BT Means Business

The Cyber Agile Organisation:

Healthcare

Transforming security into a platform for better care

business.bt.com

Contents

Foreword 3

About the study 4-5

Part 1: The cyber agile advantage 7

Digital disconnect? 8

Part 2: Becoming cyber agile 9

Preparedness: Keep it visible 10

Performance: Innovation platform 11

Steps to cyber agility 12

UK market spotlight 13

Conclusion 14

Foreword

The healthcare sector depends on cyber security like no other. Recent high-profile attacks on healthcare systems globally have highlighted the devastating consequences of compromised patient data, privacy breaches, and disruptions to essential services. Unlike in most industries, having the right tools, people and plans in place to identify, repel and recover from a cyber attack could equate to saving lives.

Sadly, the fact that healthcare professionals are responsible for our physical and mental wellbeing doesn't dissuade criminals from subjecting their employers to sustained cyber attacks. The threat to the healthcare sector is real and attacks are common, so watertight security is a must.

But along with shoring up sensitive data and defending potentially vulnerable systems, healthcare organisations have the chance to structure their operations in such a way that encourages collaboration, innovation and positive outcomes for patients.

By getting security right, these organisation can establish a foundation for seizing opportunities, meeting targets, and achieving ambitions.

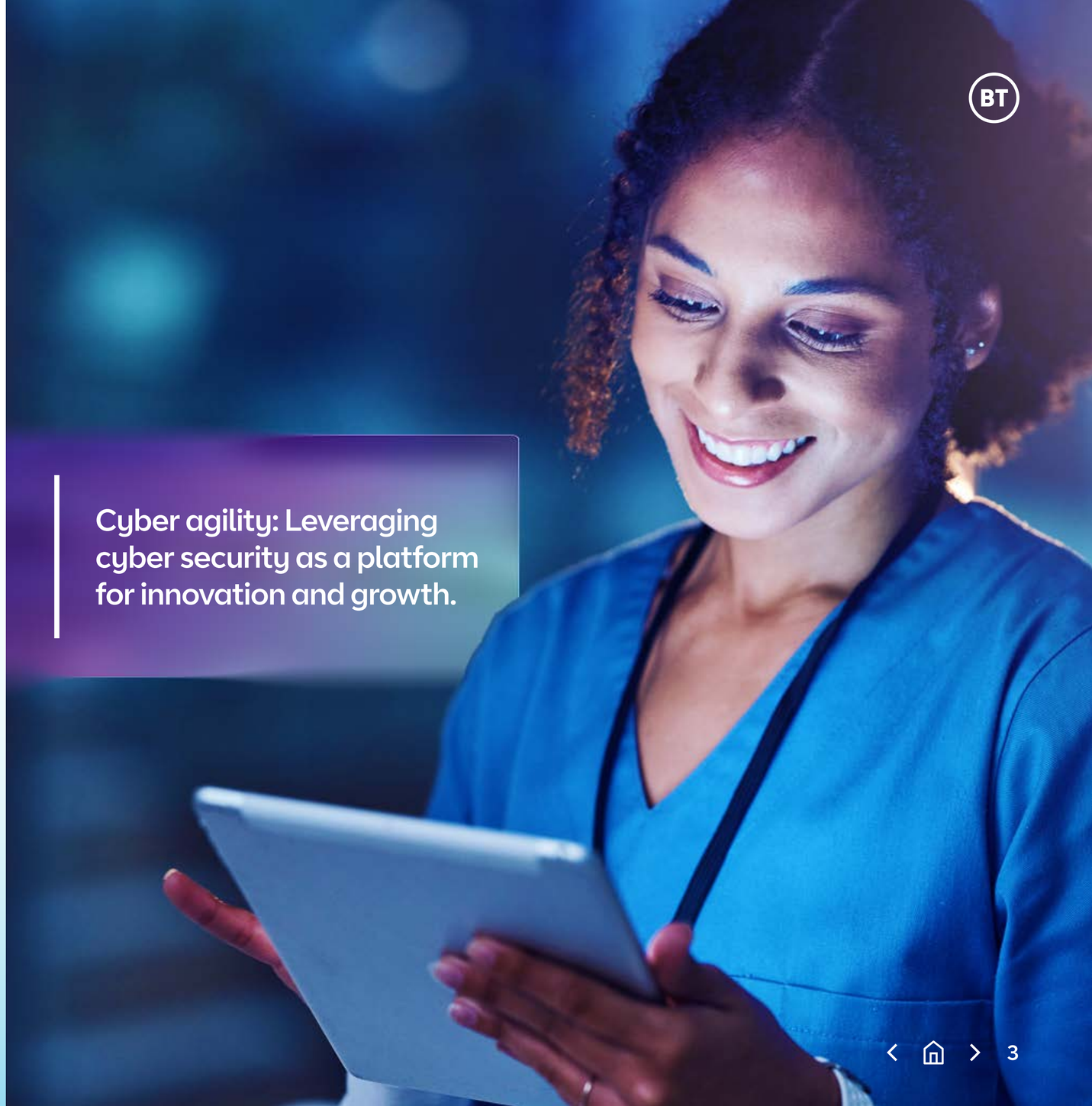
Cyber agility in healthcare

At BT, we wanted to investigate the essential attributes of organisations that excel in this area and help others become more cyber resilient. By distilling these ingredients into a profile of cyber security we uncovered a new concept, which we call 'cyber agility'.

Cyber Agile Organisations are able to deliver better outcomes for patients and staff, equipped with the best tech tools and strategies not just to shield themselves from danger but also to improve standards of care across the board, while staying on the right side of all regulations and setting the standard for service provision.

Throughout this study, we shine a light on what 'brilliant' looks like in the healthcare sector, highlighting the criteria for becoming a Cyber Agile Organisation and some best practice guidance on how to get there, so that organisations can emulate the success of providers who are getting it right.

