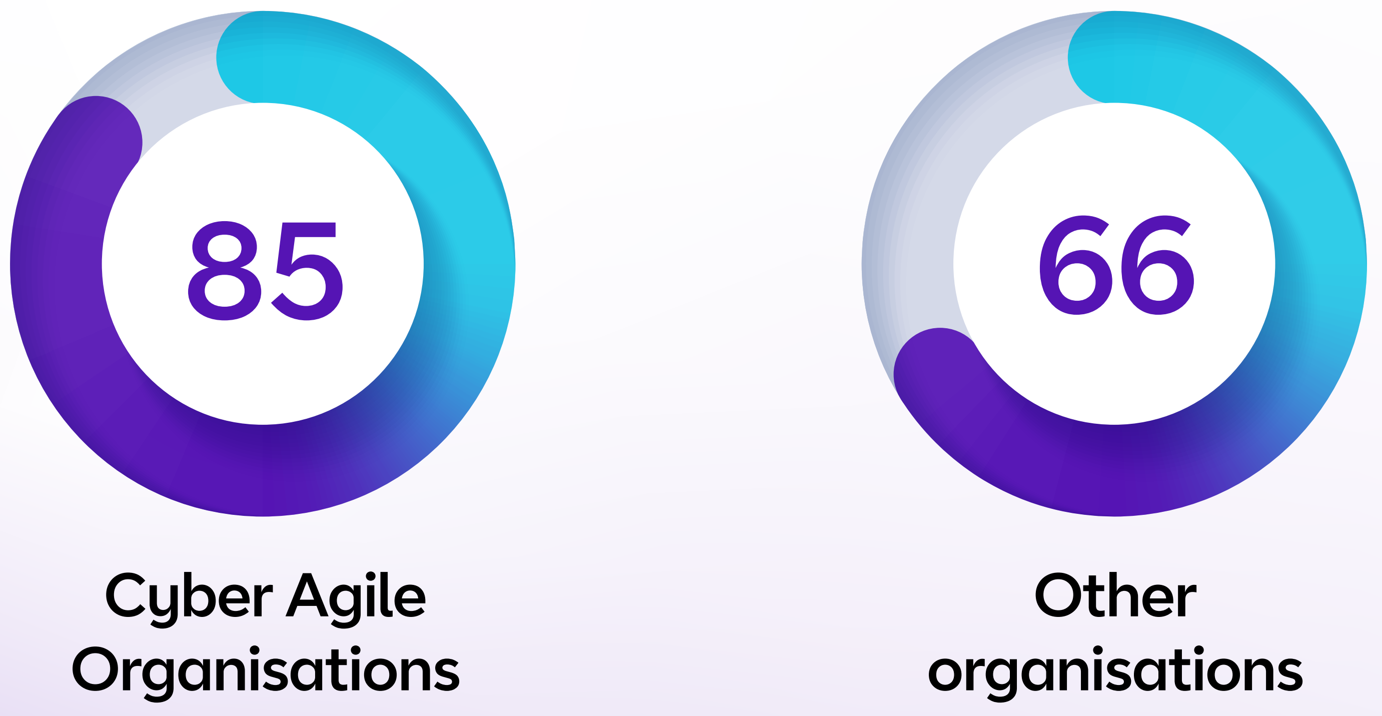
Dimension 4
Strategy

Dimension 4
Strategy

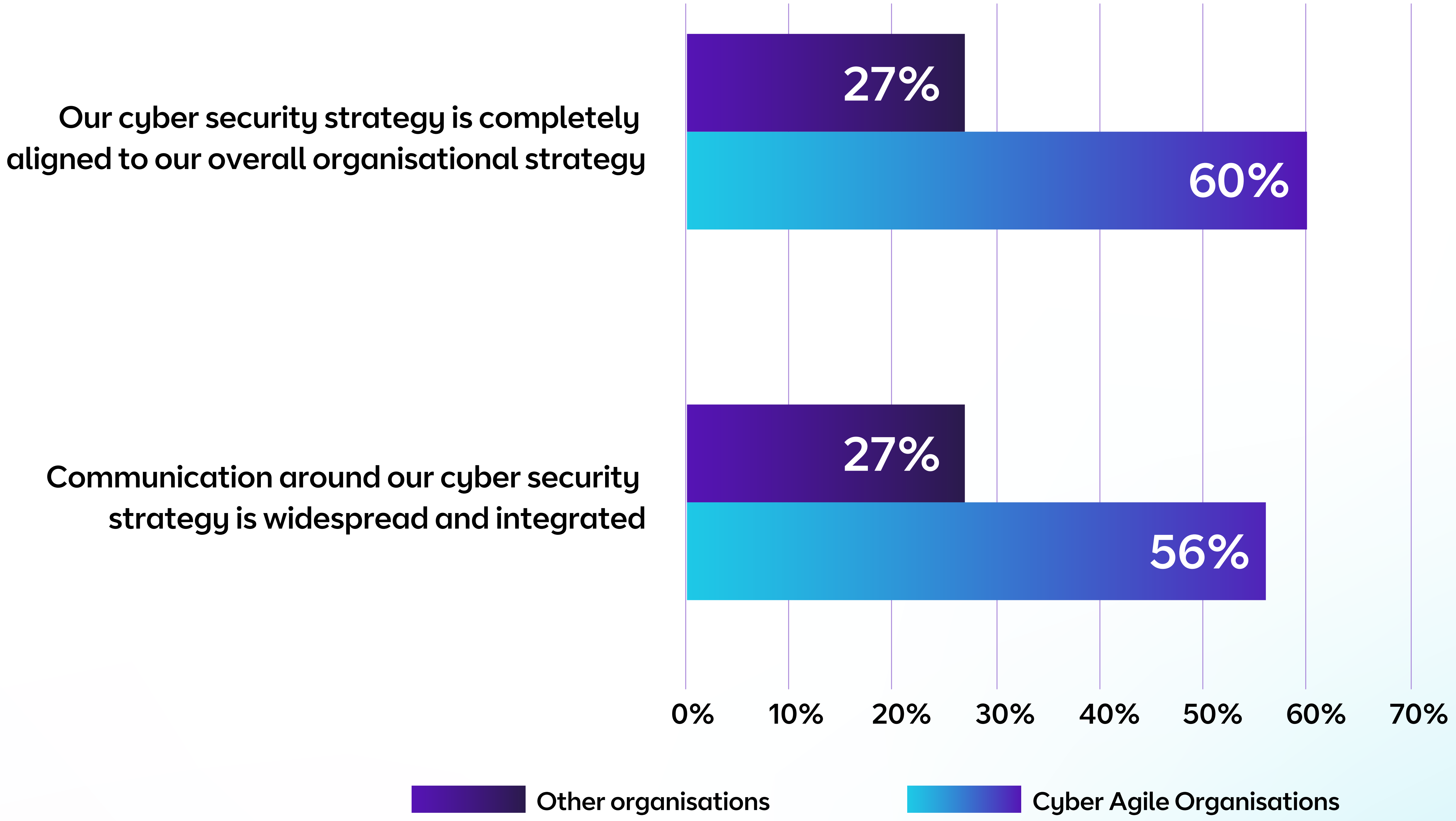
Security is no longer an IT issue but a business issue. This makes a robust cyber security strategy - aligned with broader organisational goals - essential to build a proactive cyber security culture and drive sustainable growth.

A cyber security strategy is the overarching vision that outlines the objectives of an organisation's approach to cyber security and the reasons behind them, such as safeguarding sensitive data, ensuring business continuity and maintaining stakeholder trust. This strategy sets the direction for the development of specific plans to mitigate cyber risk and enhance resilience.

Average Strategy scores



Organisations' approaches to cyber security strategies



The importance of alignment

When it comes to cyber security, continuity is key. **Six in 10 leaders** in Cyber Agile Organisations say their cyber security strategy is completely aligned with their overall organisational strategy, compared to just over a quarter of leaders across other organisations.

In cyber security, as in all business areas, the top team must agree on the cultural direction of the business. That ensures clear communication of principles and direction of travel down the chain of command.

However, our research shows that while three-quarters of chief technology officers and chief information security officers say their organisation is actively building a cyber security culture, only two-thirds of chief executives agreed.

Insufficient security funding

Four in 10 leaders believe their organisation's cyber security budget is not keeping pace with the increased level of cyber threat, with just £1 in every £10 within IT budgets allocated to security.

Rising cyber threats

This is a stark finding given the rising tide of global cyber security threats and their increasing levels of sophistication. Failing to keep pace with criminal enterprises could spell disaster for businesses that leave themselves vulnerable.

Affordable cyber security

Budget is a pressure on all businesses, so while many leaders fear they aren't keeping pace with the financial needs of cyber security, there could be scope to deal with threats via cost-effective channels like outsourced managed services, automation and AI.

Steps to cyber agility: Strengthening strategy

1

Synch 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. 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

Secure by design

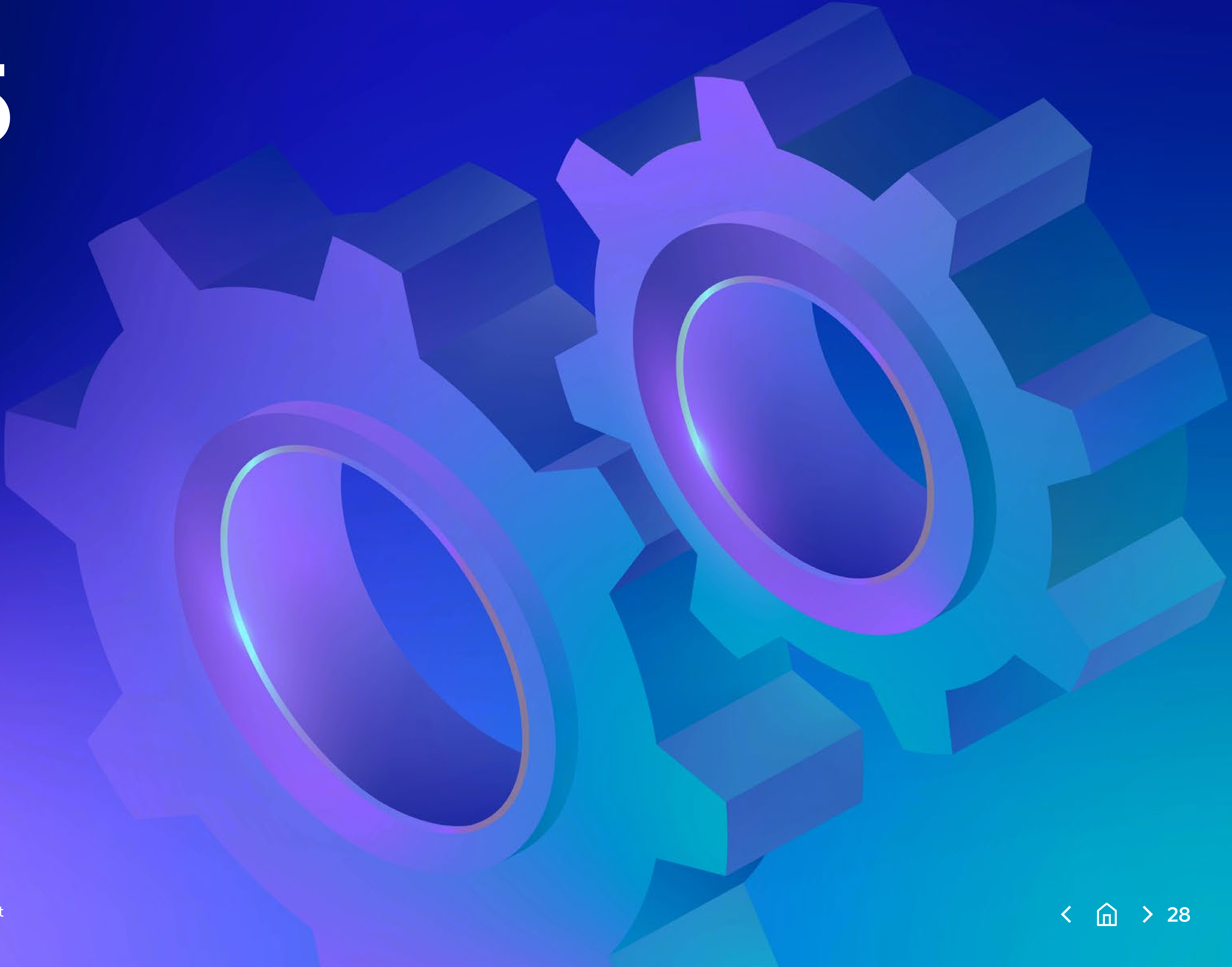
Security should be seen as not just a technical consideration, but a business issue that is fundamental to the success of all projects. This involves integrating security considerations from the initial design phase through to deployment and maintenance. Building cross-functional teams – including developers, security experts and business leaders – ensures that potential vulnerabilities are identified early, and robust security measures are implemented.

