



Means
Business

The Cyber Agile Organisation: Manufacturing

Transforming security
into a platform for growth

business.bt.com



Contents



Foreword	3-4
About the study	5-6
Part 1: The cyber agile advantage	7-8
The importance of being agile	9
Part 2: Becoming cyber agile: Key focus areas for manufacturing businesses	10
Preparedness: Securing the network	11-12
Performance: Manufacturing innovation	13-14
Conclusion	15
BT's got your back	16

Foreword



Manufacturing businesses are on the front line of the current digital revolution, sweeping through supply chains.

From industrial AI and robotics to cloud computing and the Internet of Things, advanced technologies are enabling more efficient methods of production.

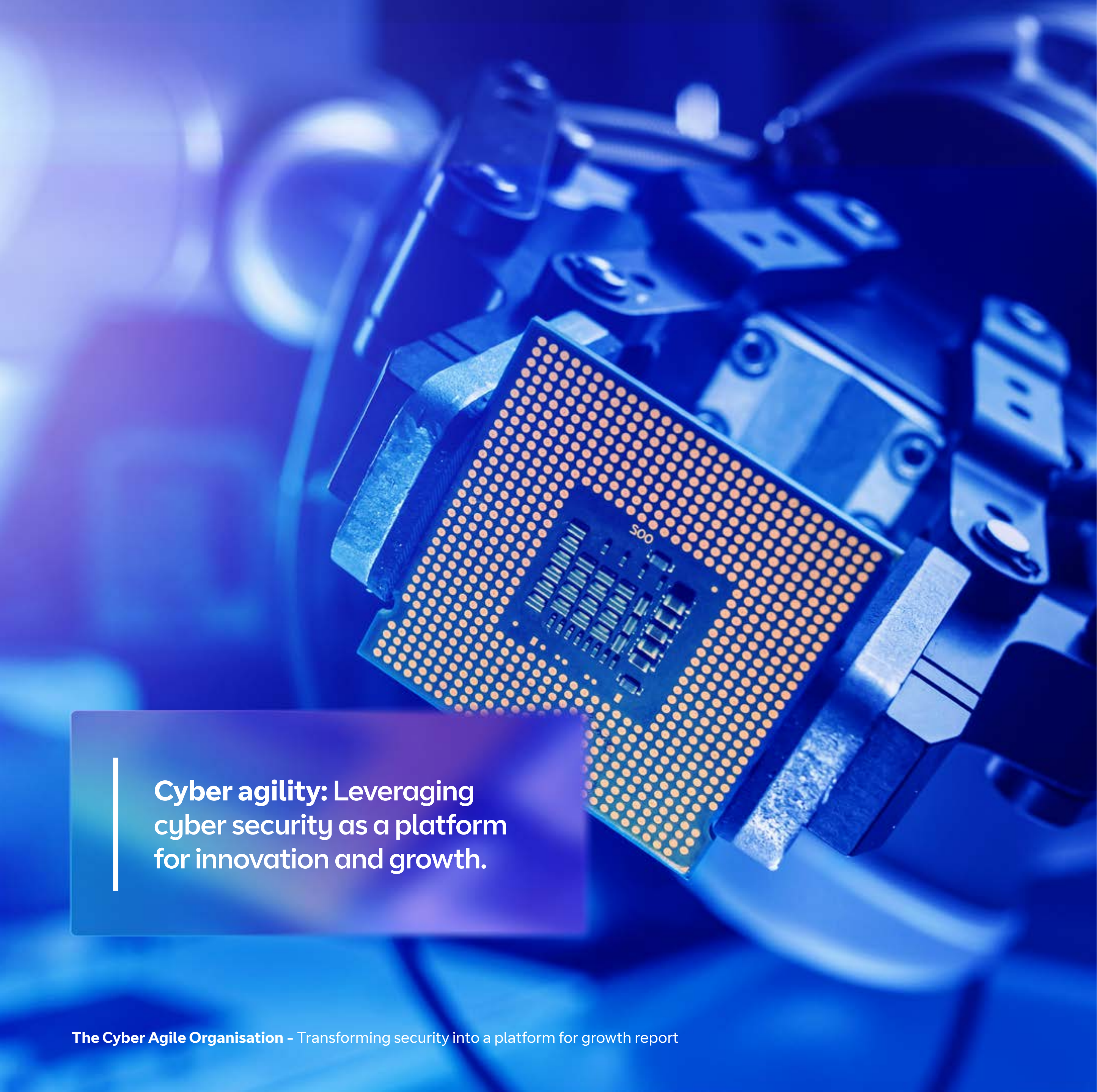
Industry 4.0 has brought opportunities for manufacturers to become leaner, more productive, and more innovative. There's potential for a streamlined supply chain, getting products to the factory gate faster and with fewer cost inputs, via innovative processes fuelled by connected devices and big data.

