BT Means Business

The Cyber Agile Organisation:

Retail

Transforming security into a platform for growth

business.bt.com

Contents

Foreword

Opportunities abound in the retail industry as the shift to online shopping is supercharged by advancements in AI, cloud services and data analytics. New technology greases the wheels of e-commerce from the warehouse to the customer's front door, helping companies optimise inventory management, recommend tailored products and personalise shopping interactions across a multitude of channels.

Chatbots and AI assistants are improving customer service and easing the burden on hard-pressed call centres. Powerful analytics tools are fuelling insights in market research, customer segmentation and real-time decision-making, enabling more targeted campaigns. Additionally, the Internet of Things (IoT), radio frequency identification (RFID) and blockchain are enabling real-time monitoring and traceability throughout the supply chain.

Simultaneously, sustainable sourcing platforms and carbon tracking tools are helping businesses become more efficient, aligning with environmental regulations and consumers' green expectations, which increasingly influence buying decisions.

In a sector ripe for advancement, pioneering companies are busy optimising processes to stay ahead of the competition. However, these advances come at a cost. More digital technology means more opportunities for cyber criminals; the attack surface is expanding, and businesses must remain vigilant to cyber risk.

By focusing on cyber security strategies, organisations can create a safer environment for innovation to flourish. This means bringing together the best people, tools, technologies and processes, as well as devising protocols that can mitigate the impact of a cyber attack, minimising damage and reducing the time needed to get back up and transacting.

Foreword

Cyber agility in retail

In this study, we aim to distil the key elements of what confers cyber agile status upon businesses. 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 customer trust, business growth 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 threat landscape. It's also your chance to elevate your business to the status of a Cyber Agile Organisation and enjoy all the incredible benefits that cyber agility brings.

Want to understand more about these advanced organisations and perhaps 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 from organisations across eight markets and eight industries (including the retail sector).

Respondents were split into two groups:

- **1,275 IT C-suite technology leaders**, (384 from the retail industry).
- **1,225 other C-suite leaders**, including Chief Executives, Chief Operating Officers and Chief Compliance Officers, (392 from the retail industry).

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

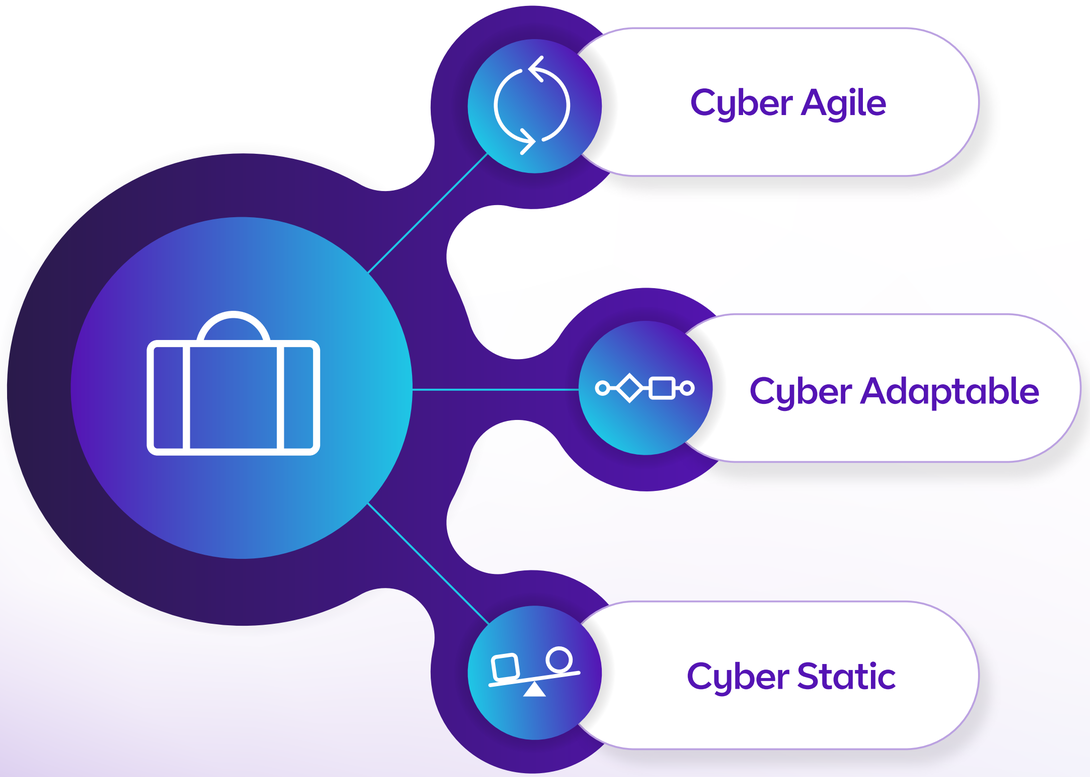
The extent to which cyber security is used as an enabler for innovation and broader organisational transformation.