3

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.

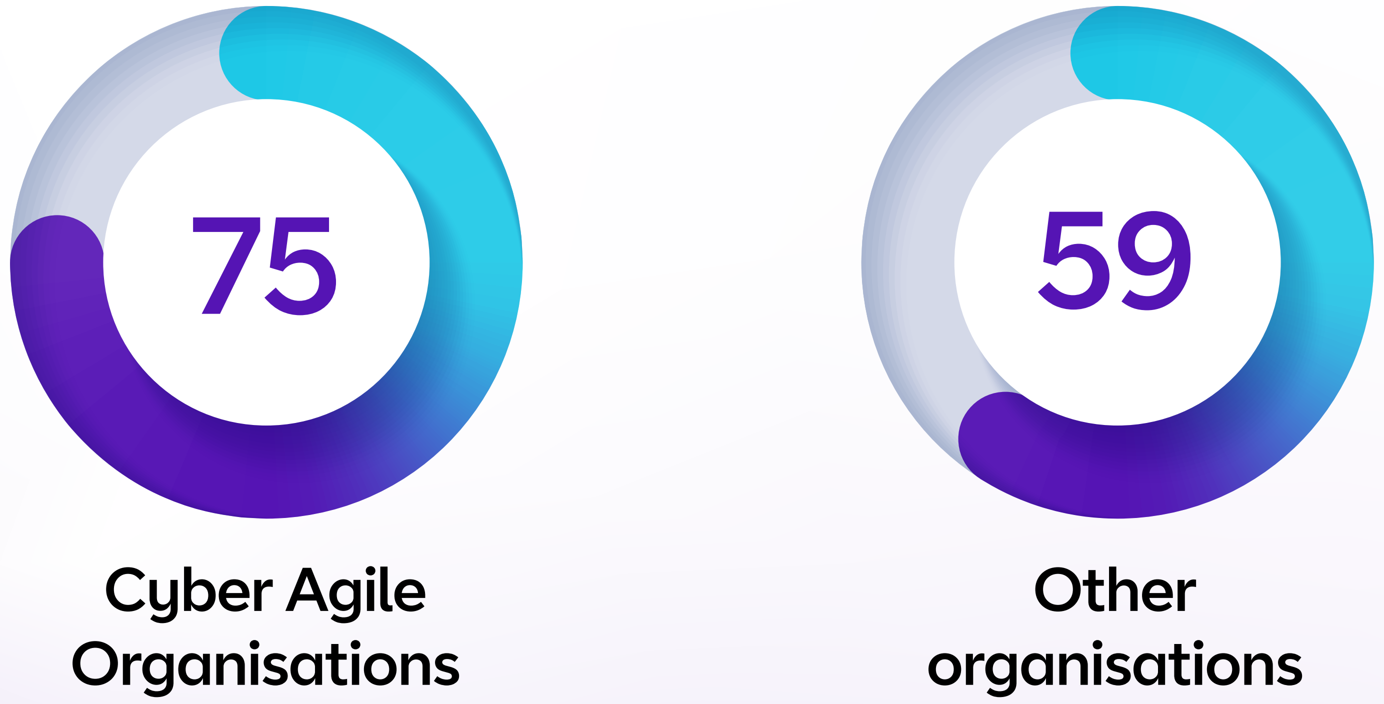
Dimension 5
Skills



Dimension 5
Skills

Recruiting, training and retaining a diverse team of skilled cyber security professionals helps organisations implement cutting-edge strategies that will help to stay ahead of rapidly evolving threats. However, achieving true cyber agility will require organisation-wide awareness and understanding of what's at stake.

Average Skills scores



Security as a team sport

Cyber threats don't always originate outside the organisation; often they begin closer to home. That doesn't necessarily mean bad actors within the organisation, although this shouldn't be ruled out, but simple mistakes made by honest, hard-working members of staff. In fact, almost two-thirds of leaders (**63%**) believe that human error is the biggest threat to their organisation's cyber security.

An important aspect of any cyber security strategy is acknowledging that everyone has a role to play in keeping the organisation safe. Hackers, for example, look for weaknesses across the board, not just in the IT department.

Cyber Agile Organisations understand this, with three-quarters (**75%**) of their leaders claiming that every employee within their organisation knows they are responsible for IT security, compared to **64%** of non-cyber agile organisations.

$3.5m invested in cyber security training.

Investing in people

It seems that organisations are putting their money where their mouth is, investing on average $3.5 million each in cyber security training in the last 12 months.

Of course, this investment must be strategically allocated. When evaluating the strength of their organisation's cyber security skills and knowledge, business leaders identify the following areas of weakness.

Organisations' five greatest cyber weaknesses

1. Network security practices
2. Operational technology (OT) security
3. Phishing awareness
4. Digital identity management
5. Data protection and encryption

Specialist skill sets

Developing a diverse toolkit of cyber security skills gives organisations the best chance to build resilience against cyber threats. Cyber Agile Organisations are more likely to have these specialist capabilities in place, with **61%** already employing a Chief Information Security Officer compared to **52%** of other organisations.

Additionally, **55%** already have a Security Operations Centre Analyst, and **52%** have a Cyber Security Architect.

Currently, **43%** of Cyber Agile Organisations are actively recruiting for AI and Machine Learning Security Specialists, and **40%** are recruiting for Security Compliance Specialists. This highlights the diverse skill sets required to survive and thrive in the current environment.

52%

of organisations have a Cyber Security Architect

Steps to cyber agility: Supercharging skills

1

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.

2

Build awareness

It's not good enough to confine cyber security learnings and protocols to the IT crowd. Organisations that build company-wide awareness about the importance of staying safe stand a better chance of resisting attacks. Your people should feel empowered to report potential threats.

3

Train to gain

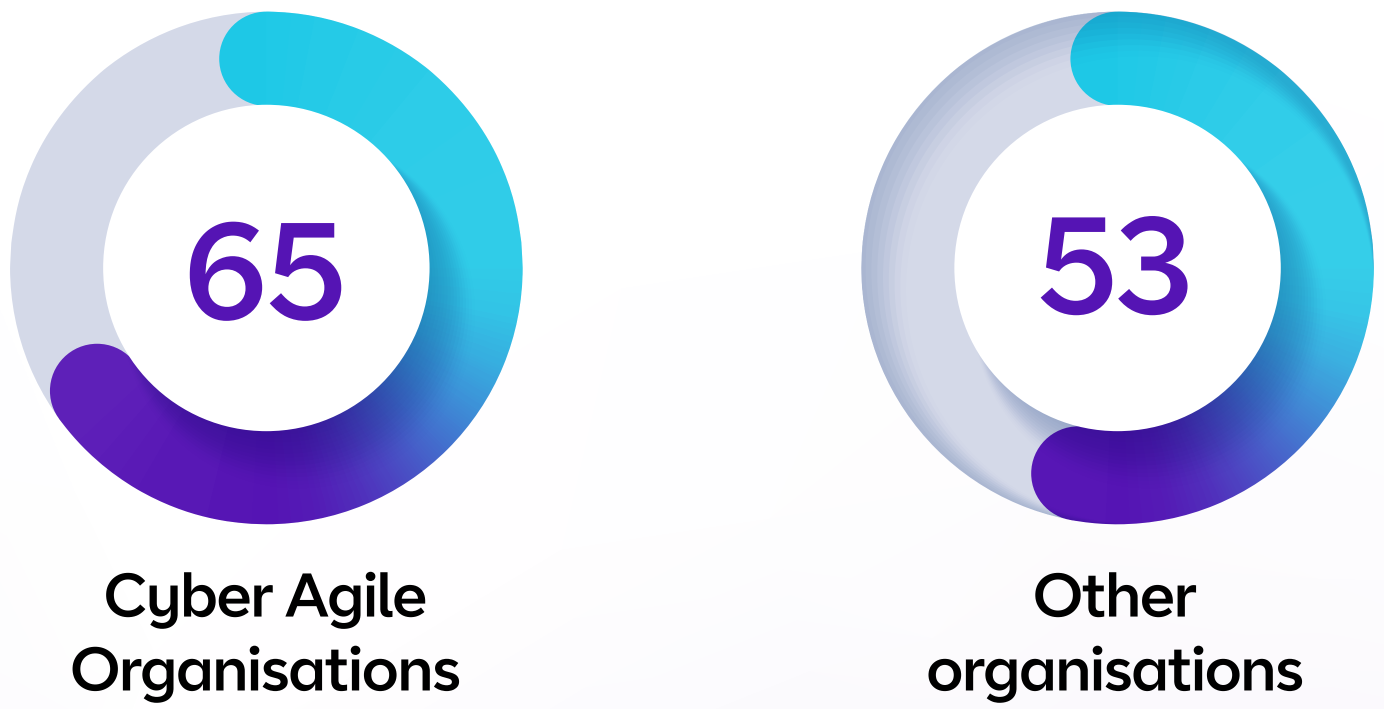
Because cyber threats are constantly changing, it's important that your people stay in touch with the latest developments in this space. Invest in training to upskill everyone from new recruits to old hands to build knowledge and encourage a proactive approach to cyber security.

Dimension 6
Innovation

Dimension 6 Innovation

Cyber security is no longer just a protective measure – it provides a platform for innovation and transformation, helping you work smarter and more collaboratively with a view to building fast, sustainable growth.

Average Innovation scores



> "Innovation needs a secure IT ecosystem to flourish. Forward-thinking businesses understand this, and are shifting their perspective on cyber security from a defensive measure to a platform that helps unleash creativity and achieve wider transformation goals".
>
> **Lee Stephens**, Director of Security Advisory Services, BT

Innovate to secure

Technology waits for no one, so organisations' security must keep up. Leaders in cyber agility are implementing innovative solutions that enhance cyber security at every stage.

When it comes to mitigating threats, Cyber Agile Organisations are leveraging threat intelligence platforms and enlisting ethical hackers to pinpoint vulnerabilities. Many are also adopting zero trust architecture to enhance their system security.

Additionally, Cyber Agile Organisations are using identity threat detection and response (ITDR) solutions and automated incident response mechanisms to minimise damage and aid rapid recovery when incidents do occur.

And these innovations are paying off. Cyber Agile Organisations are almost twice as likely as others to report that their incident resolution and recovery process has been extremely useful in mitigating the impact of cyber security threats, ensuring quick recovery and minimal disruption.

The top five cyber security innovations implemented by Cyber Agile Organisations

1 Threat intelligence platforms

2 Identity threat detection and response (ITDR)

3 Recruiting an 'ethical' hacker to test cyber security

4 Automated incident response

5 Zero trust architecture

AI risk and reward

Artificial intelligence, despite bringing a huge boost to innovation and experimentation across industries, is also contributing to cyber risk. Some **73%** of leaders across all organisations say the explosion of generative AI and shadow AI in the workplace has made cyber security more important than ever.