Leading manufacturers are proactively adopting these technologies, feeding innovation into their corporate strategies to compete on the global stage.

But with innovation comes new threats that must be identified, managed, and reduced to maintain business continuity. For example, the increased risk of IP theft and cyber attacks can result in unplanned downtime, halting production. Ensuring your security keeps pace with your development is critical. Balancing this risk-reward dynamic is the key to unlocking sustainable growth in the 21st century.

At BT, we decided it was high time to investigate the DNA of manufacturers who get this formula right. These are businesses that utilise cyber security, not just as a sticking plaster or even a shield, but as a strategic asset, a bedrock that supports growth throughout the business.

Industry 4.0 has brought opportunities for manufacturers to become leaner, more productive and more innovative.



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

Foreword



Becoming a Cyber Agile Manufacturing Organisation

We labelled the top performers ‘Cyber Agile Organisations’: businesses that mandate company-wide security training, adopt modern protocols, acquire the best security software, and proactively respond to the regulatory environment.

In doing so, they gain a strategic advantage. Safe in the knowledge that threats are repelled and risks are at a minimum, they are free to innovate, collaborate, and hit targets without worrying about vulnerabilities.

The aim of the study is to shed light on the ingredients and attributes of a Cyber Agile Organisation, providing other manufacturers with a ‘true north’ goal to aim for, as well as details of which aspects of their businesses might need an upgrade.

If you’re interested in taking your cyber security further, and want to understand the steps to 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 from organisations across eight markets and eight industries (including the manufacturing sector).

Respondents were split into two groups:

- **1,275 IT C-suite technology leaders** (166 from the manufacturing sector).
- **1,225 other C-suite leaders**, including Chief Executive Officers, Chief Operating Officers and Chief Compliance Officers (134 from the manufacturing 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.



