BT Means Business

# The Cyber Agile Organisation:

# Professional Services

## Transforming security into a platform for growth

business.bt.com

# Contents

# Foreword

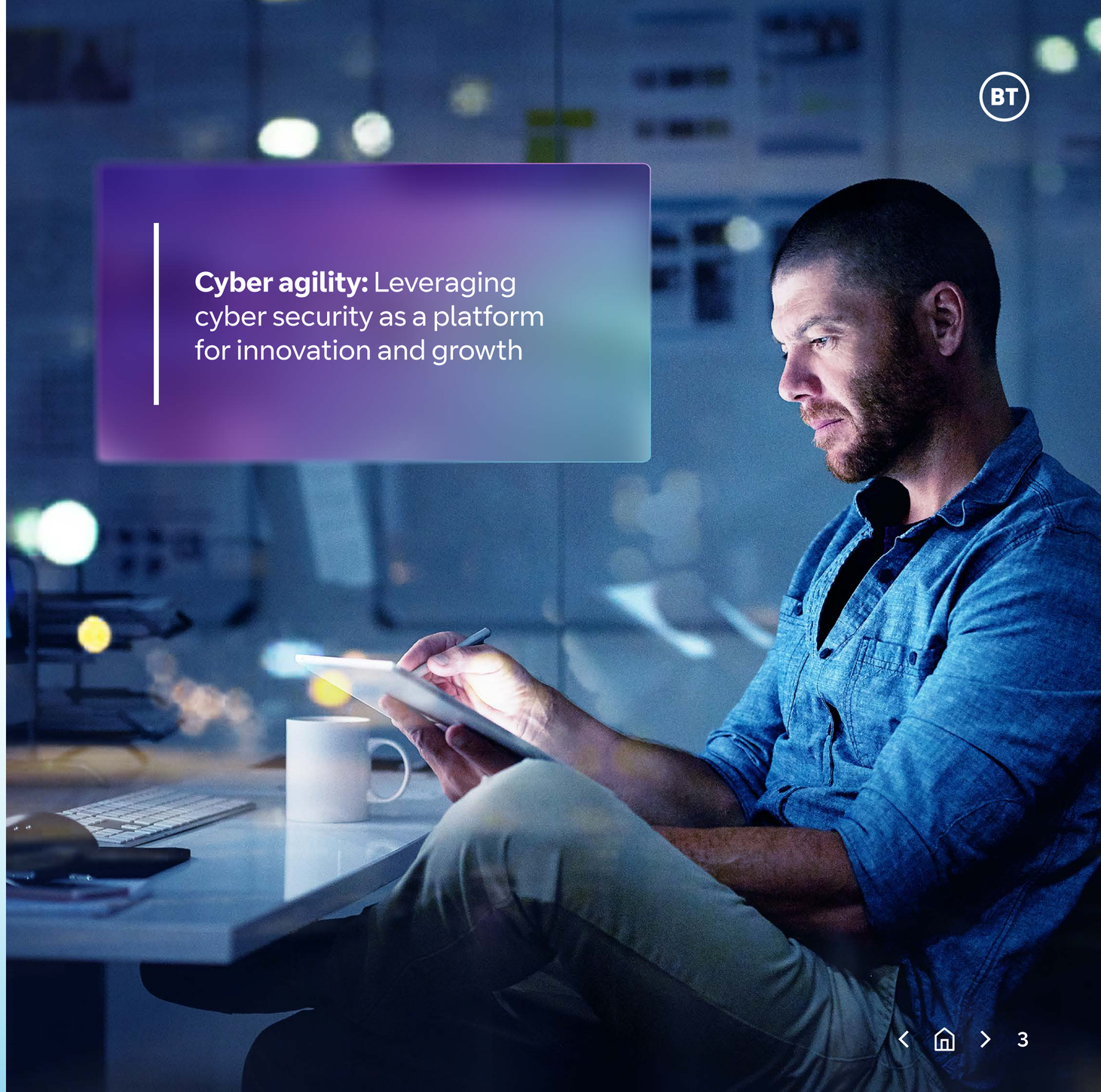
**The professional services sector faces a rapidly evolving cyber threat landscape.**

Legal firms, consultancies and accountancy practices are all prime targets due to the sensitive data they handle and their integral role in high-stakes transactions. Cyber criminals and nation-state actors alike seek access to confidential client records, intellectual property and strategic business information.