However, AI also has a role to play in mitigating cyber threats. More than two-thirds (**68%**) of organisations in our study have either fully implemented or partially implemented AI or machine learning for threat detection.

By implementing automation solutions to help manage the high volume of incidents, organisations can allocate more resources towards tackling critical cyber security issues and strengthening response strategies.

Secure to innovate

Cyber Agile Organisations are innovative organisations, according to findings from our research.

82%

Over three-quarters (**82%**) of leaders in these organisations believe that by innovating their approach to cyber security, they become more innovative overall.

Robust cyber security serves as a foundation for innovation by mitigating the threats surrounding new technologies and initiatives. When security is prioritised, teams can focus on developing and implementing creative solutions without the fear of compromising sensitive data or facing disruptions.

Steps to cyber agility: Driving innovation

1

Collaborate for continual improvement

Security doesn't stand still, but collaboration can help you keep up. Partner with organisations within your industry, or even internally between different departments, to understand where you can innovate. A strategy of continuous loop improvement increases your chances of staying ahead.

2

Embrace change

Revisit, assess and adapt cyber strategies to account for new and disruptive technology, particularly AI and, further off, quantum computing. At the same time, embracing the latest cyber security solutions will facilitate technological advances, mitigating threats without encumbering teams. This way, cyber security can provide a platform for greater efficiency and organisational agility.

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

Resilience

Cyber security is a fundamental building block for improving business performance, with our findings showing that Cyber Agile Organisations see greater growth than their non-cyber agile peers.

Advantage

The twin advantage of reducing risk while enhancing performance puts Cyber Agile Organisations in the driving seat in a brave new world powered by AI and other game-changing technologies.

By blending robust security protocols with the best new tech, businesses have the opportunity to grow sustainably and mitigate the inevitable risks accompanying any major leap forward.

Future-proof

Cyber Agile Organisations are the future of business. They are ready to partner, to collaborate, and to surprise and delight users, clients, and customers.

If you already qualify as a Cyber Agile Organisation, then congratulations. But don't celebrate for too long, because keeping pace with best practice is a full-time job. If you fall shy of this leading group, all is not lost; now is the time to assess your strategy, invest in the right tools, train your people, and pivot to improve your cyber agility.

BT: Your partner for cyber agility

BT is leading the way in creating advanced cyber security solutions for a new era of business. We are prioritising innovations in artificial intelligence and machine learning to keep our customers safe, secure and ready for what's next.

With our support, organisations can secure operational technology down the supply chain and at every touchpoint to reduce multifaceted risks.

> **This frees up businesses to collaborate with partners and drive unrestricted growth.**

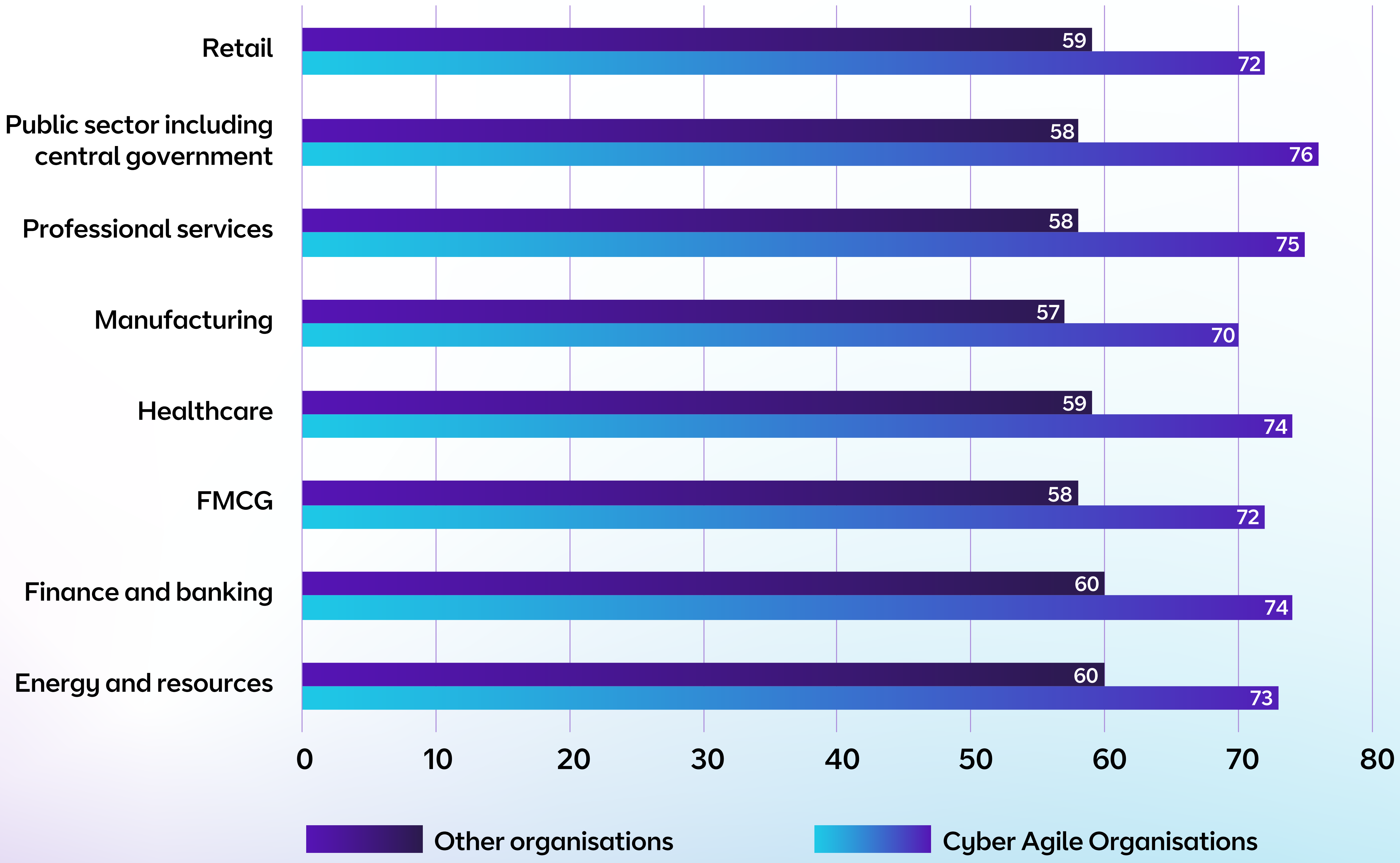
Our managed security controls ensure business continuity, with **round-the-clock support** from our expert team keeping your business safe from cyber attacks. We also offer consulting to help you at every stage of your security journey.

Our talented cyber security professionals assess, build and test your defences, to create effective security strategies that are easy to adopt. Plus, we support boardroom buy-in, to ensure smooth communication, adoption and progression towards cyber agile status.

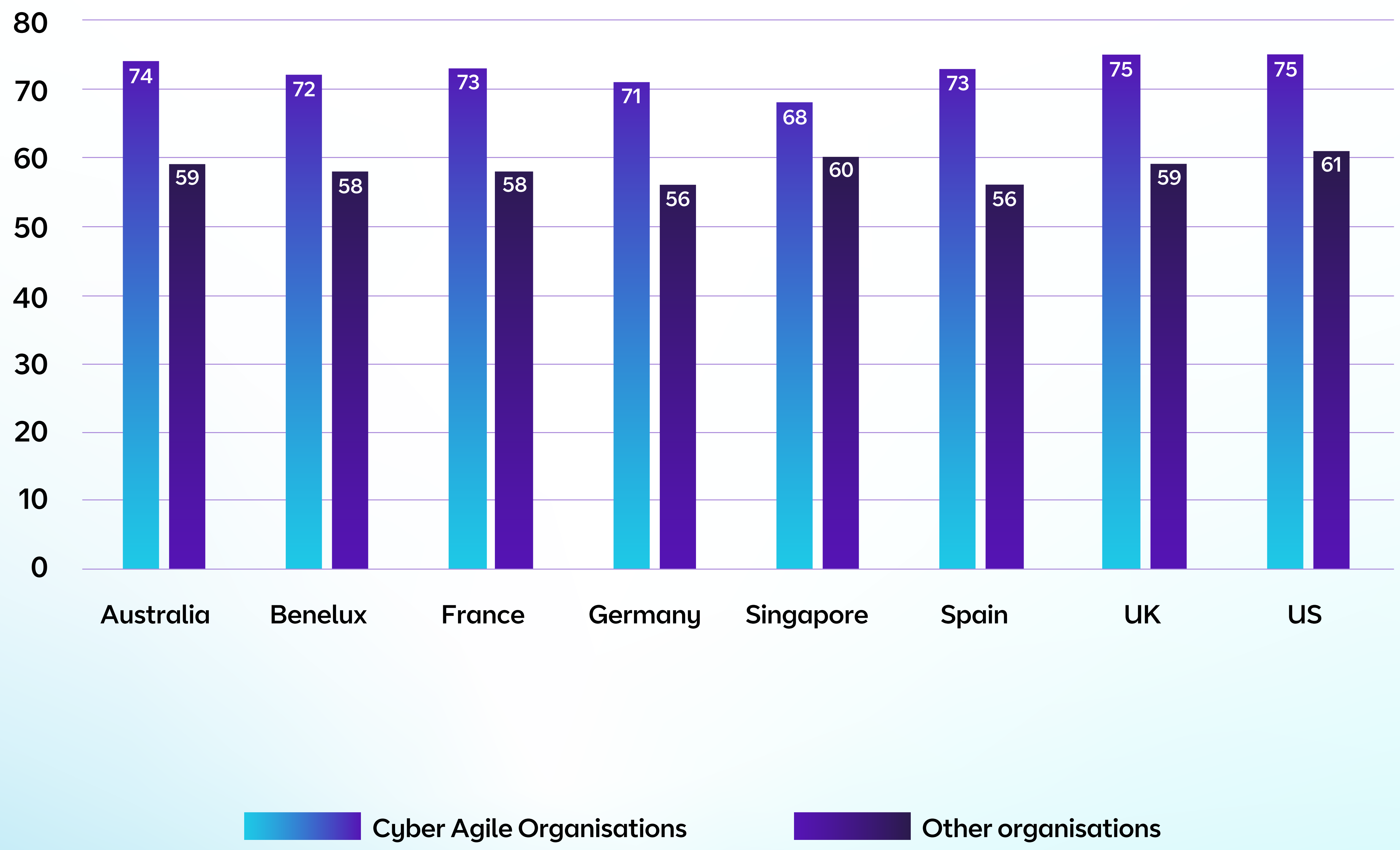
Appendices - Industry and market scores by dimension