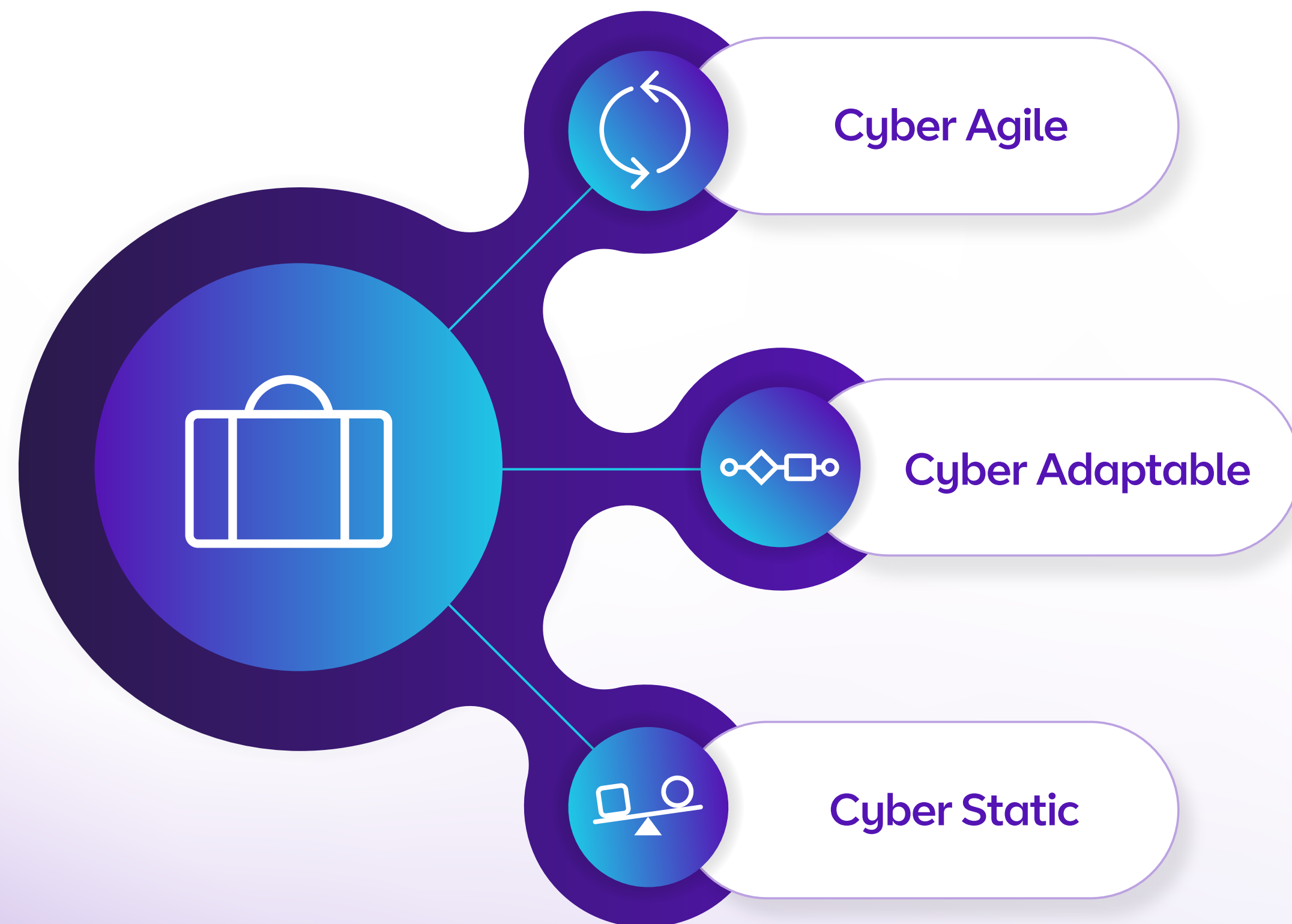
Innovation

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

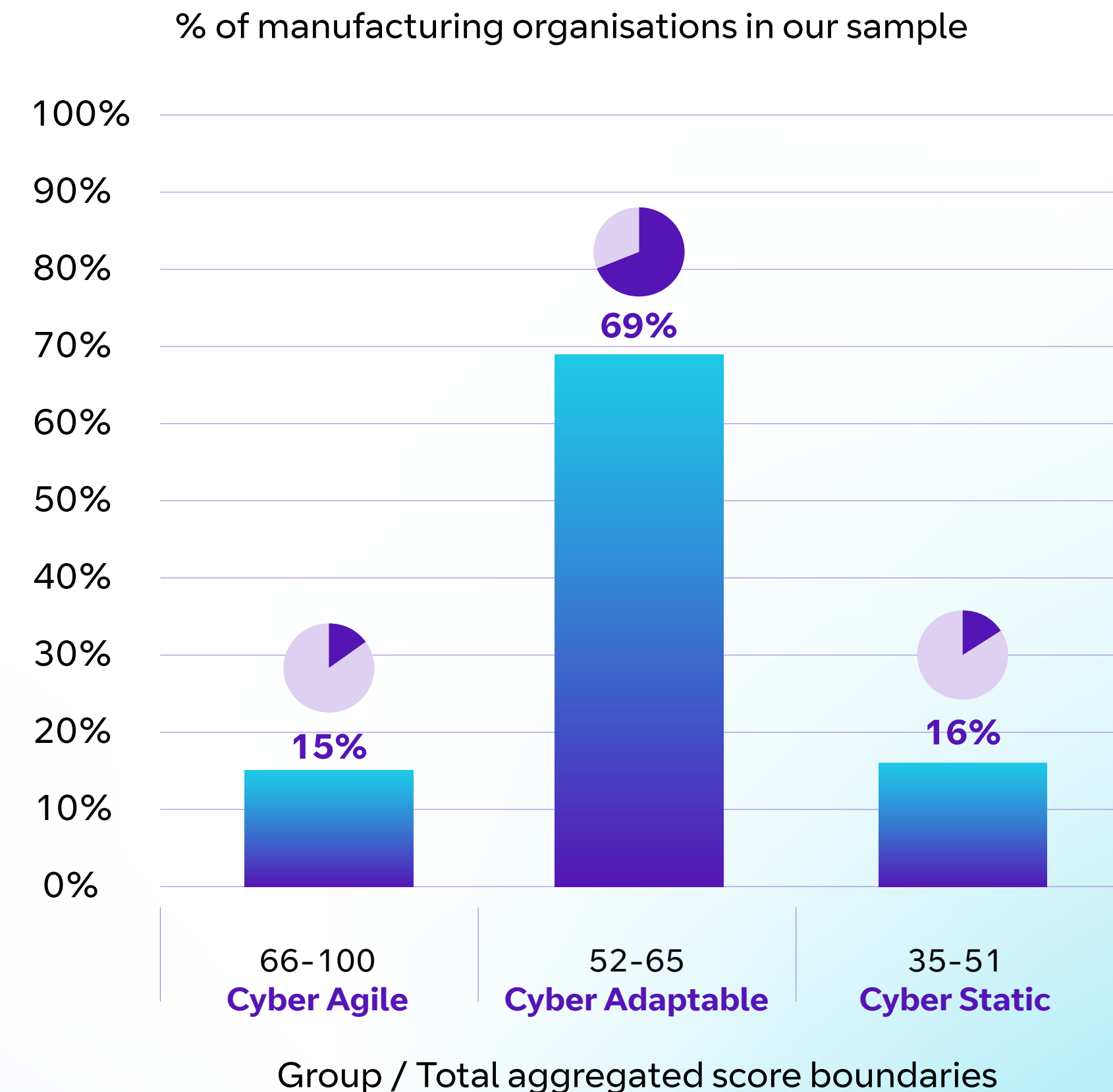
The cyber agility scoring system

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



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

Cyber attacks are on the up. In an increasingly online world, with almost all business activity taking place in the cloud, hackers are finding manufacturers to be lucrative targets for their attacks.

This risk is not solely limited to the digital realm, with the continuous introduction of new devices and the rise of the Internet of Things technology further adding complexity to the picture. Manufacturers must protect both the IT and OT sides of their estates, as well as employee devices connected to the corporate network.

Perhaps partly due to this bewildering backdrop, some **36%** of manufacturing leaders in our study say they are experiencing high or very high cyber attack severity. And there's no respite in the short-term future either: the figure rises to **43%** who anticipate high or very high severity in the next three years.