The cyber agility scoring system

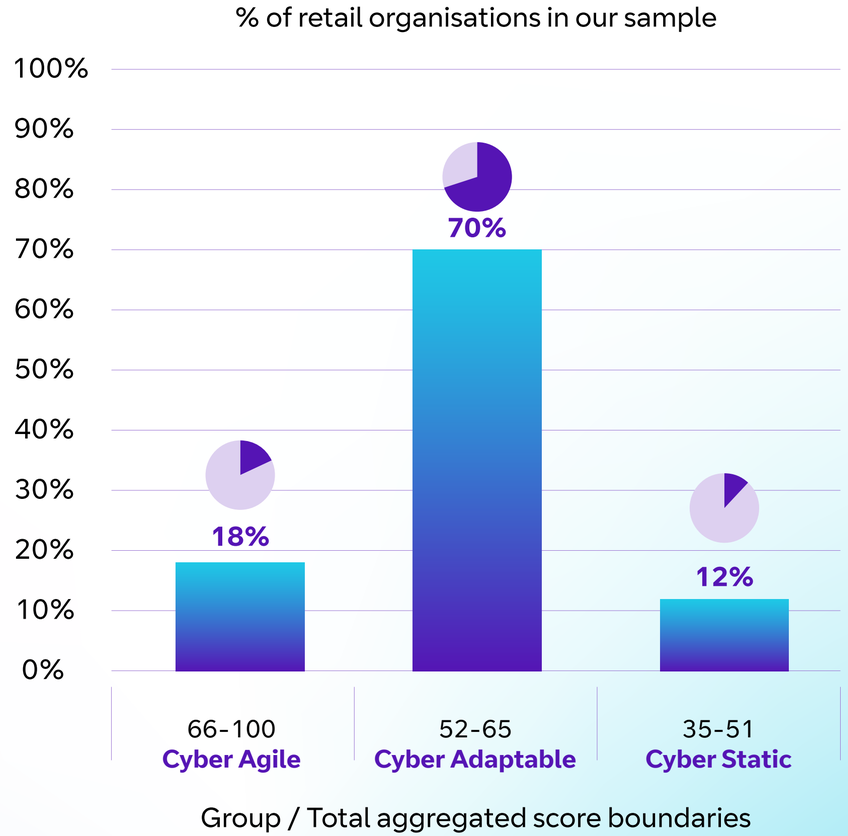
Cyber agility scores were based on performance in the six dimensions: Awareness, Compliance, Connectivity, Strategy, Skills and Innovation. Each dimension comprised a set number of questions from the opinion research which were attributed different weightings. In total, each dimension was valued at 30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