Tristan Morgan
Managing Director,
Security, BT

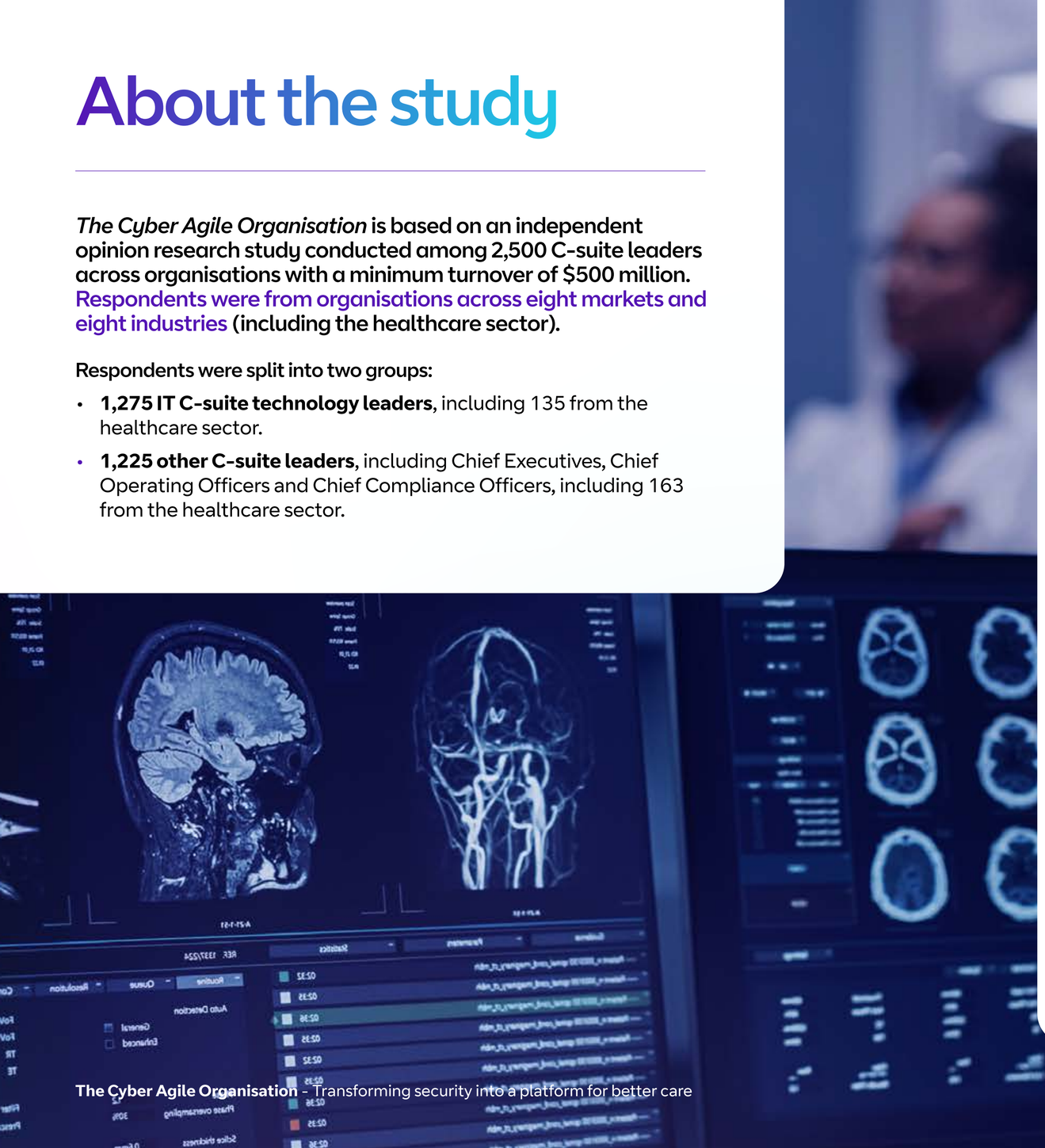


About the study

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 healthcare sector).

Respondents were split into two groups:

- **1,275 IT C-suite technology leaders**, including 135 from the healthcare sector.
- **1,225 other C-suite leaders**, including Chief Executives, Chief Operating Officers and Chief Compliance Officers, including 163 from the healthcare 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.