Regardless of the type of attack – from denial of service to IP theft and ransomware attacks – they all have the potential to completely halt factory operations, limit the sharing of data across the business, and give attackers access to customer and IP data. All of these will have serious ramifications on manufacturers, including lost revenue and missing customer deadlines from the costly unplanned downtime, as well as reputational damage and regulatory fines.



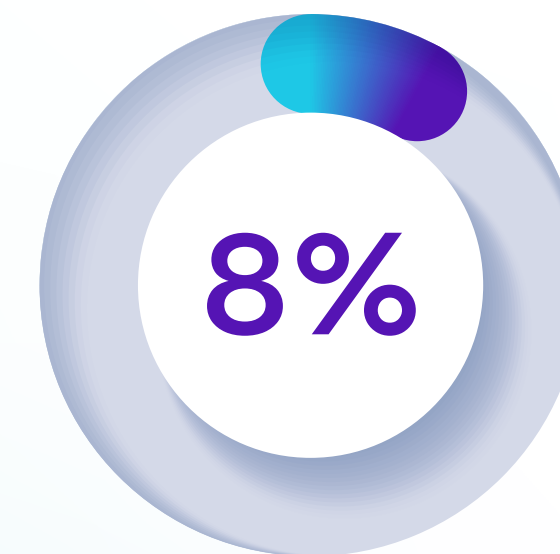
Nearly six in 10 see a cyber attack as their main existential threat.

The significant consequences of a potential attack are keeping manufacturing leaders awake at night, with nearly six in 10 (**57%**) believing that a major cyber attack is the main existential threat to their organisation. Building cyber resilience will give leaders the confidence that, in the event of an attack, they will be able to recover swiftly and maintain operational continuity.

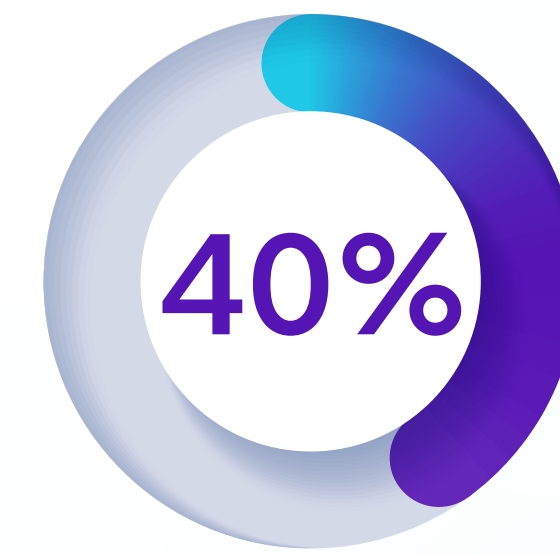
Prepared to defend

Many manufacturers are prepared for the struggle: on the flipside of the cyber security equation, half of the businesses in our study say they are currently 'very prepared' or 'extremely prepared' to deal with cyber attacks, and two-thirds (**66%**) believe they will be very or extremely prepared over the next three years.