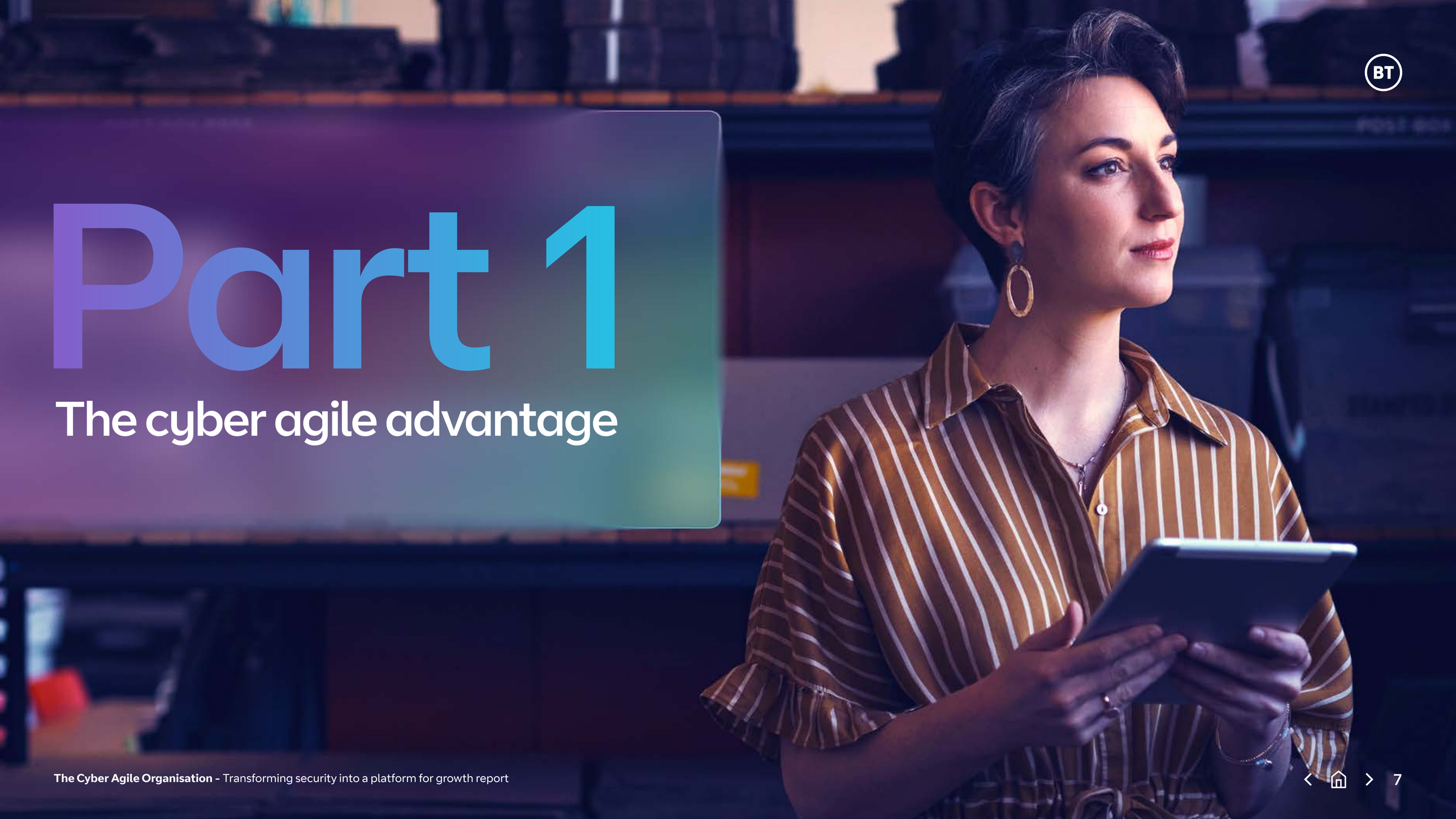
To qualify as a Cyber Agile Organisation, businesses and public sector bodies had to rank in the top-performing segment for aggregated scores across the six dimensions.



Graph: The cyber agility scoring system

Part 1

The cyber agile advantage



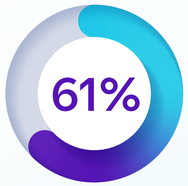
The cyber agile advantage

With large volumes of customer data, complex IT ecosystems and multiple transactions taking place every second, retail companies are at the sharp end of cyber threats.

According to our study, three in 10 organisations in this sector are currently experiencing either ‘high’ or ‘very high’ cyber attack severity. And the problem could get worse before it gets better, with nearly half **(47%)** expecting the severity they face to reach these levels within the next three years.

This rising threat is causing sleepless nights for retail leaders, with **61%** of them believing that a major cyber attack is the main existential threat to their organisation.

One in five retail business taking part in our study qualifies as a Cyber Agile Organisation.



61% say a major cyber attack is the main existential threat to their organisation.

Prepared to protect

With cyber threats increasing, many retail businesses have responded by building defences and establishing mature strategies to reduce risk. As a result, more than half (**53%**) of those responding to our study believe they are either ‘very’ or ‘extremely’ prepared to deal with cyber threats. This figure rises to **68%** for companies expecting to reach this position in the next three years.

And it seems retailers are putting budgets in place to back up their plans, with the majority expecting cyber security spending to increase in the short term – by an average of **13%** over the next three years.

Two-thirds of retail leaders see a secure network as a prerequisite for doing business, reflecting the importance of cyber security as a benchmark of a company’s overall trustworthiness.