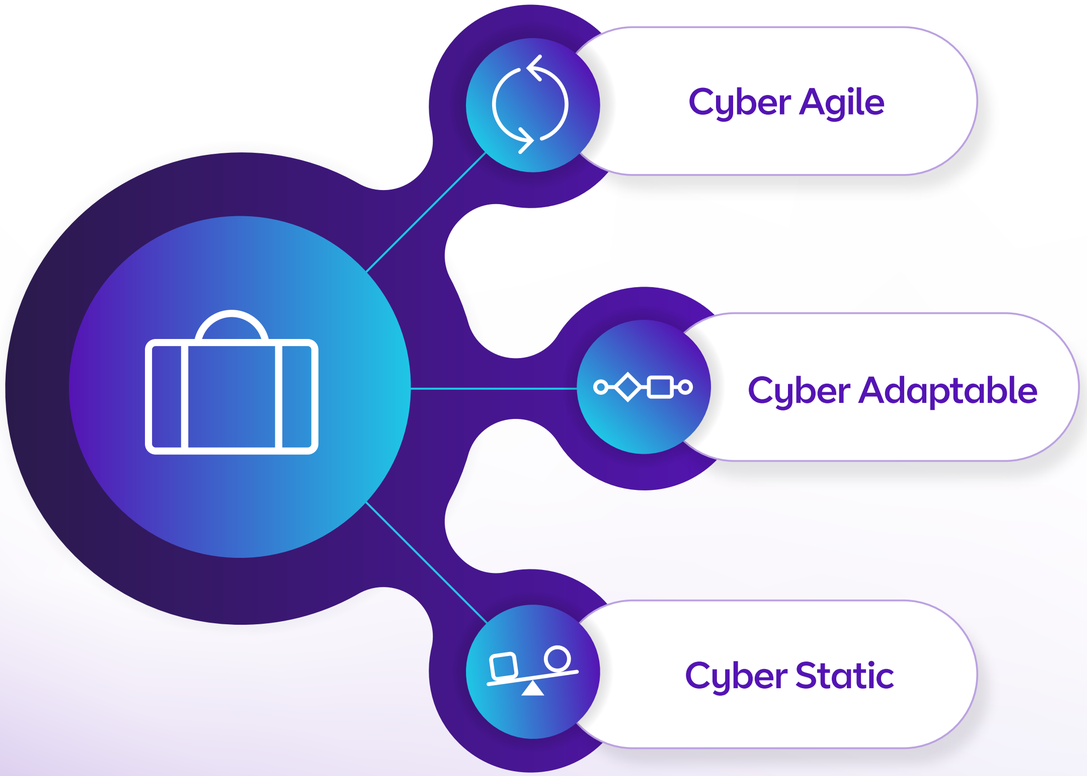
Innovation

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

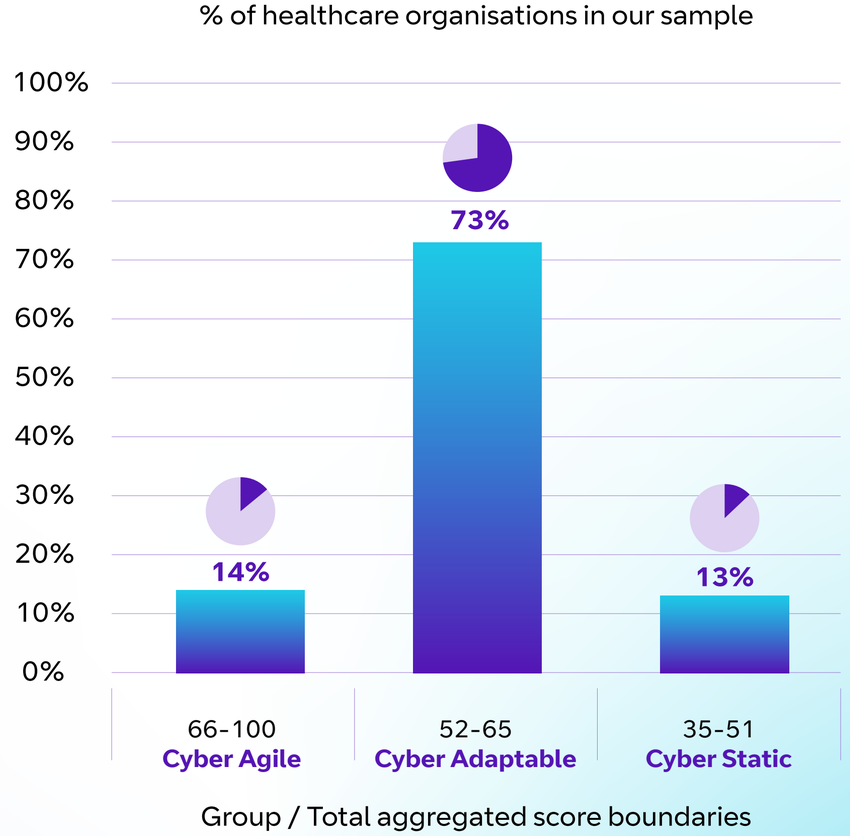
The cyber agility scoring system

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:



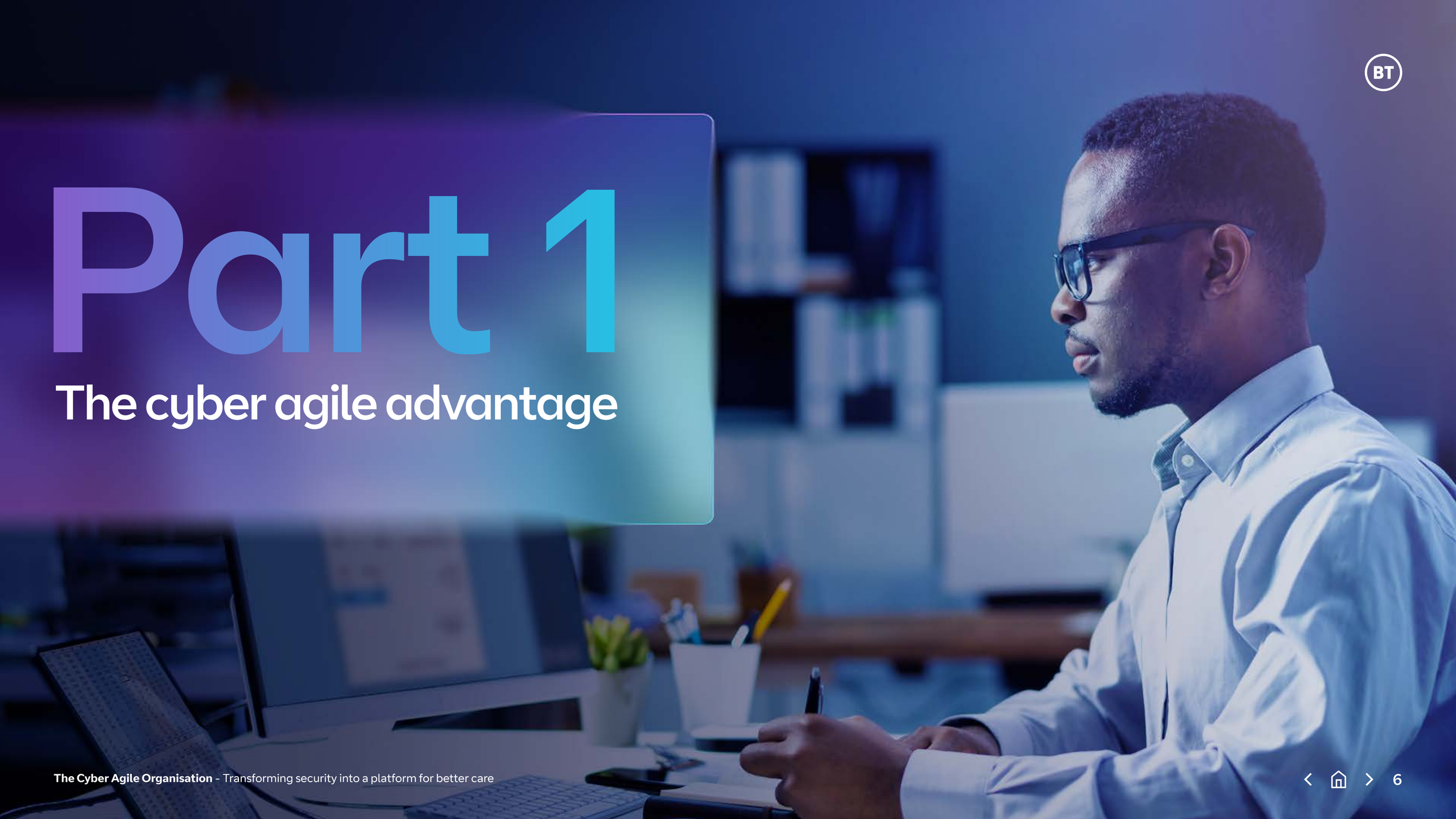
To qualify as a Cyber Agile Organisation, businesses and public sector bodies had to rank in the top-performing segment for aggregated scores across the six dimensions.