That's the good news, but it leaves half of manufacturers falling short in their defence against attacks, and **34%** expecting to fail to reach optimum levels in the short-term future, potentially leaving them exposed for years to come.



Initial implementation



Enhanced strategy



Integrates and proactive

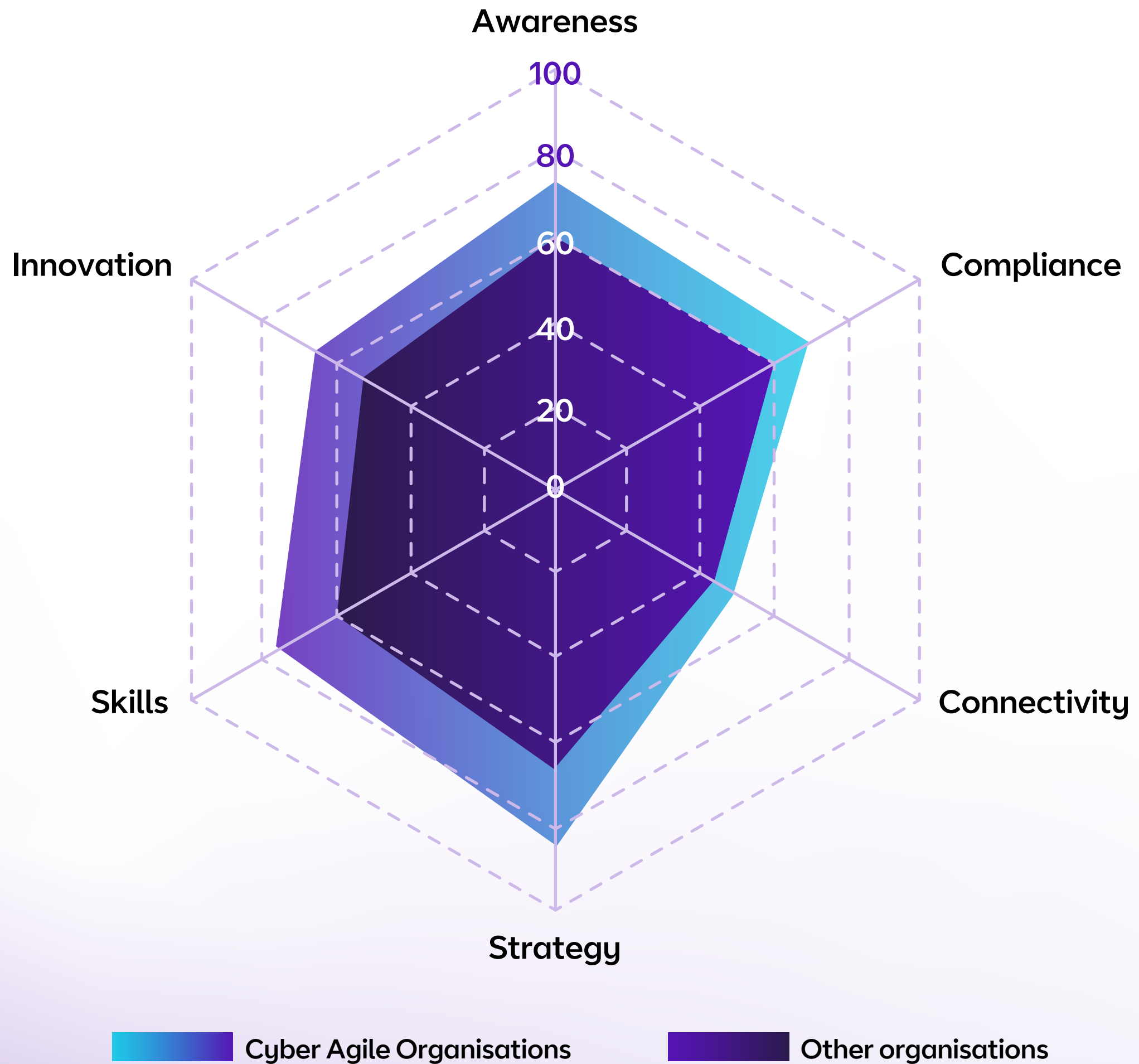


Strategic and agile

The importance of being agile



Average cyber agility scores for manufacturing organisations.