Cyber security self-assessment

Cyber security maturity self-assessment for retail organisations

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

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

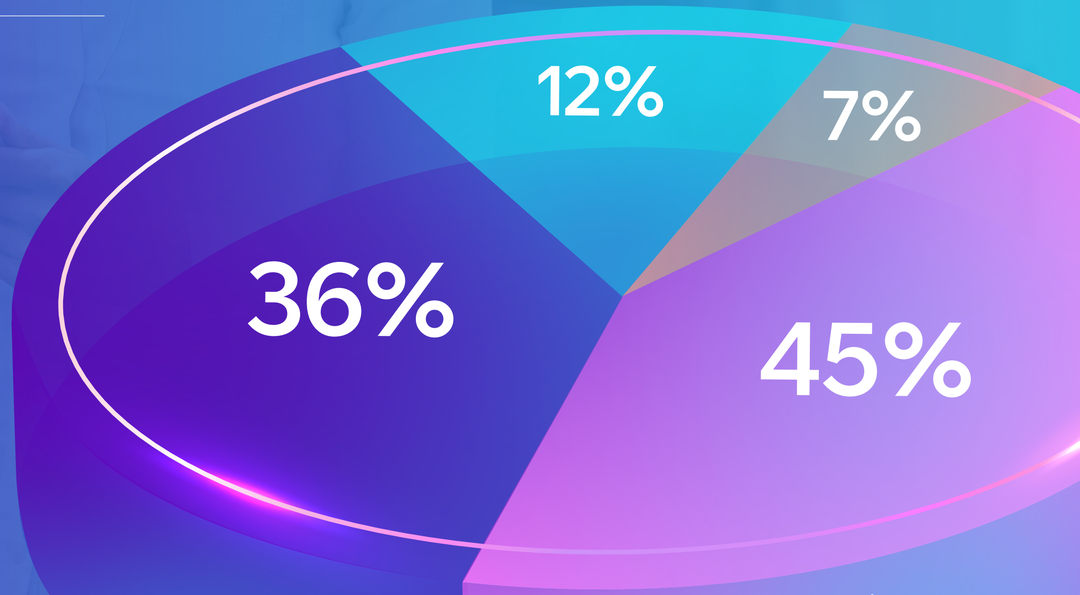
36%

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

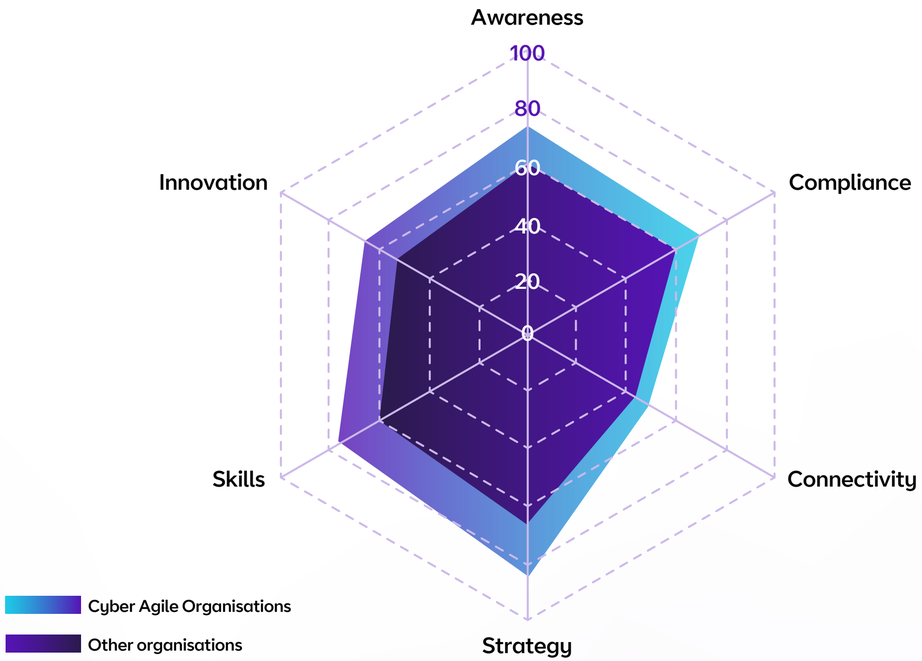
12%

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 retail organisations.



Dimension	Cyber Agile Organisations	Other organisations
Awareness	72	58
Compliance	69	61
Connectivity	49	43
Strategy	84	67
Skills	75	58
Innovation	65	54

Connectivity is a critical area of focus

Of the retail businesses taking part in our study, just under one in five **(18%)** qualify as Cyber Agile Organisations. Over the last three years, these top performers achieved 18% higher growth rates than other businesses from the same industry. On average, they also outperform other organisations significantly in the Awareness, Strategy and Skills dimensions, with the biggest gap appearing within Strategy and Skills.

> "Enhanced cyber security is a key driver of value in the retail industry. It not only safeguards innovation but also ensures a resilient, customer-centric future. By fortifying their digital defences, companies can confidently embrace new technologies, optimise operations and build trust with consumers, driving sustainable success in a competitive market."
>
> **Simone Chetcuti,**
> Director of Retail, Personal Consumer and Charity, BT

The majority **(83%)** of Cyber Agile Organisations in the retail industry believe that by innovating their approach to cyber security, they become more innovative overall. More broadly, leaders across all retail organisations recognise a range of significant benefits that improved cyber agility could bring, with the top five being:

- Increased customer trust
- Increased business efficiency
- Improved overall business agility
- Improved reputation
- Improved collaboration

UK market spotlight

Our research shows that, across all industries, UK-based organisations are strongest in the Strategy, Skills and Compliance dimensions, with Connectivity being a key area of focus.