Dimension 1: Awareness

Average Awareness score by industry



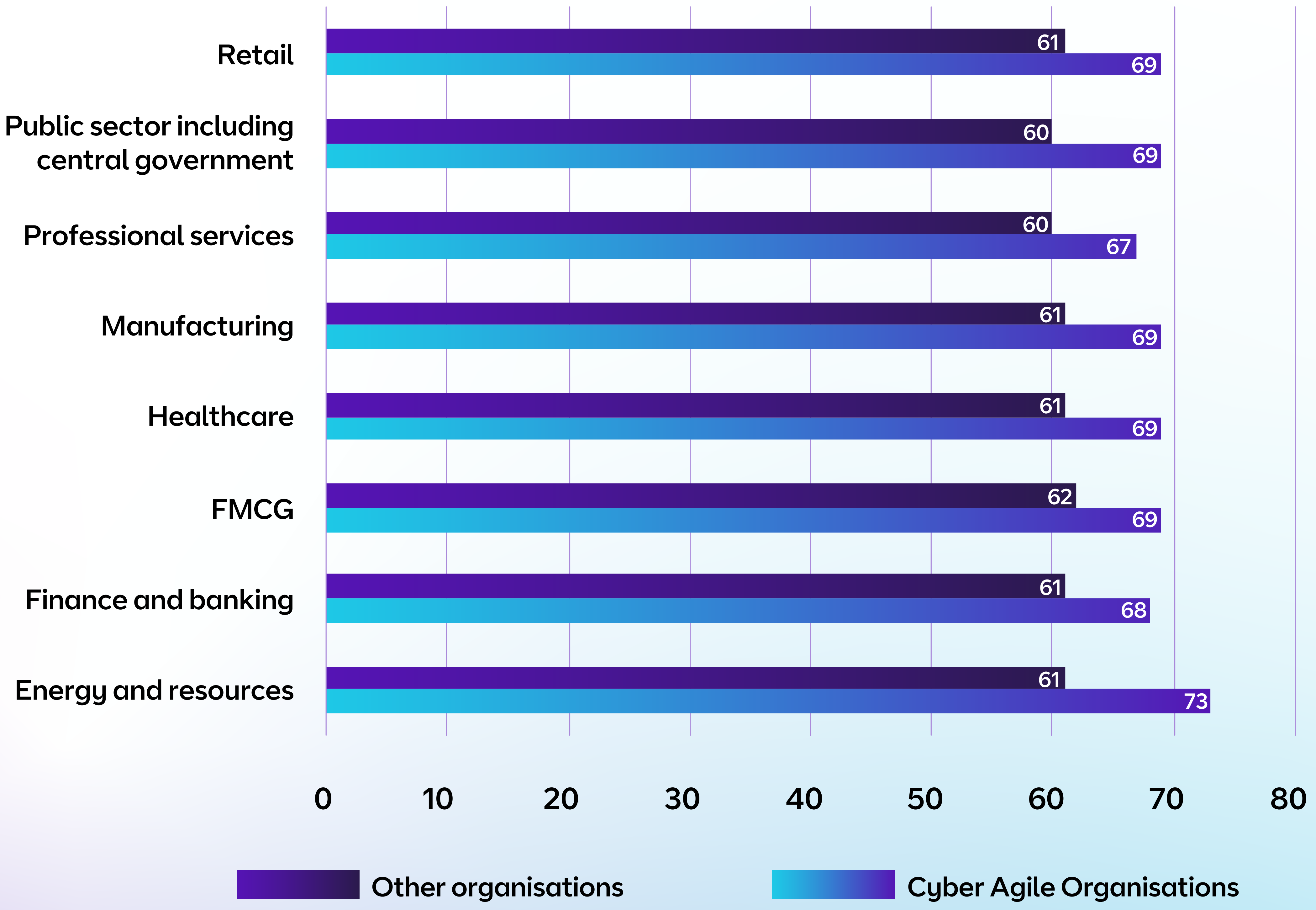
Average Awareness score by market



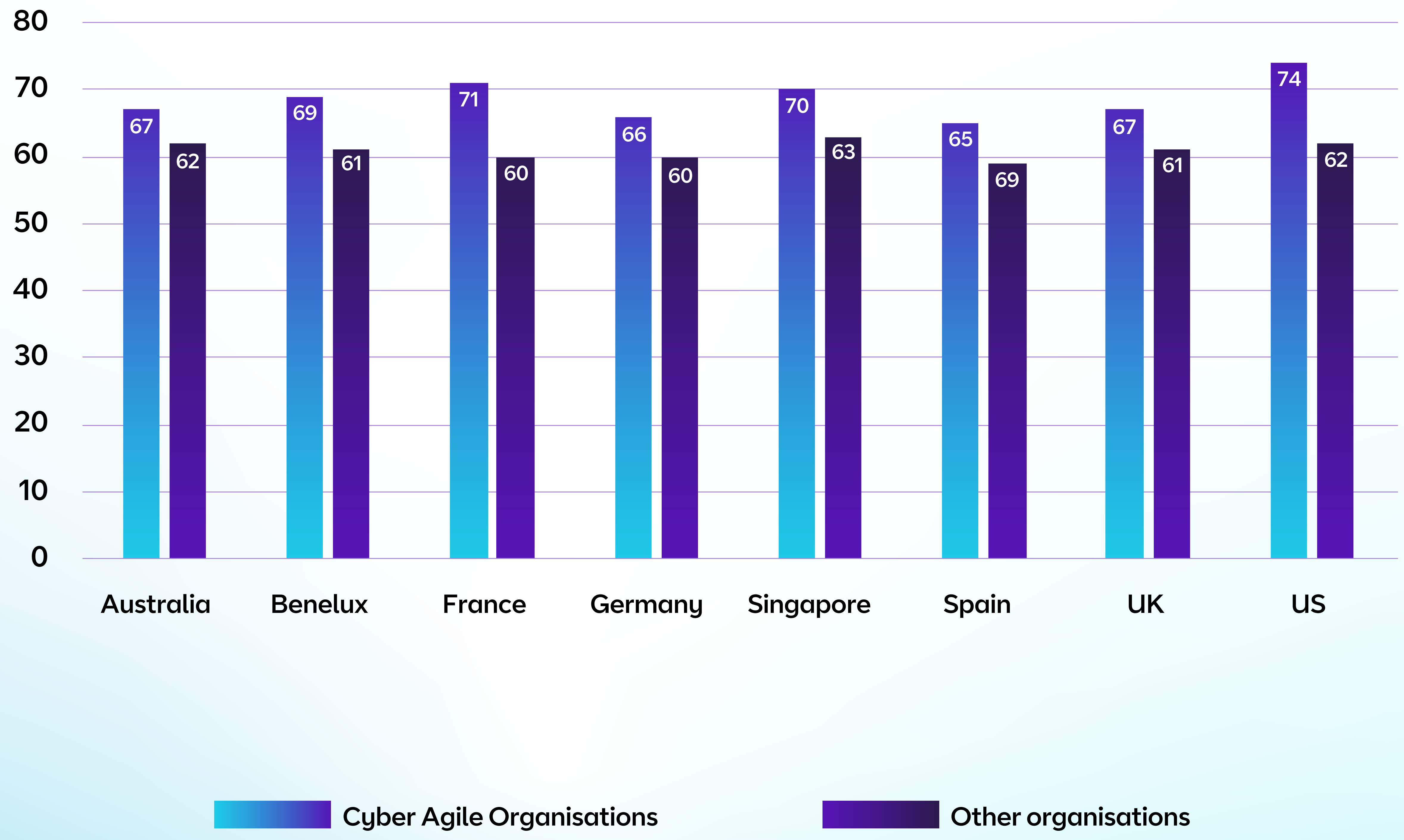
Appendices - Industry and market scores by dimension