The manufacturing industry has work to do to optimise security and transform it into a strategic asset for business growth. Just 15% of manufacturers taking part in our study were found to be Cyber Agile Organisations, the second lowest figure of all industries in our study, with only Healthcare trailing behind. However, there is scope for other manufacturing organisations to join the cyber agile crowd, with the biggest gaps – and, therefore, the greatest opportunities for growth – seen across the Awareness, Strategy and Innovation dimensions.

The incentive to upgrade to cyber agility is clear: the study also found that Cyber Agile Organisations in manufacturing achieved **24% higher revenue growth rates** than other organisations in the sector. If all other manufacturing businesses across the eight markets covered in this study matched this growth rate by improving their cyber agility, this could unlock an additional **£47 billion in revenue** and **£17 billion in gross value added (GVA)**¹ for the sector and the wider economy².

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.

² Revenue and GVA figures derived from a bespoke economic model developed for The Cyber Agile Organisation research. For methodology see p42 of the main study.

[Read full report](#)

Equally clear are the areas of business that can get a boost from cyber agility. Manufacturing leaders recognise several significant benefits that improved cyber agility would bring to their organisations, the top five being:

- Increased customer trust
- Improved reputation
- Increased business efficiency
- Improved overall business agility
- Reduced management time

“Modern manufacturing is digitally interconnected from the back office to the factory floor. In this environment, recognising cyber security isn’t just about protection – it’s about unlocking value and driving superior business performance. Resilient operations are the foundation of innovation, efficiency, and competitive advantage in Industry 4.0.”

Anthony Harrison,
Director Manufacturing and Resources, BT

Part 2

Becoming cyber agile:
Key focus areas for
manufacturing businesses

Preparedness: Securing the network

An important component of improving cyber agility is allocating sufficient funding to the best software and tools that can protect your business. **By 2027, manufacturing organisations in our study expect their cyber security budgets to increase by an average of 12%.**

However, businesses need to ensure they're investing in the right places, and building a clear picture of your IT infrastructure and network is a good place to start. Six in 10 manufacturing Cyber Agile Organisations say their organisation has high visibility over this area of business – twice as many as other organisations in the study.

But, even with proper oversight and the budget to match, challenges remain. The top three connectivity cyber risk factors cited by respondents to our study all involved the proliferation and use of devices.

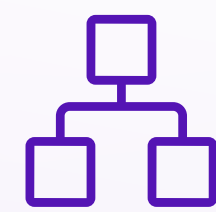
Top three connectivity cyber risk factors



Devices connecting to public or insecure wireless networks



Increasing number of devices



Internet of Things devices



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

Ensuring secure connections

Getting the supporting infrastructure right is fundamental to maintaining a productive manufacturing environment and reducing downtime. This includes updating legacy network infrastructure that often has vulnerabilities. However, networks can only be reliable and resilient if they are secure – and they can only be secure if you have full visibility of your network activity.



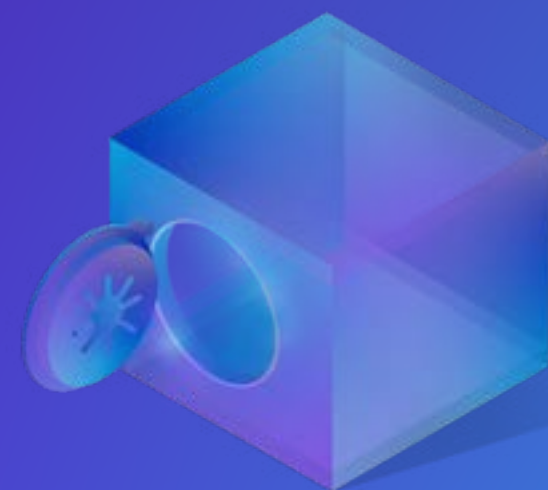
Protecting your operations

The integration of IT (Information Technology) and OT (Operational Technology) systems is enhancing workflows, reducing errors and cutting costs – helping manufacturing organisations to gain a competitive advantage. However, connecting OT up to the network exposes it to new threats and, on the flipside, it also creates new points of entry that can be exploited by cyber criminals.