The UK is a hotbed of activity in the retail sector, home to many of the world's biggest and most advanced organisations in the space. Strengthening cyber security is clearly important to UK retail businesses, with **78%** of leaders reporting that cyber security is the foundation of their IT system, and **64%** claiming that every employee in their organisation knows they are responsible for IT security.

Yet less than a third **(32%)** of UK retail leaders say their cyber security strategy is completely aligned to their overall organisational strategy: a key component of what constitutes a Cyber Agile Organisation. Conversely, **77%** say they won't work with suppliers who lack adequate security credentials.

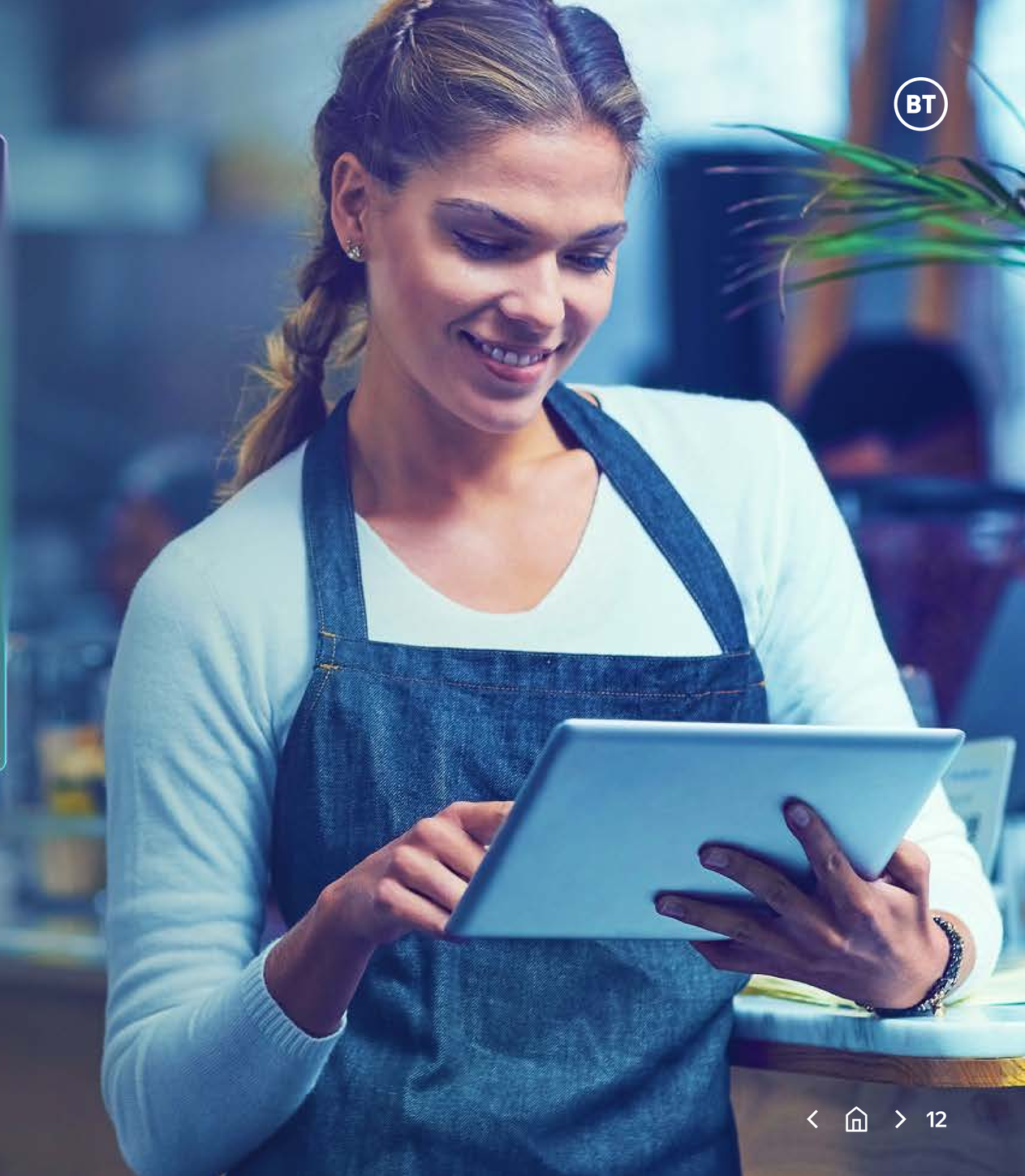
Eight in 10 UK retail organisations say that IT transformation projects have increased their organisation's cyber security vulnerabilities. And 68% believe the explosion of generative AI and shadow AI in the workplace has made cyber security more important than ever.