Dimension 2: Compliance

Average Compliance score by industry



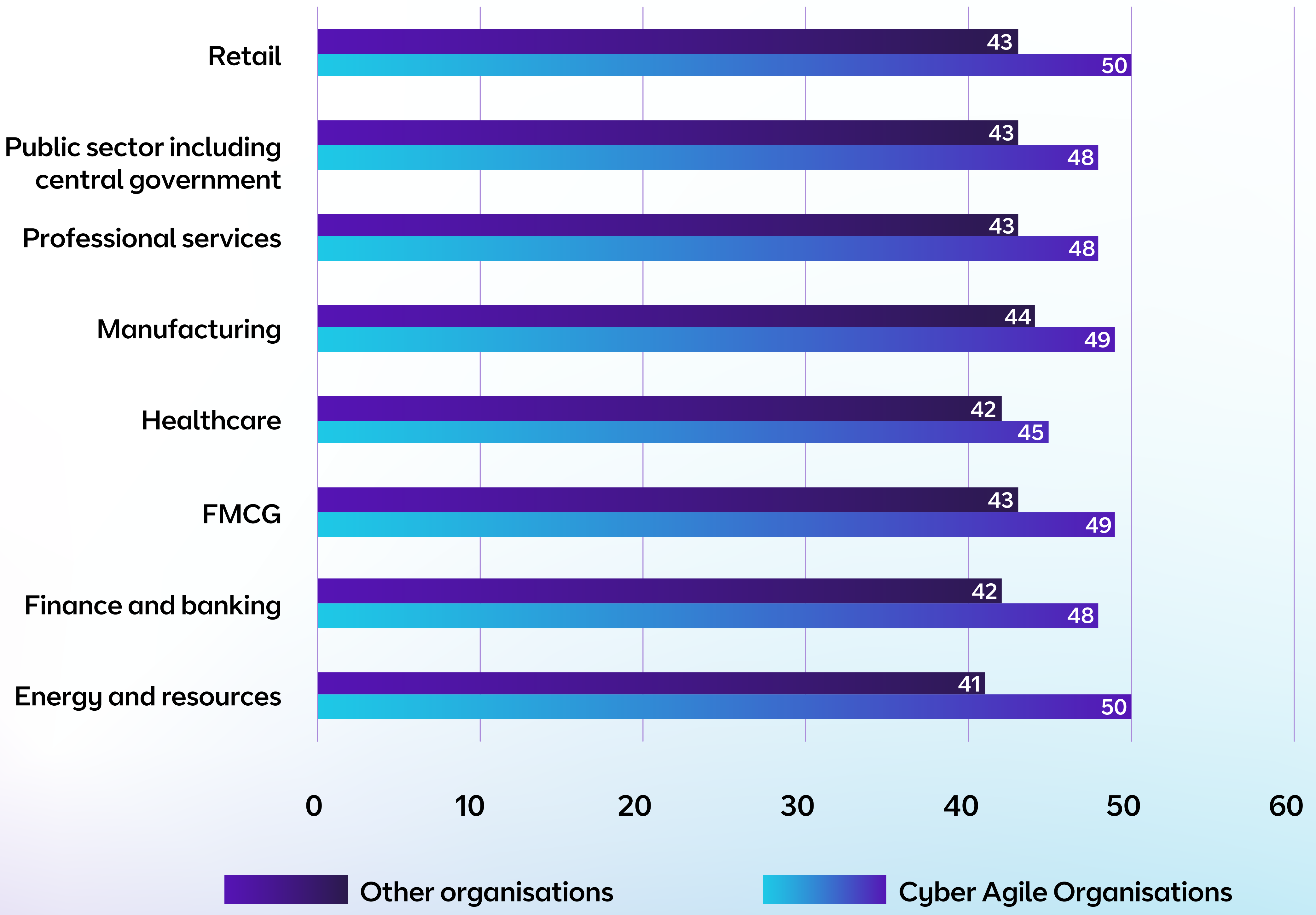
Average Compliance score by market



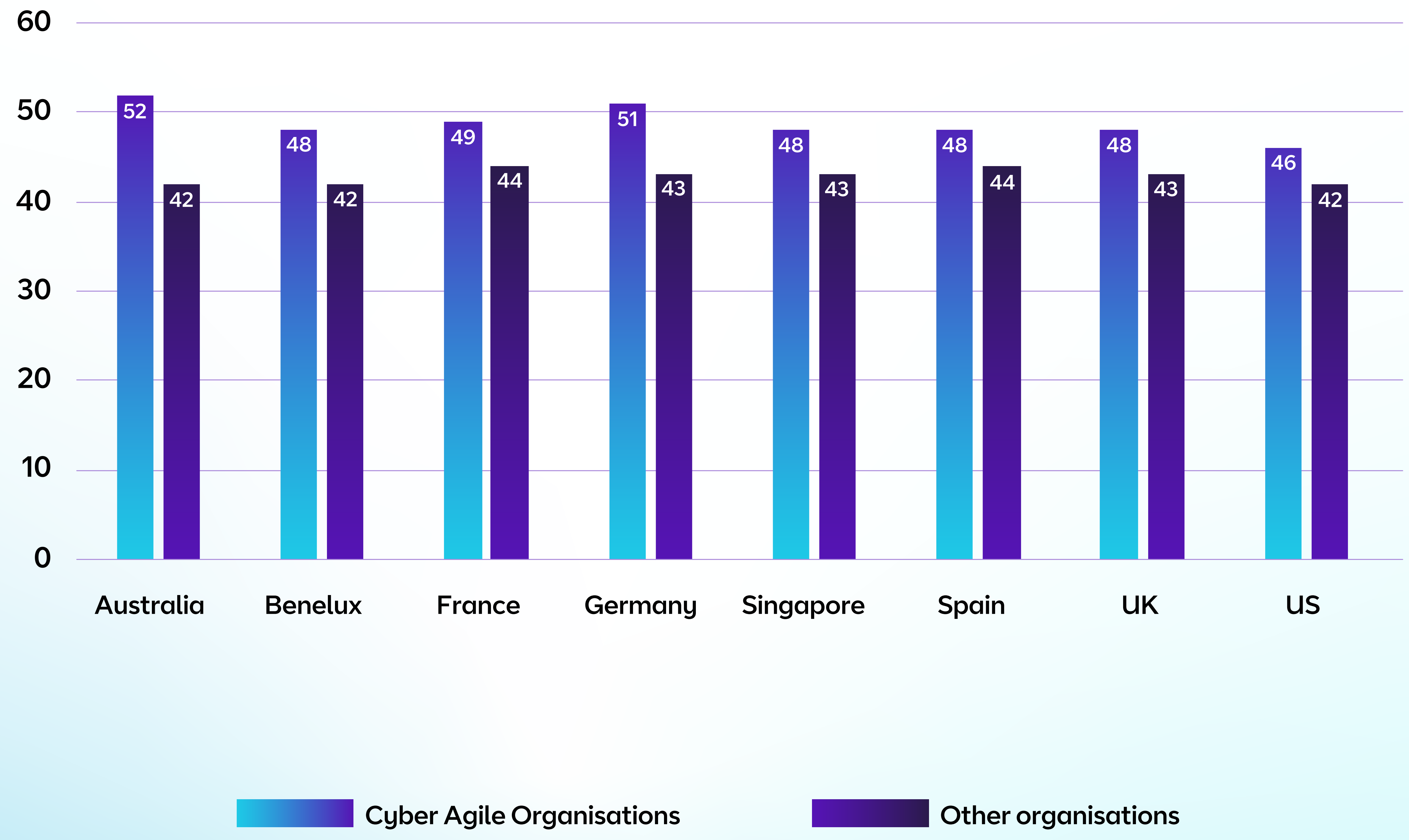
Appendices - Industry and market scores by dimension