Graph: The cyber agility scoring system

Part 1

The cyber agile advantage



The cyber agile advantage

Cyber threats are escalating across all sectors and regions, but the healthcare industry is particularly vulnerable. The rising volume, sophistication and severity of cyber incidents have the potential to impact patients, staff and the healthcare system generally. From doctors locked out of medical records to missed diagnoses, risks associated with inadequate security protocols are many and varied.

And, as healthcare organisations adopt more digital technologies like electronic health records (EHRs) and IoT medical devices, the number of entry points for attackers increases. Each connected device becomes a potential target for attackers. It is perhaps no surprise, then, that 39% of healthcare leaders taking part in our study say they are currently experiencing 'high' or 'very high' cyber attack severity. And the future seems to offer little respite: nearly half (48%) anticipate high or very high severity over the next three years.

With the cyber security forecast worsening and cyber criminals circling, many healthcare leaders fear the worst if a breach is successful. Just over half (51%) fear that a major cyber attack is the main existential threat to their organisation.

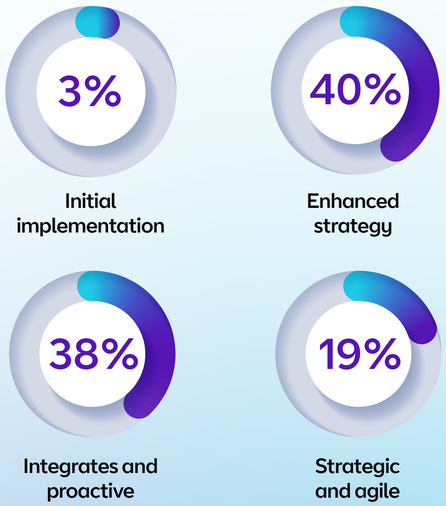
Defining cyber agility

For the healthcare industry, preparedness is key, not only for data safety, but patient safety too. So it's good to know that 57% of healthcare leaders say that, currently, they are either 'very prepared' or 'extremely prepared' to deal with cyber attacks.