The stakes are high. Beyond financial loss, a major cyber incident can shatter the trust that underpins professional services, jeopardising client relationships and competitive positioning. This makes a proactive, agile approach to cyber security not just a protective measure, but a strategic imperative.

Professional services organisations need security embedded into their operations, beyond digital infrastructure. They need to maintain security to manage risk and stay compliant with evolving regulations. A mature approach to cyber security helps organisations keep on top of tech advances and evolving cyber threats.

However, when implemented correctly, cyber security is not just a defence mechanism but an enabler of innovation and a platform for confident experimentation. Firms can execute deals, commission work and form partnerships, secure in the knowledge that their cyber safety net is in place.



# Foreword

## Cyber agility in professional services

In this study, we aim to distil the key elements of what confers cyber agile status upon businesses. This is the who, what, where, and how of cyber security, the strategies and the execution that propels them to the head of the pack.

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

Cyber Agile Organisations enjoy a strategic advantage because they can experiment, collaborate and innovate, free from concern about how it affects the risk profile.

From daily workflows and remote working, comprehensive cyber agility can enable the workforce to work from anywhere, on any device – securely. This gives a client-facing professional workforce the tools to do the job smoothly, without security measures implicating user experience and flexibility.

It's an important study for any organisation wanting to understand the DNA of cyber agility in an evolving global economy. It's also your chance to learn how you can elevate your businesses to the status of a Cyber Agile Organisation, building confidence among your people and clients.

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

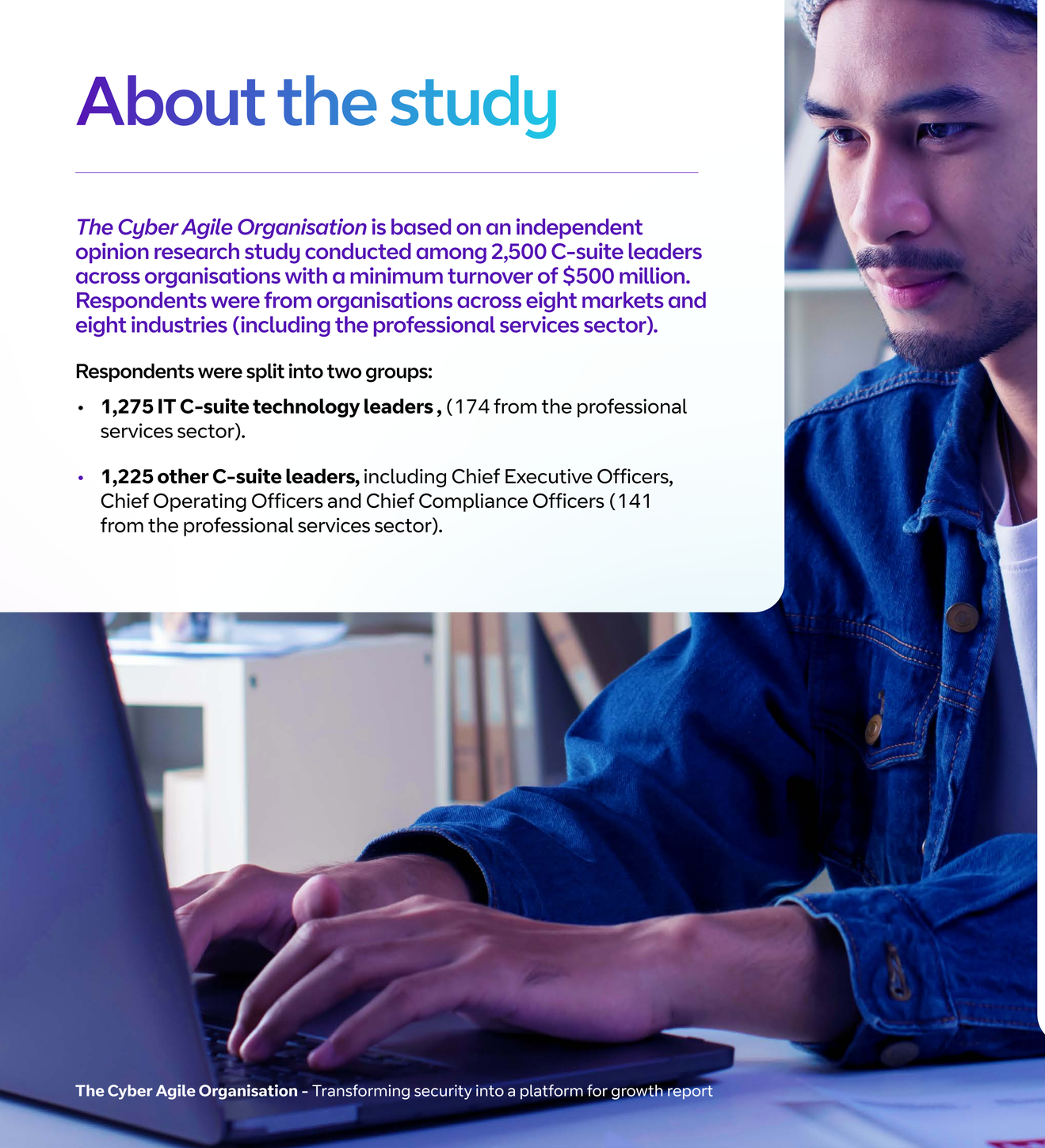
**Tristan Morgan,**
Managing Director,
Security, BT