Dimension 3: Connectivity

Average Connectivity score by industry

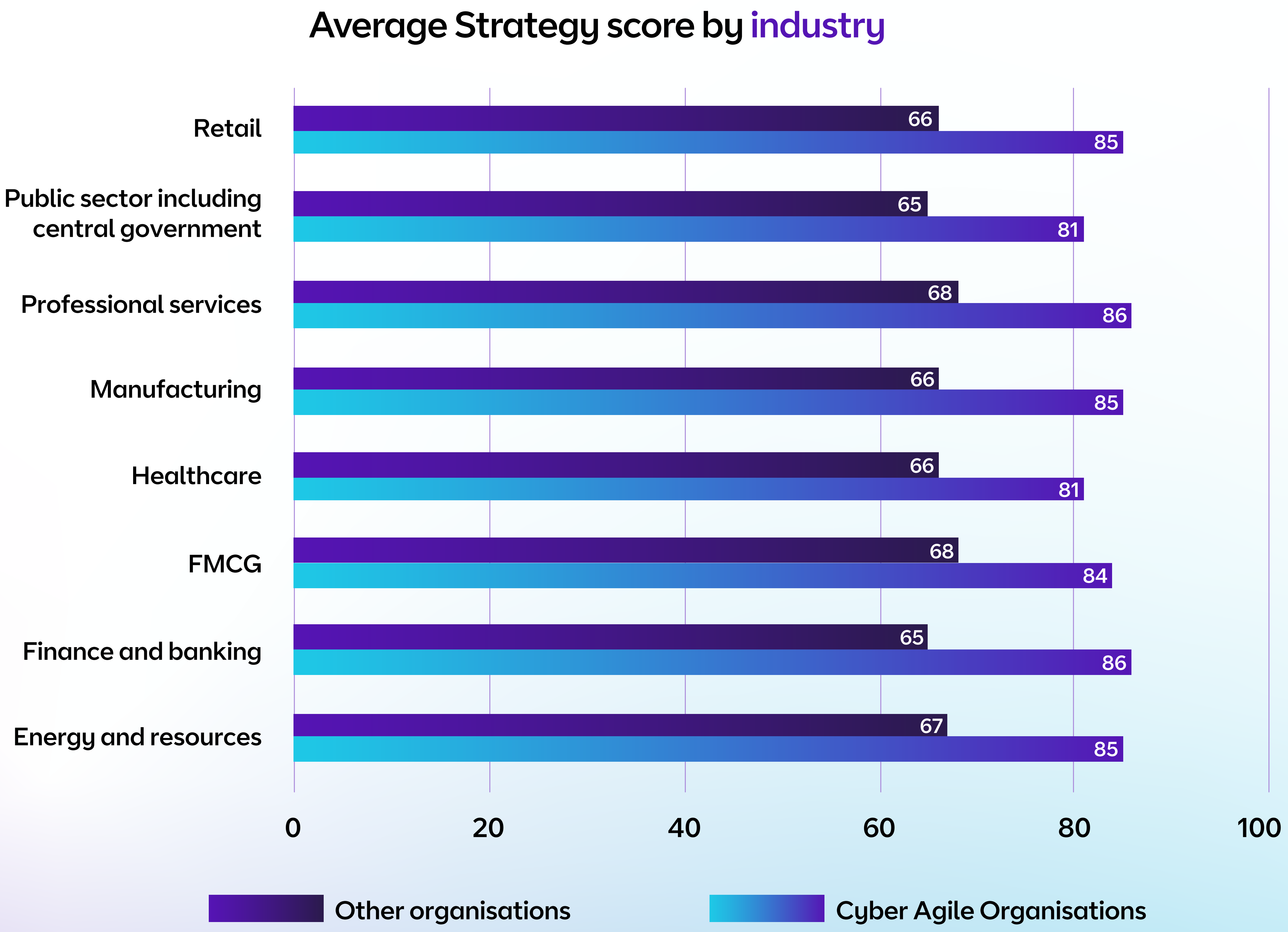


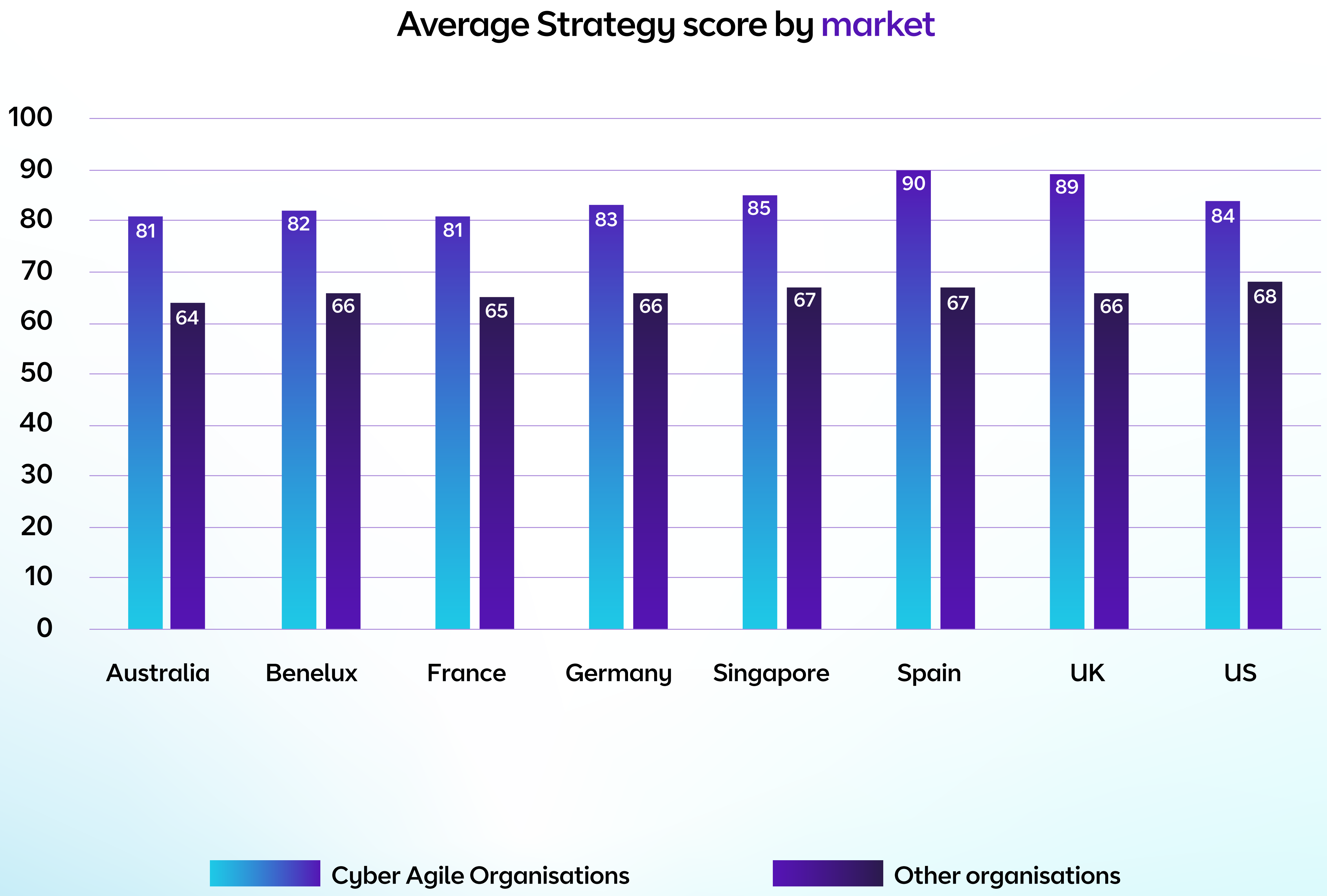
Average Connectivity score by market



Appendices - Industry and market scores by dimension

Dimension 4: Strategy

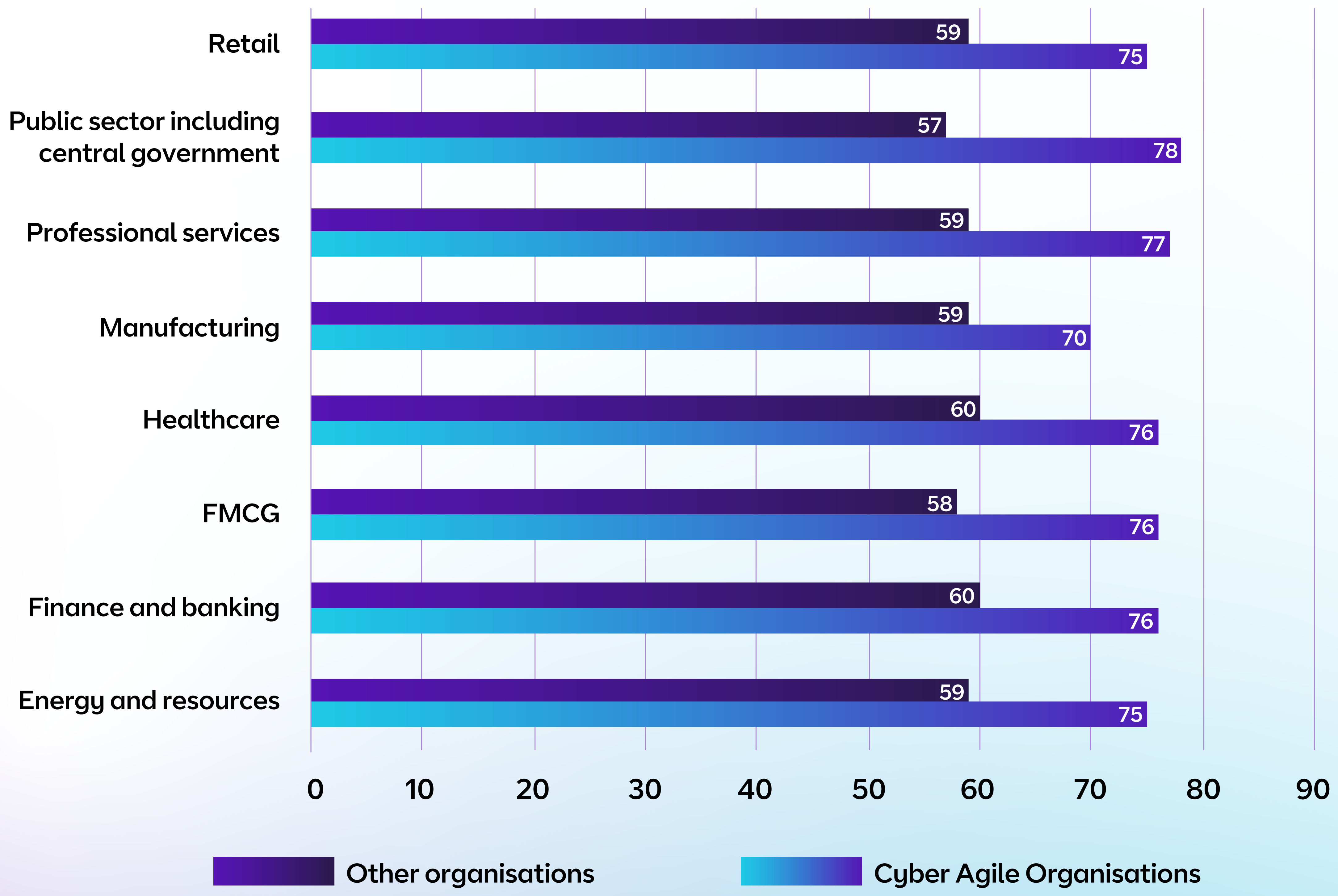




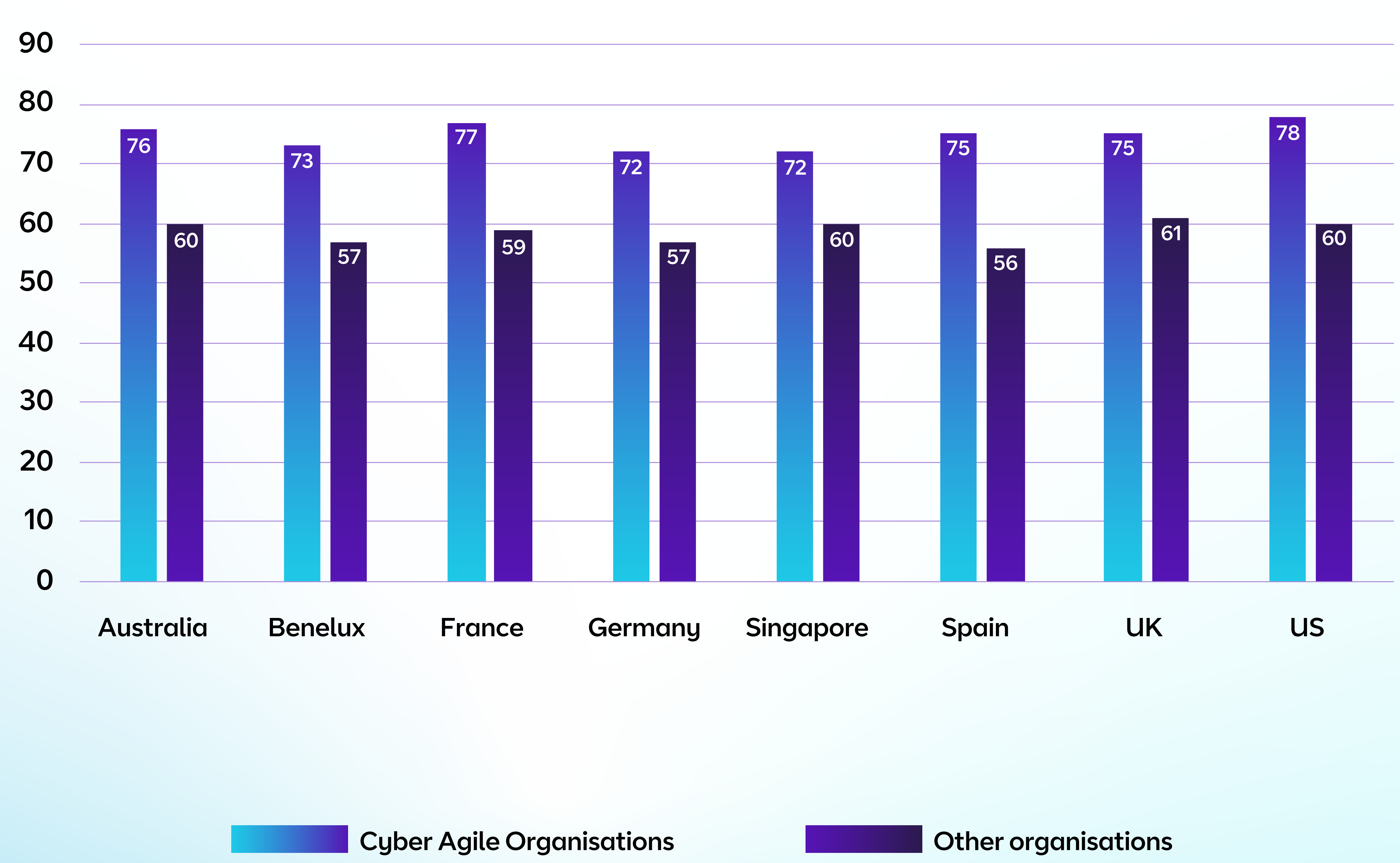
Appendices - Industry and market scores by dimension

Dimension 5: Skills

Average Skills score by industry



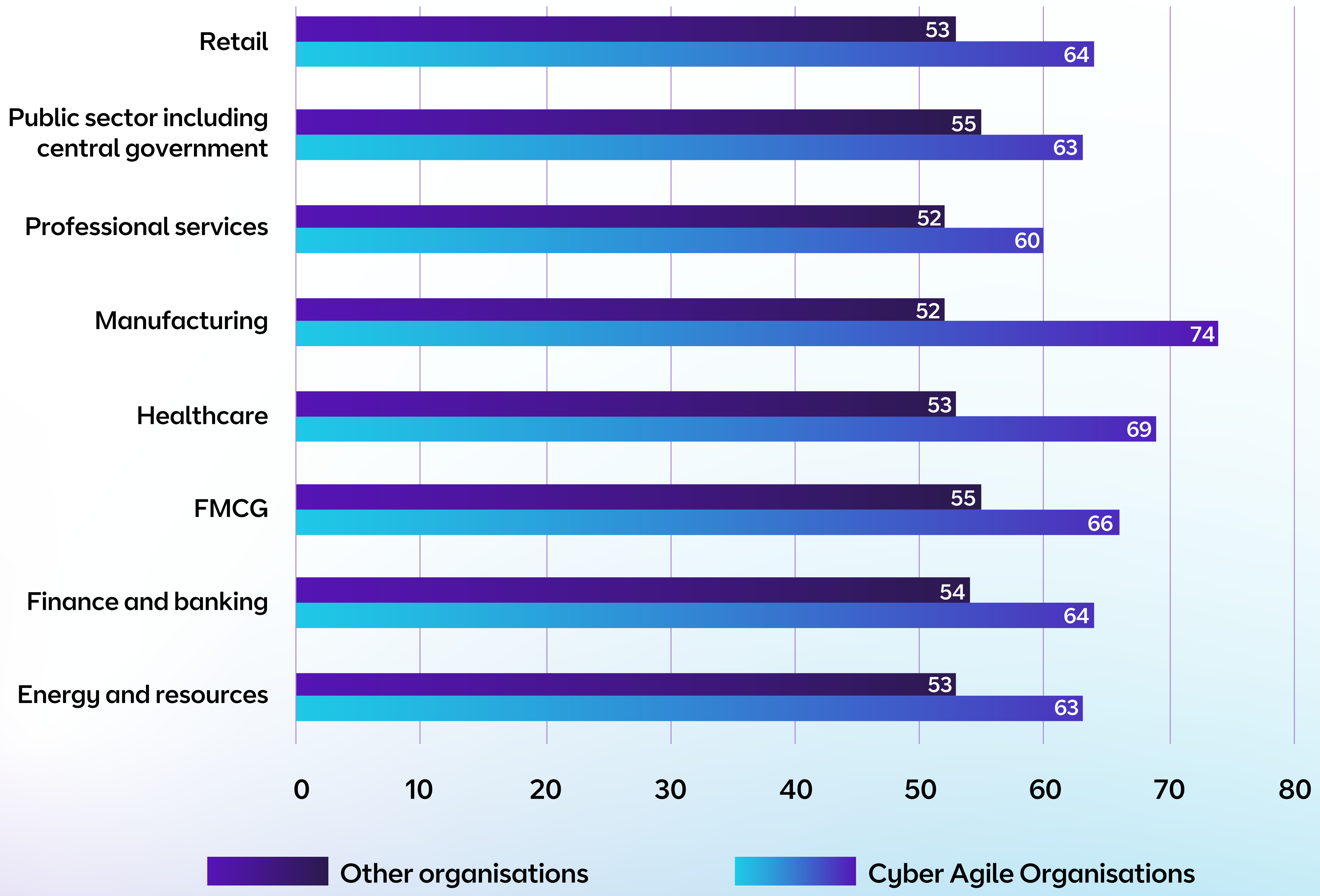
Average Skills score by market



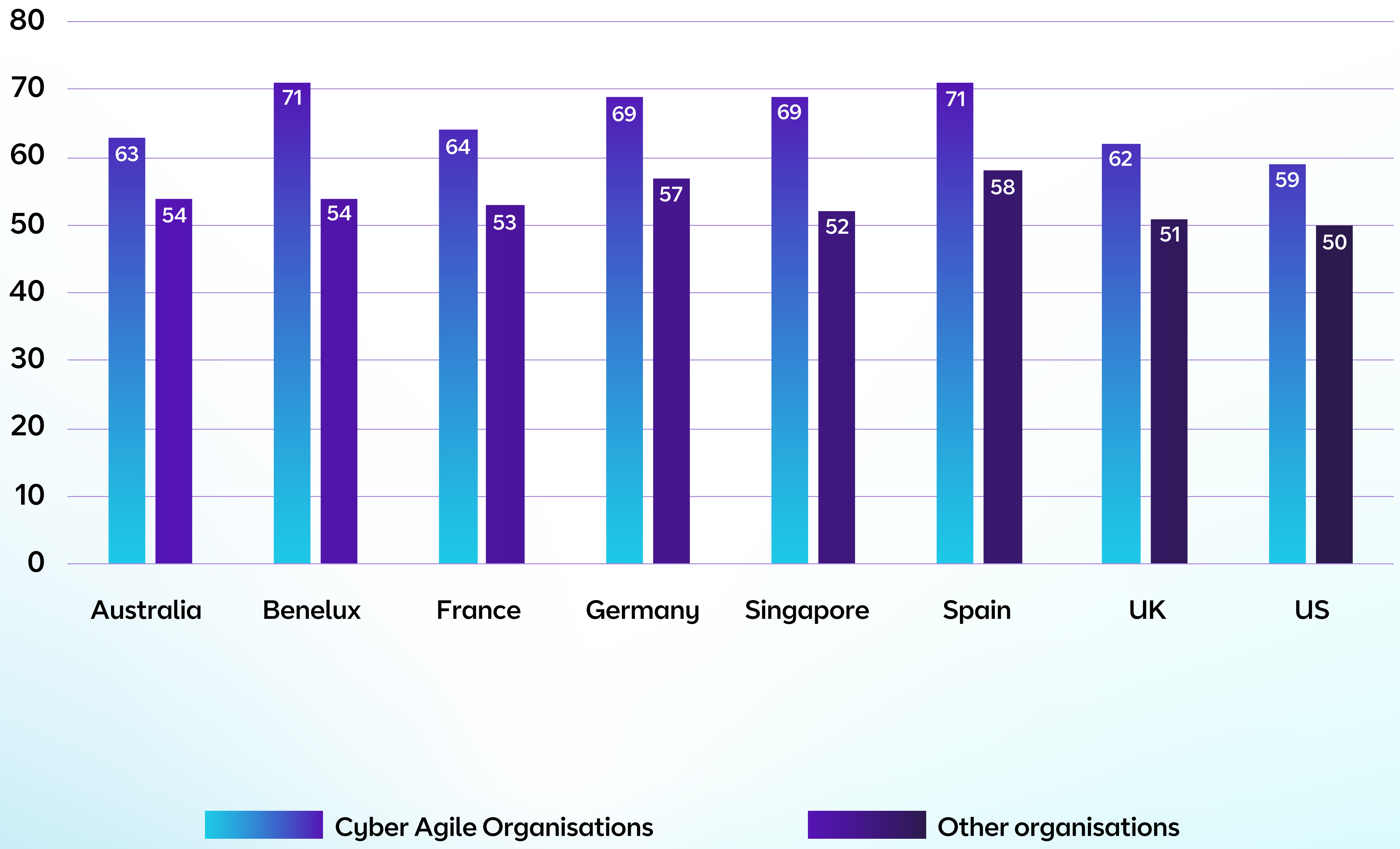
Appendices - Industry and market scores by dimension