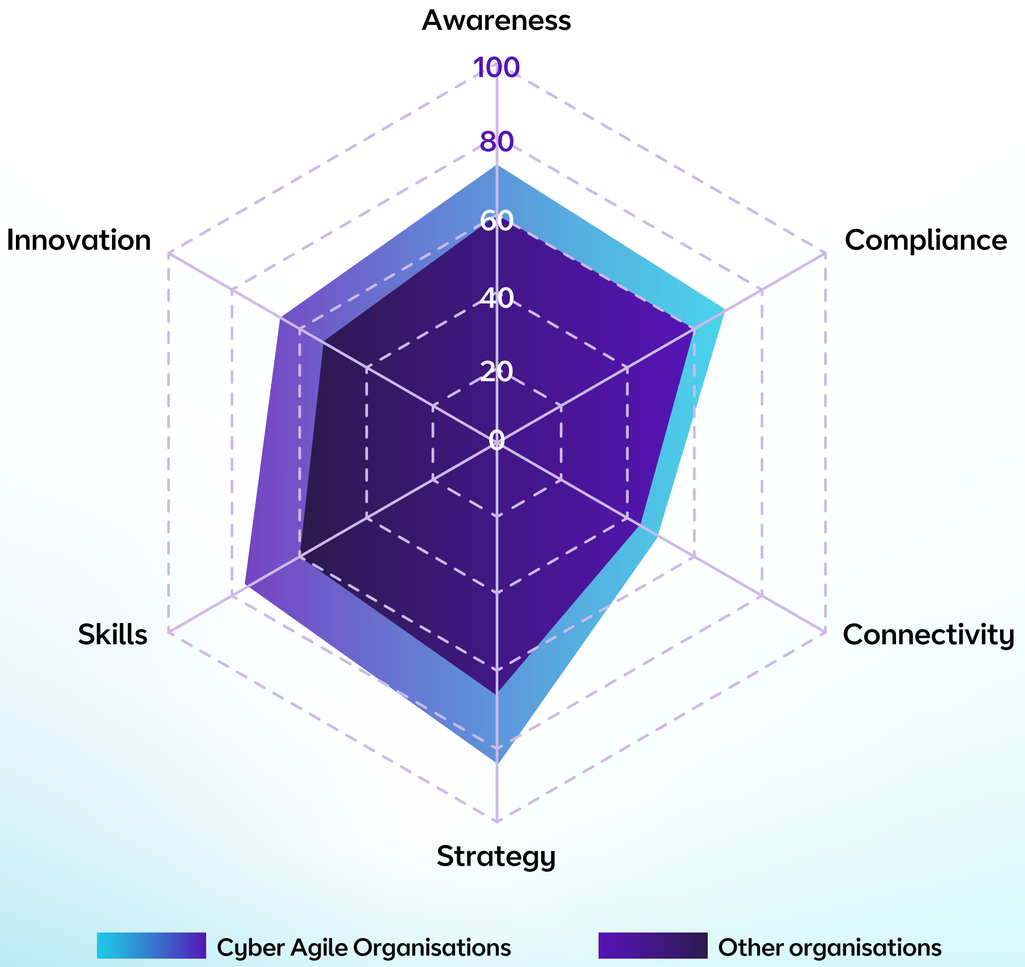
Thankfully, the level of preparation is expected to increase, with more than two-thirds (68%) of respondents anticipating being at least 'very prepared' within the next three years.

Cyber security maturity level

% of organisations



The importance of being agile



Digital disconnect?

14%

In a particularly notable finding from our study, there seems a disconnect between healthcare leaders' evaluation of their organisations' cyber maturity and the reality on the ground. The sector ranked top for the number of leaders who believe their cyber security maturity is strategic and agile, but it ranked bottom for the number of Cyber Agile Organisations **(14%)** compared to all other industries.

This could be down to a misalignment between what it means to be strategic and agile, and how security protections, systems and protocols manifest across all parts of different organisations.

81%

The gap between Cyber Agile Organisations and other organisations in the healthcare sector is widest across the Awareness, Strategy, Skills and Innovation dimensions – with the greatest divergence seen for Skills and Innovation. Low scores across the board for connectivity could be a key area of focus for the future.

Yet leaders still see plenty of major benefits in cyber agility. Respondents to our study ranked increased customer trust first, with **81%** identifying a causal link between cyber agility and customer confidence.

79%

Next came 'increased business efficiency' with **79%** saying the same, and improved reputation (77%) was a close third.

At a foundational level, seven in 10 healthcare organisations in our study see secure IT systems as nothing less than a prerequisite for doing business – a statistic that draws into sharp focus the need for cyber agility in building sustainable organisations of any kind.

> "It's clear that by prioritising robust cyber security measures and having an holistic approach to security, patient trust can be maintained, and healthcare services remain reliable and resilient."
>
> **Professor Sultan Mahmud,**
> BT Director of Healthcare

Growth

Part 2

Becoming cyber agile

Key focus areas for healthcare organisations

By 2027, healthcare organisations in our study expect their cyber security budgets to rise by an average of 12%. That's a healthy increase, but as with any IT investment, leaders must ensure they're channelling money to the right places.

Preparedness: Keep it visible

For around two-thirds of Cyber Agile Organisations (66%) in the healthcare industry, this job is being taken care of. They claim their organisation has a high level of visibility across its IT infrastructure and network, and strong safeguards to keep it secure, compared to only 34% of other organisations in the industry.

This is key given the main connectivity risk factors cited by respondents involving the proliferation of devices, increased deployment of artificial intelligence and sanctioned use of personal devices, which came higher than 'unsanctioned' use of devices, implying that while organisations are good at controlling device use, the sheer number of them is hard to manage.

Increasing number of devices

Increased use of AI

Sanctioned use of personal devices

Steps to cyber agility in the awareness, compliance and connectivity dimensions

Build transparency

Ensure comprehensive visibility and monitoring of your entire IT infrastructure, including operational technology and unmanaged devices. It is important to keep a 'live' threat analysis, tracking key areas of risk and highlighting emerging vulnerabilities.