However, UK-based organisations are taking steps to defend against the problem, with **40%** actively recruiting an AI and machine learning security specialist and **22%** planning to fill this role in the future.

Part 2

Achieving cyber agility: How retailers can strengthen cyber defences

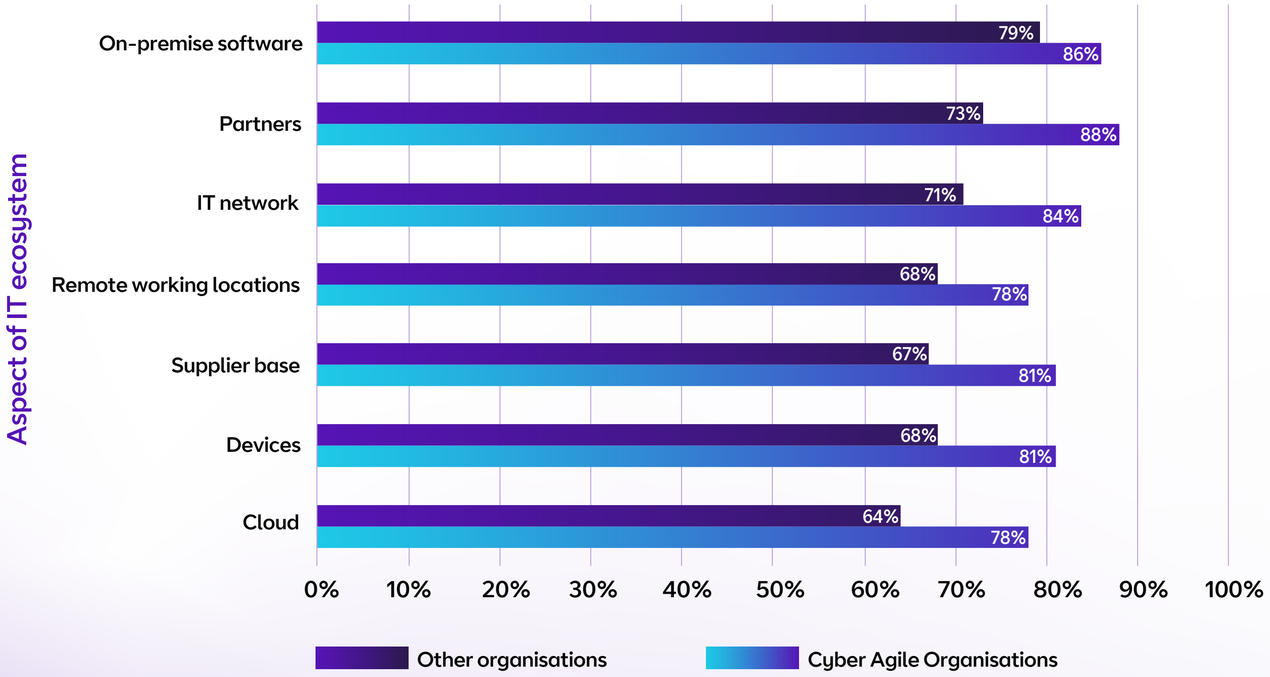
Developing awareness of potential cyber security vulnerabilities and having the skills to address them are two key components of cyber agility. So, how do retail businesses fare in these areas of best practice?



Preparedness: Building awareness

You can't secure what you can't see. This principle applies not only to internal operations but across the entire supply chain, where a single vulnerability could lead to significant disruptions. So, it's no surprise that 81% of Cyber Agile Organisations in the retail industry say they have 'complete' or 'high' visibility over their supplier base, compared to only 67% of other organisations.

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



Cyber Agile Organisations in the retail industry also fare better when it comes to the resiliency of their IT ecosystems. More than eight in 10 **(82%)** believe their cloud ecosystem is either 'extremely' or 'very' resilient, compared to **63%** of others, while their supplier base is also more likely to be resilient (76% versus 60%).

The cyber threat landscape evolves rapidly, with a year often feeling like an eternity in cyber security. On average, organisations in the retail industry review and update their cyber security policies every six months. When conducting these reviews, it is important for businesses to use a range of reliable information sources to accurately assess risk.