Dimension 6: Innovation

Average Innovation score by industry



Average Innovation score by market



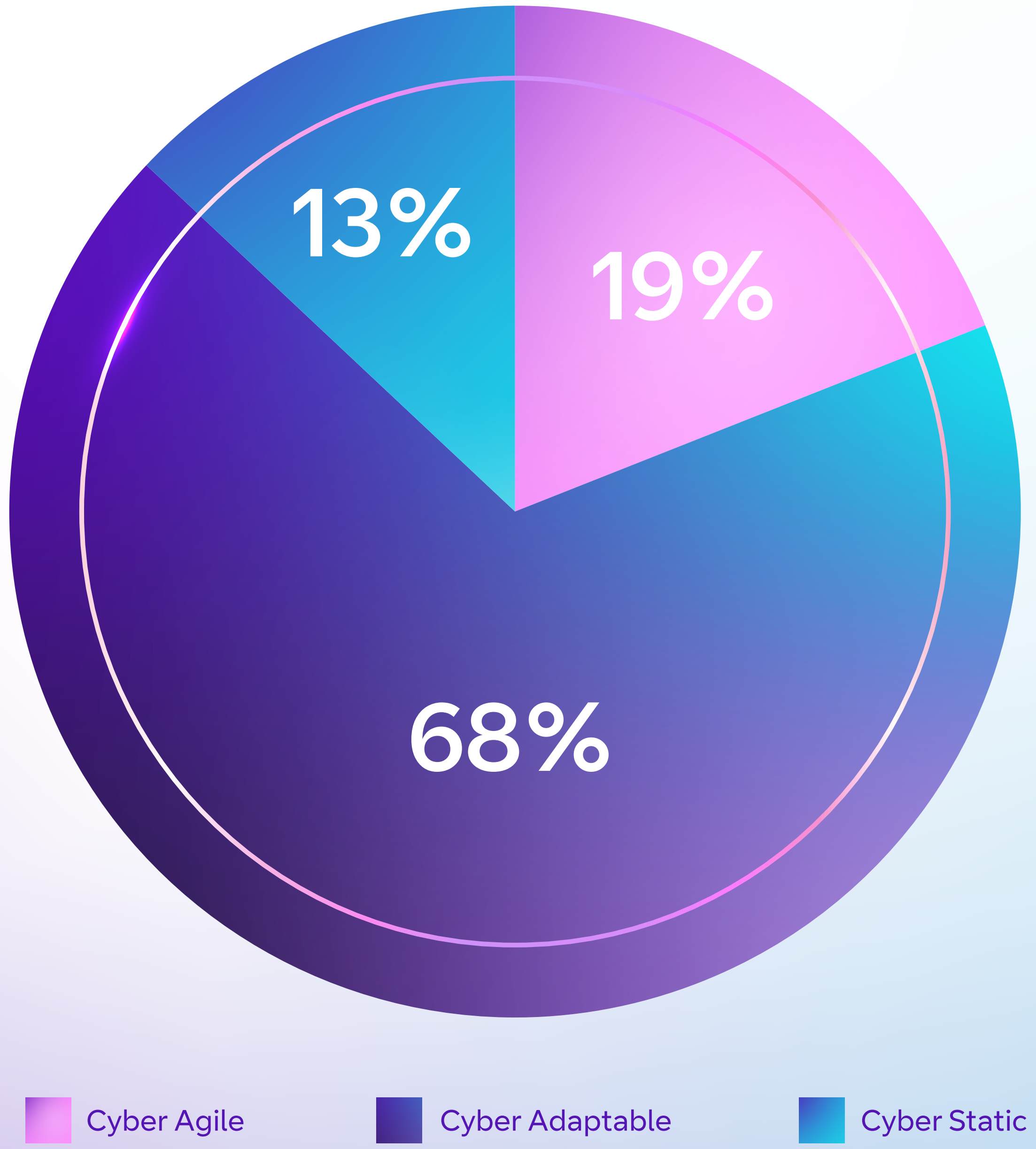
Detailed methodology

Opinion research

The Cyber Agile Organisation is based on an independent opinion research study carried out by BT in late 2024, in partnership with Man Bites Dog and with research completed by Coleman Parkes Research.

Cyber agility scores are based on six dimensions: **Awareness**, **Compliance**, **Connectivity**, **Strategy**, **Skills** and **Innovation**. To assess how organisations performed against each dimension, the opinion research data was run through a bespoke scoring system.

Based on these scores, organisations were divided into three groups:



Group	Total aggregated score boundaries	% of research sample
Cyber Agile	66-100	**19%**
Cyber Adaptable	52-65	**68%**
Cyber Static	35-51	**13%**

Using the groups, it was possible to distinguish between Cyber Agile Organisations and the rest of the organisations that fell into the Cyber Adaptable and the Cyber Static groups to provide a clear comparison.

The research sample consisted of 2,500 C-suite leaders from organisations across eight industries and eight markets.

2,500 C-suite leaders Minimum company turnover: $500m	**1,275 IT C-suite leaders** • Chief Technology Officer • Chief Information Security Officer • Chief Information Officer • Chief Security Officer • Chief Privacy Officer **1,225 other C-suite leaders** • Chief Executive Officer • Chief Financial Officer • Chief Operating Officer • Chief Compliance Officer • Chief Risk Officer • General Counsel
8 industries	• Energy and resources • Finance and banking • FMCG • Healthcare • Manufacturing • Professional Services • Public sector including central government • Retail
8 markets	• UK • USA • Benelux • France • Germany • Spain • Australia • Singapore

Detailed methodology

Further detail on each dimension and the scoring system:

Each dimension comprised a set number of questions, which were attributed different weightings. In total, each dimension was valued at 30 points, making 180 the best possible score across the six dimensions. **This figure was recalibrated to return a final result out of 100.**

Dimension	Criteria	Question weighting	Dimension weighting
Awareness	An organisation's level of visibility and resiliency of its IT ecosystem.	15	30
	How often an organisation reviews and updates its cyber security policies.	5	
	The information sources that an organisation uses to assess risk from cyber threats.	10	
Connectivity	How an organisation characterises its approach to cyber security within the organisation's IT network.	15	30
	The cyber security risks posed by various factors within an organisation's network and the associated level of risk.	15	
Compliance	An organisation's approach to dealing with changes in cyber security regulations.	4	30
	The measures that organisations have in place to ensure it complies with cyber security regulations.	11	
	The barriers preventing an organisation from proactively complying with cyber security regulations.	15	
Strategy	The parameters for cyber security strategies within an organisation.	30	30
Innovation	The implementation of various innovative cyber security technologies within an organisation.	30	30
Skills	An organisation's current recruitment plans for security related roles.	10	30
	An organisation's approach to cyber security upskilling.	5	
	The strength of an organisation's skills and knowledge in various areas of cyber security.	15	
		Total	180

Detailed methodology

Economic modelling

To estimate the potential macroeconomic benefits of improving the cyber agility of the businesses not deemed 'Cyber Agile Organisations' BT and Man Bites Dog engaged Capital Economics to build an economic model. The model estimated the impact at both a total revenue and gross value added[3] (GVA) level across the eight focus markets as well as the manufacturing and finance sector globally.

The methodology consisted of three core phases:

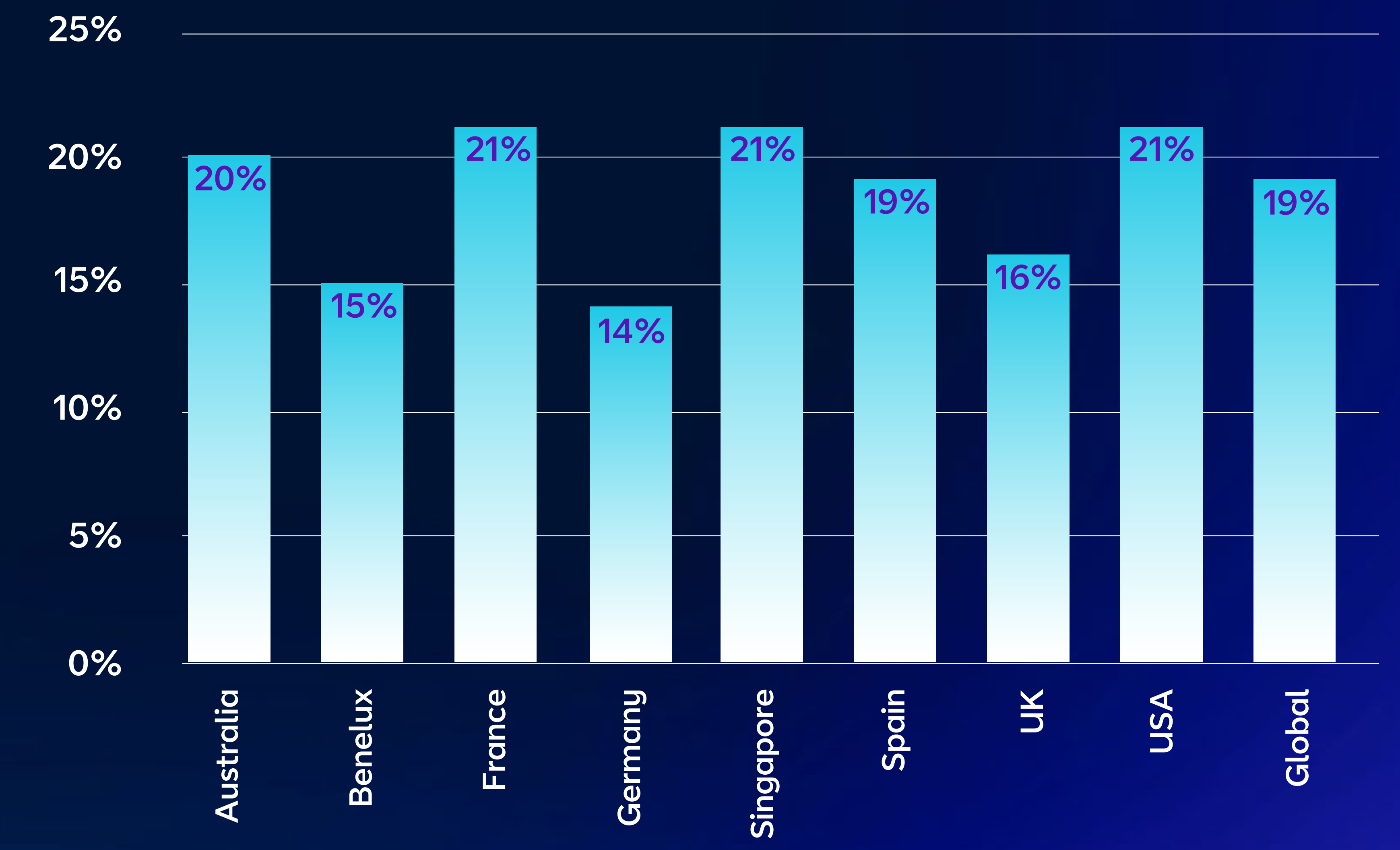
1. **Estimate the total revenue and GVA impact of large firms across the eight markets in the study (i.e. firms with a revenue of over $500mn to match our research sample)**
   Data sources used for revenue by business size included the ONS (for the UK), Eurostat (for Benelux, France, Germany and Spain), ABS (for Australia), Singstat (for Singapore) and the BEA (for the US).