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.

Meet regulatory standards

Keep up to date on the cyber security regulations and frameworks relevant to your organisation. You might have the opportunity to give feedback on proposed regulations, so give your views and be a part of the process.

Performance

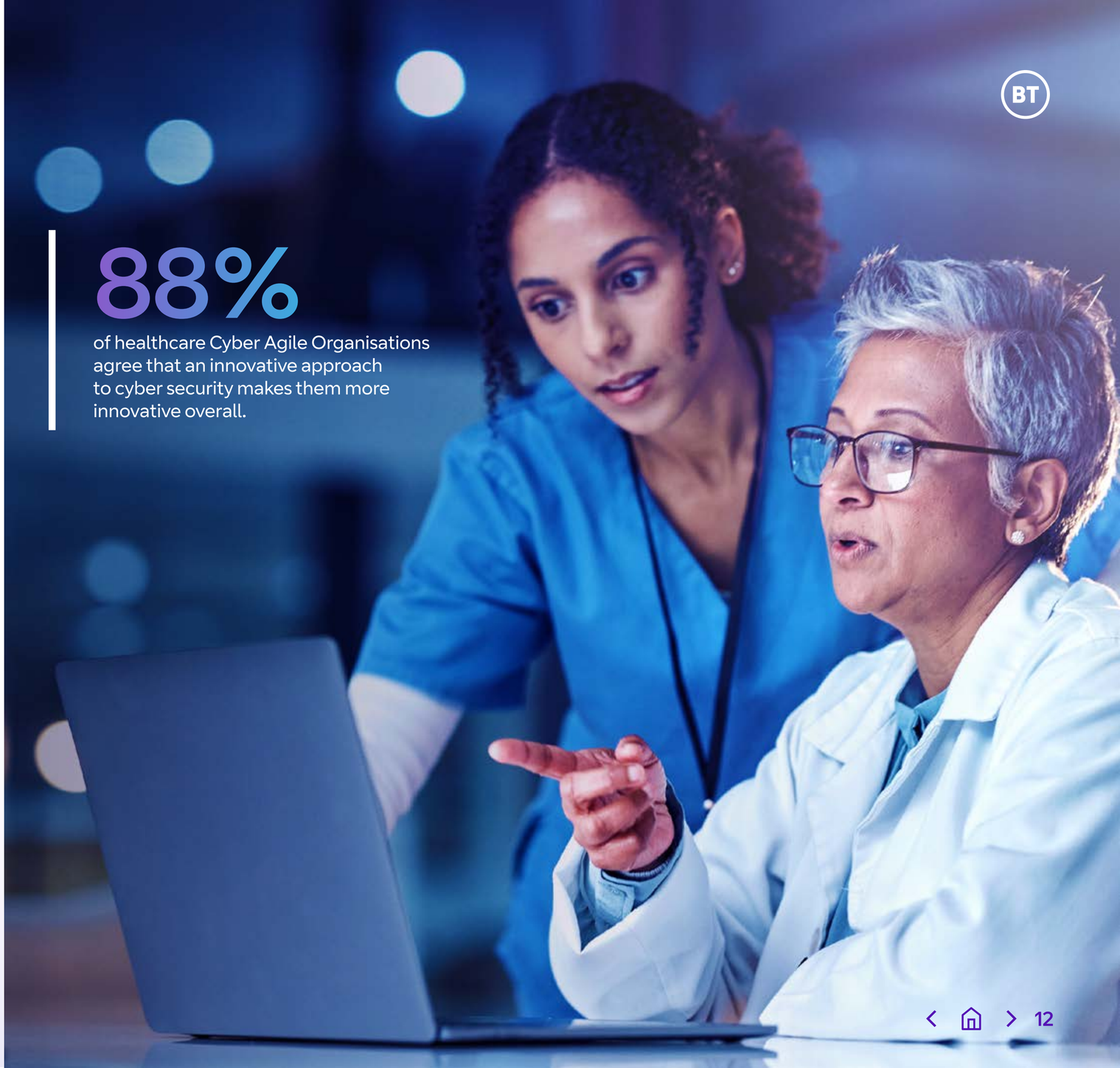
Innovation platform

Performance:
Innovation platform

With new technology entering the market and influencing positive outcomes, there has never been a better time to revisit innovation strategies. Nearly nine in 10 (**88%**) of healthcare Cyber Agile Organisations agree that an innovative approach to cyber security makes them more innovative overall.

With the increasing influence of productivity tools like GenAI and shadow AI, three-quarters of respondents believe this makes cyber security more important than ever, yet **65%** have turned this on its head, adding that they have implemented AI or machine learning tools for use in threat detection.