Top information sources Cyber Agile Organisations use to assess risk from cyber threat:

- Cyber security frameworks and standards
- National Cyber Security Centre (NCSC)
- Online cyber security publications and blogs
- Cyber security conferences and events
- Government and international agencies

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

1

Assess your cyber security risks and controls

Ensure network security involves a comprehensive understanding of your existing cyber security posture. This means evaluating existing security controls across people, processes and technology, pin-pointing any gaps in your defences, then prioritising areas for improvement. Regularly assess cyber security risks and implement robust safeguards to keep your network secure, now and in the future.

2

A different view of how your business connects

It is important to develop robust protocols to safeguard all forms of data, particularly when your employees are working remotely or introducing personal devices to the IT network. With distributed services and third-party access to information the norm, implementing Zero Trust principles and de-perimeterisation will ensure that every request is thoroughly verified, minimising the risk of unauthorised access and data breaches.

3

Know your industry regulations

Stay aligned with security frameworks and industry-specific regulations critical to your organisation. The retail industry must comply with various cyber security frameworks, such as the General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS). They should also review their security posture against security frameworks such as CIS (Centre for Internet Security). 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, put in place best practices and protect against potential breaches.

Performance:
Sharpening security skills

The rapid pace of technological change brings major opportunities for businesses, but it also comes with risk. More than half **(54%)** of retail leaders in our study say their team struggles to stay one step ahead of the cyber threats they face. Given the increasingly sophisticated nature of attacks, it makes sense that **63%** believe human error is the biggest danger to their organisation's cyber security.

Cyber Agile Organisations in the retail industry are seeking to patch this problem: **88%** say they are actively building a cyber security culture among their people, compared to only 68% of other organisations in the industry.

In total, retail businesses invested an average of $3.1 million in cyber security training for employees over the last 12 months.

Piecing apart this data:

- **37% of Cyber Agile Organisations support employees in obtaining advanced cyber security training and industry-recognised certifications, compared to 24% of other organisations. 53% of Cyber Agile Organisations provide role-specific cyber security training for key departments, such as IT and finance, compared to 41% of other organisations.**

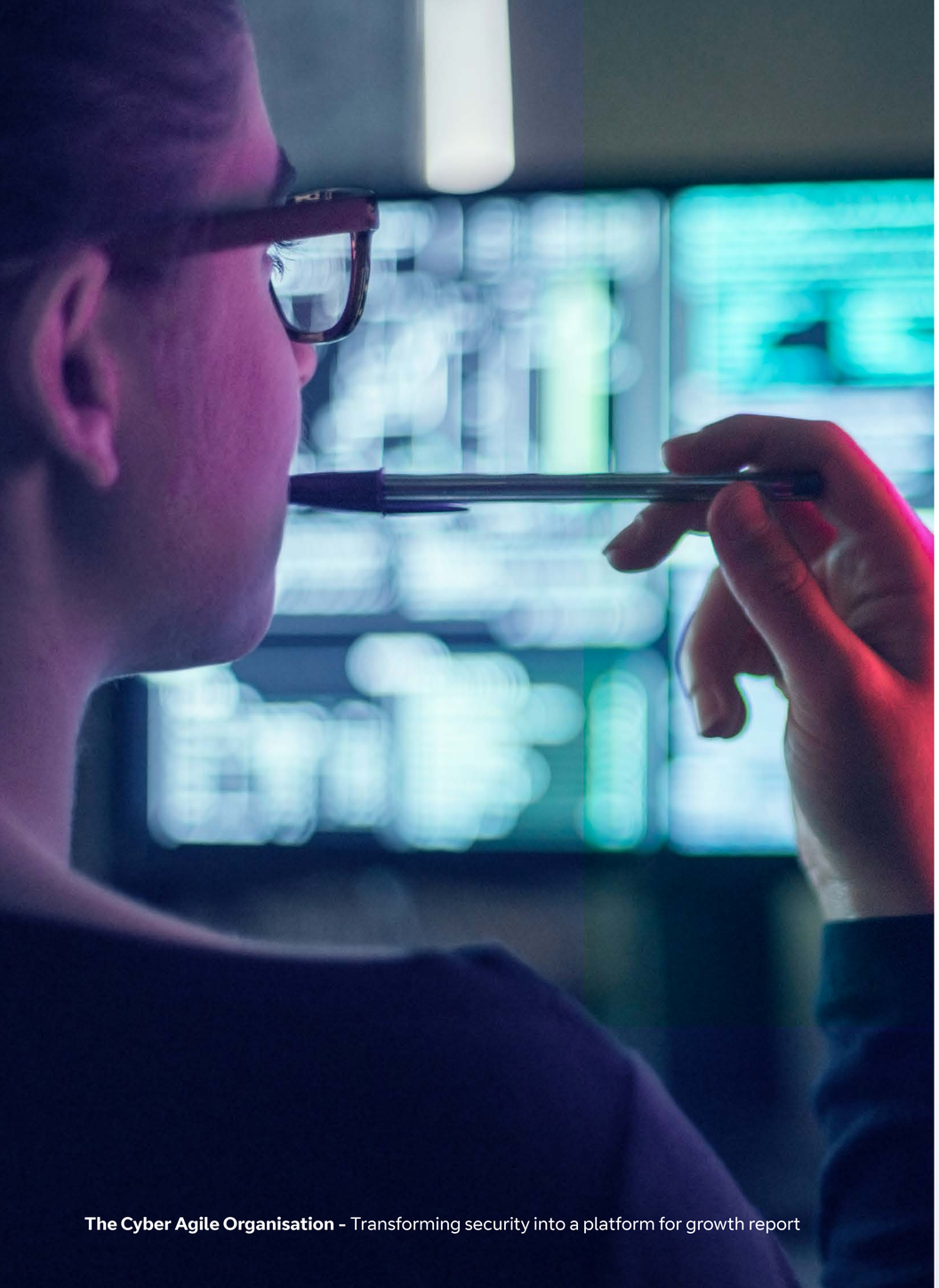
- **47% encourage security teams to acquire professional qualifications and participate in industry events, compared to just 19% of other organisations.**