Safeguarding your data

Leveraging advanced technologies and real-time data analytics depends on your ability to securely transfer data across factory floors, warehouses, back offices and hybrid workforces. Implementing Zero Trust principles will be important to ensure that every request is thoroughly verified, minimising the risk of unauthorised access and data breaches.



Keeping compliant

It is crucial to keep ahead of industry standards and ensure your operations are compliant. For example, the NIS2 Directive, which came into force in October 2024, aims to establish a common level of cyber security across critical sectors within the EU. Adhering to this legislation safeguards supply chains, critical infrastructure and valuable intellectual property.



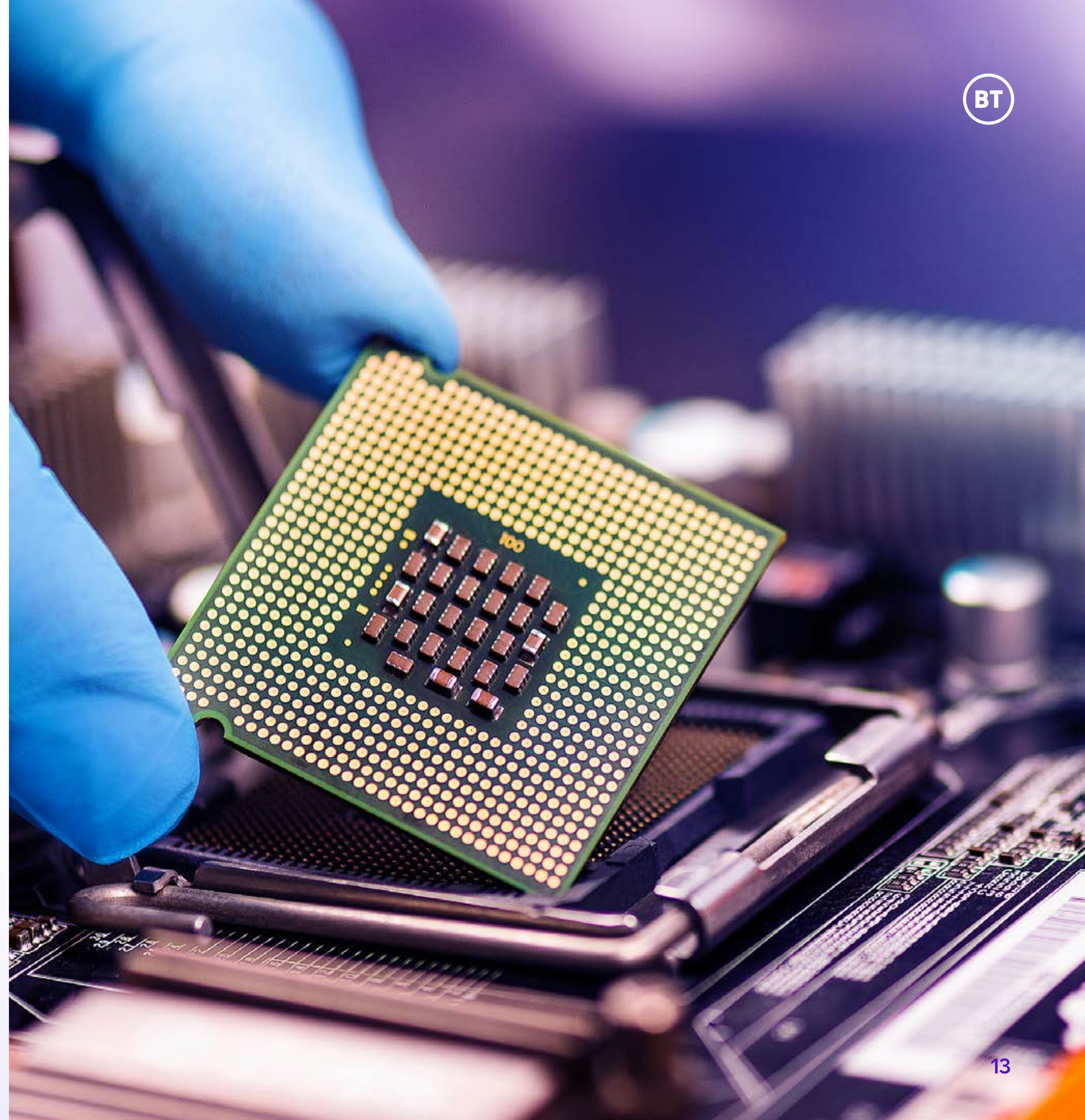
Performance:

Manufacturing innovation

Cyber Agile Organisations are more than just secure — they use security as a platform for innovation, giving employees the freedom to test new ideas and adopt cutting-edge technologies in a safe IT ecosystem. Security is also the keystone of a functional digital supply chain, allowing teams to acquire new products and services to optimise goods at the factory gate.

That's why **73%** of Cyber Agile Organisations in the manufacturing industry believe that an innovative approach to security helps them become more innovative overall. About the same number (**76%**) point to the explosion of productivity tools like generative AI and shadow AI in the workplace meaning cyber security is more important than ever. Of all the manufacturing organisations in the study, a similar proportion (**71%**) have turned this equation on its head by mobilising AI and machine learning for threat detection.

Incident resolution and recovery processes help keep the wheels of innovation turning, so it's fitting that a higher proportion of manufacturing Cyber Agile Organisations say their processes are extremely useful in mitigating the impact of cyber risk (**38%**) than other businesses (**23%**).



Steps to cyber agility in the strategy, skills and innovation dimensions

Complementary strategies

Aligning security strategies with broader business objectives will help to optimise people power, avoid wasted effort and ensure manufacturing processes are running at their most efficient. To achieve this, it will be important for cyber security to have a permanent seat at the boardroom table, ensuring that security considerations are embedded in all strategic decision-making.



Never stop training

Cyber threats are morphing and transforming constantly, so your people must stay informed of the latest developments in the security space. Any connected workers, including the front line, unable to recognise phishing attacks can be detrimental to the business. Invest in training to upskill everyone on the latest cyber attacks and how they can act as a human firewall.



Secure by design

As manufacturers adopt Industry 4.0 technologies like AI, AR/VR and cloud computing, security measures must evolve to address new threats. A secure-by-design approach mitigates downtime caused by cyber attacks and enables rapid scaling to meet market demand. Investing in innovative security solutions also unlocks new use cases and technological advantages. For example, secure mobile connectivity for frontline factory workers can enhance real-time data access and decision-making, boosting efficiency and responsiveness.



Utilise partners

Engaging a Managed Security Services Provider (MSSP) helps take the strain off your in-house team, allowing them to focus on maintaining operational productivity, while reducing your vendor and network complexities.



Conclusion



Essential

Now, more than ever before, cyber security is a business-wide issue and not something to be left to the IT team. A major breach could prove fatal to your business, so proper protections, training and protocols are a must.

Resilience

Manufacturing businesses face a unique set of challenges. From the proliferation of the Internet of Things expanding your attack surface to nation states looking to steal your IP: make no mistake, bad actors are targeting businesses like yours every day.

Cyber agile manufacturers understand this – and they're taking it a step further, mobilising cyber security, not just as a shield against the attentions of hackers and data breaches, but as a strategic asset and a launchpad to innovate and grow.

Advantage

As we have seen, customer trust, greater efficiency, improved reputation, and more opportunities for collaboration are the rewards for getting the cyber agility balance right. Not to mention the increasingly tough security standards set by companies for access to their supply chain; businesses that fail to meet these levels could miss out on lucrative contracts. Cyber Agile Organisations stand a better chance of excelling in these areas, while others must work harder just to achieve the same results.

BT's got your back



We're here around the clock

We've got 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. Our Cyber Security Operations Centres around the globe offer expertise to manage customers' security and ensure they are protected 24/7.

We can help bridge the IT/OT divide

We guide organisations to select the solutions that best match their security needs by combining head office and plant management insights. Our Operational Technology Threat Management and Managed Security services cover a range of security controls, with solutions selected from market-leading vendors. We can also provide integrated IT/OT Security Operations Centre services to give you a single pane of glass view over your entire estate.

We are constantly innovating

Our Cyber Assessment Lab delves into technology to uncover innovative new solutions. For example, we're investing in automation to enhance our managed services security responses. Our security research and innovation programme is focused on building a layered approach to future security to stay ahead of evolving cyber threats.





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.