To keep innovating, organisations need robust protocols for staying in the game should a cyber attack prove successful. Healthcare Cyber Agile Organisations are more than twice as likely to recognise this than other organisations, arguing their incident resolution and recovery process is extremely useful in mitigating the impact of cyber risk (**37%** vs 16%).



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

1

Align your strategies

Strategies work best when everyone is moving towards a common goal. By aligning your security strategy with your organisation's 'true north' objectives, you can optimise people power and ensure your organisation is running at its most efficient.

2

Bring in the boffins

The first step on the road to cyber agility involves a highly-skilled security team. Recruit skilled experts, train teams across departments and empower them to communicate potential threats to top teams. Where a limited talent pool makes recruitment challenging, there is also the option to outsource specialist expertise to provide cyber security solutions that are tailored to your organisation.

3

Security for growth

Cyber security is a platform for innovation within your organisation. Take advantage by allowing free access to the latest technology and facilitating smooth collaboration between different groups.

UK market spotlight

In the UK, research published in 2023 shows eight in 10 healthcare providers have experienced a security breach since 2021.

As the backbone of the UK's health infrastructure, the National Health Service (NHS) faces unique vulnerabilities that threaten not just patient safety but the nation's overall resilience. In May 2023, the NHS experienced 1383 attempted cyber attacks per week, according to recent data. That compares with just 797 in May 2022, a near-doubling of the problem, plus it's reported that around 21 million malicious emails are blocked every month.

With the increasing digitisation of healthcare and reliance on interconnected systems, a robust and secure network is paramount to protecting sensitive medical data, ensuring operational continuity and safeguarding public trust.

Within our study, the increased use of AI and Internet of Things (IoT) devices rank as the two most significant cyber security risks within UK healthcare organisations' networks. Connecting medical devices via IoT significantly increases cyber security risks, as these devices can be vulnerable to hacking and unauthorised access. A breach could compromise sensitive patient data and disrupt critical care – making robust security measures essential.

While UK healthcare organisations may have oversight of their cyber risks, many lack resilience: **44%** report high visibility of their IT infrastructure and network, but do not have the adequate safeguards to keep it secure.

However, our research indicates significant innovation within the industry, with more than four in five UK healthcare leaders (**82%**) reporting that their organisation uses cutting-edge cyber security technologies.

> "Innovative approaches to threat detection and response are vital for the UK healthcare industry, empowering organisations to stay one step ahead of cyber threats which could harm patients and care standards. AI and machine learning tools can be used to monitor network behaviour, detect anomalies and automatically respond to potential threats in real time."
>
> **Professor Sultan Mahmud,** BT Director of Healthcare

Case study: NHS Integrated Care Board and BT

Discover how a security health check from BT's Security Advisory Services helped the **South West London Integrated Care Board** to better understand their cyber security posture and improve resilience.

Top 3 solutions either partially or fully implemented by UK healthcare organisations

- Threat intelligence platforms
- Automated incident response
- Deception technologies

Conclusion

Given the critical nature of healthcare services, bolstering cyber security is imperative to safeguard patient data and ensure uninterrupted care delivery. But a mature cyber agility strategy can help your organisation in other ways too.

Healthcare organisations that balance watertight security with the scope to continually improve can boost continuity of care and keep more people safe and comfortable. They are also less likely to fall foul of regulations and suffer fines from accidental or intentional data breaches.

Cyber agility, then, is a facilitator of best practice across the organisation, ensuring reputations remain untarnished and teams operate at their brilliant best. In short, healthcare organisations already meeting these criteria have the chance to do more, quicker and better across the board. As for the rest, now is the time to upgrade. Invest time, energy and budget in the latest security tools, specialist training and the brightest minds, and you will soon be reaping all the benefits that cyber agility brings.

BT's got your back

We take cyber security off your hands: At BT, we help protect mission-critical systems, freeing up your team's time to focus on what matters – patient care. With 24/7 round-the-clock support, we help you build full visibility of your network, so you can prevent breaches or stop them early before they disrupt clinical service delivery.

We consolidate your security: We understand many businesses have fragmented services across their security ecosystem. At BT, we can bring it all together and manage the process for you.

Cyber Assessment Framework (CAF) Assessment: Utilising our CAF assessment, we help healthcare organisations better understand their cyber security posture and provide a holistic view of their infrastructure and any vulnerabilities that are present. Using our assessment can help organisations define clear actions to strengthen their defences.

BT Means Business

Get the conversation started

Talk to us

Offices Worldwide

JN: 1634561879