43% of retail organisations are actively recruiting for AI and Machine Learning Security Specialists

Cyber Agile Organisations in the retail industry are also far more likely to have specialist cyber security professionals in place, with **64%** already employing a Chief Information Security Officer compared to **51%** of other organisations. In addition, six in 10 (**61%**) have a Security Operations Centre Analyst (compared to **38%** of other organisations), and **53%** have a Cyber Security Architect in post (compared to **35%** of other organisations).

Currently, **43%** of retail organisations are actively recruiting for AI & Machine Learning Security Specialists, and **38%** are recruiting for Threat Intelligence Analysts. All of which show that the retail sector is aware of the cyber risks it faces and is taking steps to reduce them.

> "It's essential to extend cyber security learnings and protocols beyond the IT department. Organisations that build company-wide awareness about the importance of cyber security stand a better chance of fending off attacks. Empower your people to speak up and report security issues to protect your business."
>
> **Lee Stephens**, Director of Security Advisory Services, BT



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

1

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 means 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.

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 and management that can be flexed to meet changing business needs.

3

Collaborate for continual improvement

Security doesn't stand still, but collaboration can help you keep up. Joining industry communities and events – such as Cyber UK – and forming internal partnerships between different departments will help to build knowledge and spark innovation. A strategy of continuous loop improvement increases your chances of staying ahead.

Conclusion

Retail businesses have a golden opportunity to make their operations leaner, faster and stronger with technology. From warehouse processes to back-office routines, tools are at their disposal to transform business, improving customer experiences to surprise and delight.

To take advantage, these businesses should learn from Cyber Agile Organisations, who acquire the best defences, appoint experts and develop their culture to support robust cyber security strategies. This creates a solid platform from which to innovate, experiment and grow, backed by an increased confidence in security risk mitigation and management strategies.

BT’s got your back

BT is transforming retail from the inside-out with secure, scalable and solid solutions for the future of business.

We live and breathe retail

BT works with many of the biggest retail brands. Partnering with us means benefitting from the insights we’ve gained through every success and challenge we’ve helped industry leaders navigate. Don’t forget, we’re a retailer ourselves, and our EE consumer brand blazes a trail when it comes to customer experience.

We make solid foundations secure and scalable

With over 70 years of experience protecting critical national infrastructure, our security credentials are unparalleled. We are consistently voted as a ‘Leader’ in network and security managed services by Gartner and IDC. Our Cyber Security Operations Centres offer expertise to manage customers’ security and ensure they are protected 24/7.

We’re vendor-agnostic

Our longstanding partnerships with leading suppliers put us in a unique position to advise on the right partners for your journey. Our Cyber Assessment Lab cuts through vendor noise to identify the right technologies for you. And we have the capabilities to secure your cloud regardless of the vendor you choose.

We have a renowned network

We’re a reliable partner with the research and development capabilities to turn the latest innovations into resilient and trusted services at scale. Our approach means that multiple technologies and legacy systems can be easily managed to create a single, secure network for your business.

We simplify complexity

Integrating emerging technology requires complex systems and processes which can feel overwhelming to any retailer. We seek to remove this complexity: few technology companies can respond like BT, especially when bespoke solutions are required. We serve 98% of FTSE 100 companies, so we’re well-placed to prepare your technology stack for the future.

BT Means Business

Get the conversation started

Talk to us

JN: 1634561879