   These statistics were also cross referenced and supplemented by data from the OECD. Due to data availability, estimates for the number of firms with revenue over $500 million were made using data on businesses and turnover by employment size-bands. To estimate GVA we used turnover-to-GVA ratios from OECD input-output tables.

2. **Ascertain the proportion of these firms that could be classified as Cyber Agile Organisations**
   The proportion was derived from our survey data and was applied on a by market basis. We applied this data to the estimates from Phase 1 to produce revenue and GVA estimates of cyber agile and non cyber agile large firms.

[3] 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. It is a key input into GDP at the national level and is used to measure economic value for subsets of the economy as it avoids double counting as would be an issue with total income measures.

Source data: Proportion that are Cyber Agile Organisations

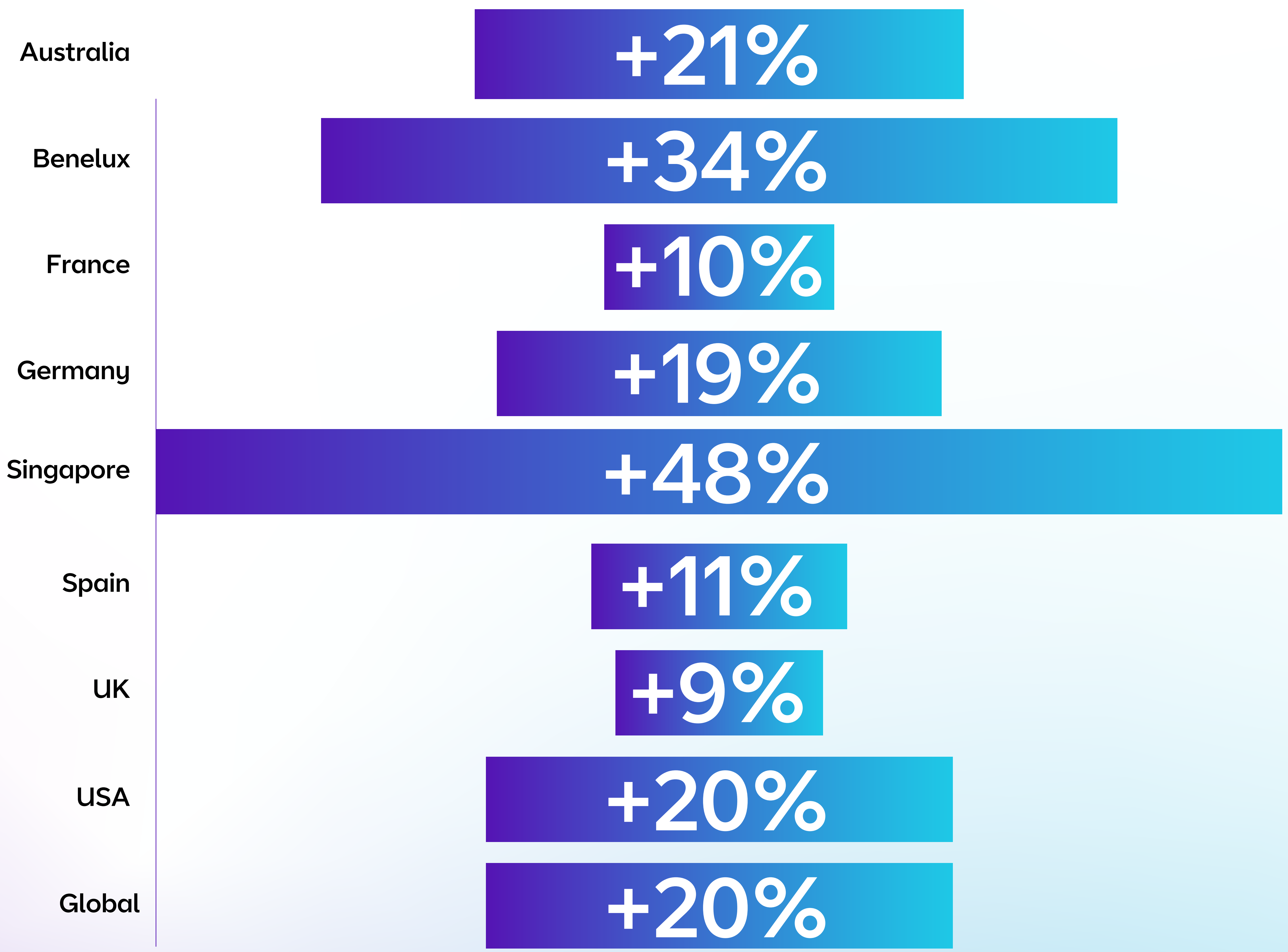


3. **Calculate the potential increase in revenue and GVA of businesses not classed as cyber agile if they had grown at the same rate as Cyber Agile Organisations:** A key finding from the opinion research study was that Cyber Agile Organisations, on average, had a 20% higher growth rate between 2021-2023 than other organisations (although the difference differed between markets is accounted for in the final calculations). We used this insight to apply the difference in growth rates to non-cyber-agile firms' turnover and GVA over the past three years, with 2021 as the starting point, to estimate the "missed" potential revenue and GVA for non-cyber agile firms.

This calculation represented the additional growth that non-cyber-agile firms could have achieved if they had grown at the rate of Cyber Agile Organisations across the eight markets in this study (reported in the study in GBP).

Detailed methodology

Source data: Percentage difference in growth rate between Cyber Agile Organisations and other organisations 2021-2023



Please note reasonable assumptions and proxies have been used to produce estimates where there are limitations on available data. Estimates provide indication of scale of potential benefits, but modelling does not account for causality or displacement effects.

About BT Group

BT Group is the UK's leading provider of fixed and mobile telecommunications and related secure digital products, solutions and services. We also provide managed telecommunications, security and network and IT infrastructure services to customers across 180 countries.

BT Group consists of three customer-facing units: Consumer serves individuals and families in the UK; Business covers companies and public services in the UK and internationally; Openreach is an independently governed, wholly owned subsidiary wholesaling fixed access infrastructure services to its customers - over 700 communications providers across the UK.

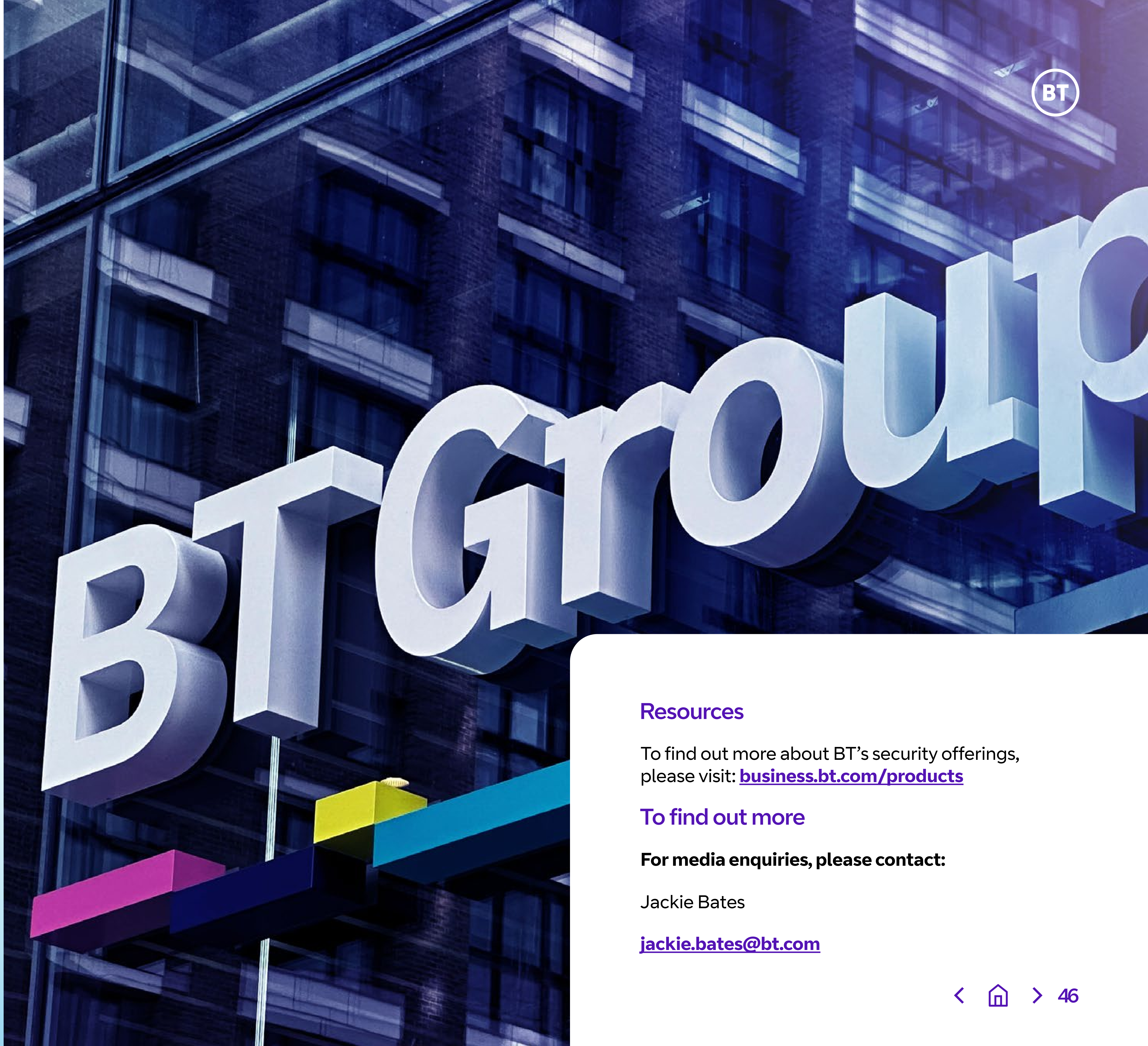
British Telecommunications plc is a wholly owned subsidiary of BT Group plc and encompasses virtually all businesses and assets of the BT Group. BT Group plc is listed on the London Stock Exchange.

For more information, visit:

Learn more

Disclaimer and acknowledgements

The concept development and research design for this report were carried out by BT and thought leadership consultancy, Man Bites Dog. The opinion research fieldwork was conducted in September and October 2024.



Resources

To find out more about BT's security offerings, please visit: business.bt.com/products

To find out more

For media enquiries, please contact:

Jackie Bates

jackie.bates@bt.com

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.

Registered in England No. 1800000. January 2025.

JN: 1634561879