# 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 professional services sector).

Respondents were split into two groups:

- **1,275 IT C-suite technology leaders ,** (174 from the professional services sector).
- **1,225 other C-suite leaders,** including Chief Executive Officers, Chief Operating Officers and Chief Compliance Officers (141 from the professional services 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.

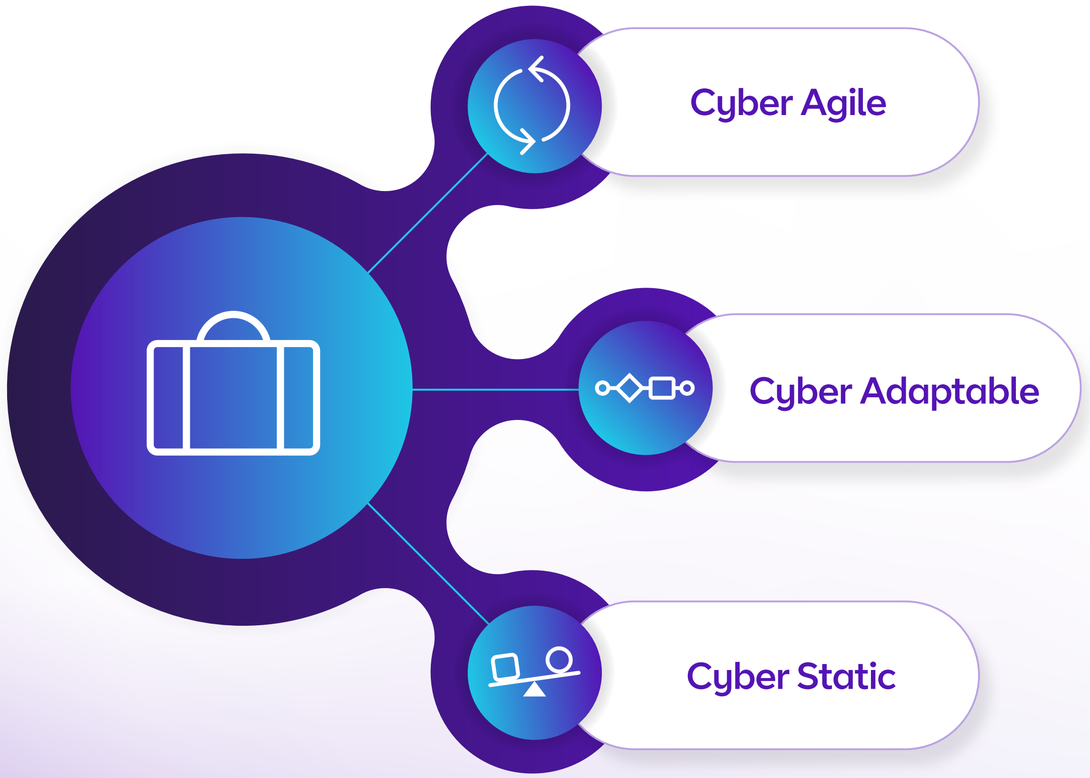

### Innovation

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

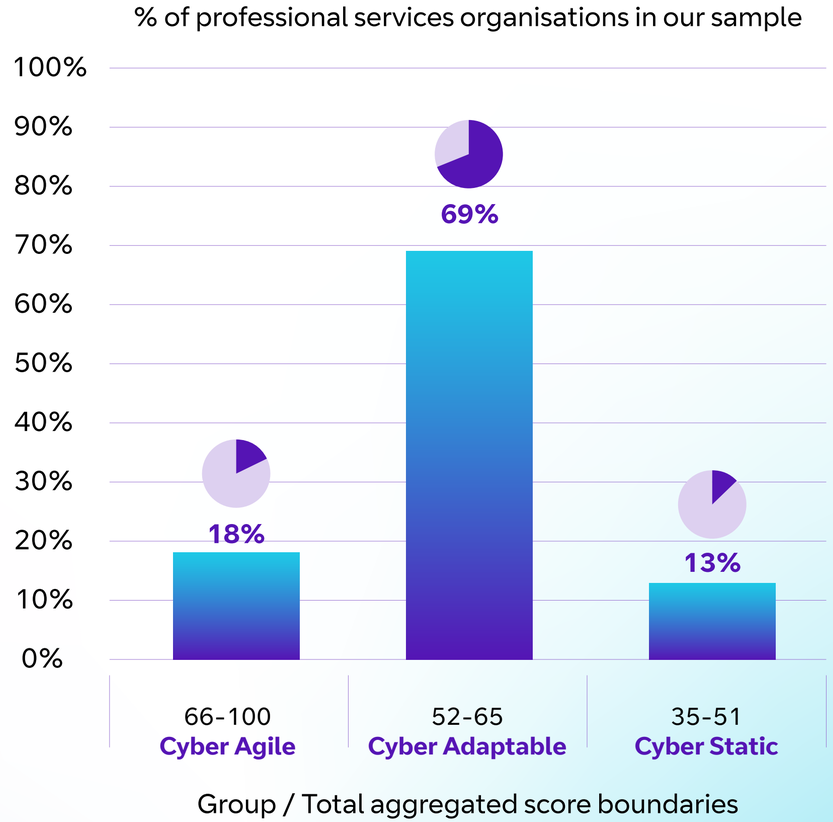
# The cyber agility scoring system

**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 attack surge

The professional services sector is perhaps not the first industry that springs to mind when people think of primary targets for hackers and cyber criminals.


**33% of organisations say cyber attack severity is high or very high**

Yet around a third (**33%**) of the organisations taking part in our study perceive the current severity of cyber attacks their organisation has experienced as either ‘high’ or ‘very high’. This figure is set to jump to nearly half (**46%**) that expect the severity of cyber attacks to be ‘high’ or ‘very high’ over the next three years.


**62% say a major cyber attack is their main existential threat**

Furthermore, 62% of professional services leaders say that a major cyber attack is the main existential threat to their organisation.

## Prepared to protect

Better news comes in the form of professional services organisation’s preparedness to deal with the challenge they face. While a third are experiencing high levels of cyber attack severity, nearly 6 in 10 (**58%**) say they are either ‘very’ or ‘extremely’ prepared to deal with them. And a larger number (**71%**) believe they’ll be very or extremely prepared in the next three years – demonstrating that cyber agility is on the agenda.

**Nearly 6 in 10 (58%) say they are either ‘very’ or ‘extremely’ prepared to deal with cyber attacks**

# Cyber security self-assessment for professional services organisations

## Maturity level

### Initial implementation

5%

We're 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

43%

We've 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

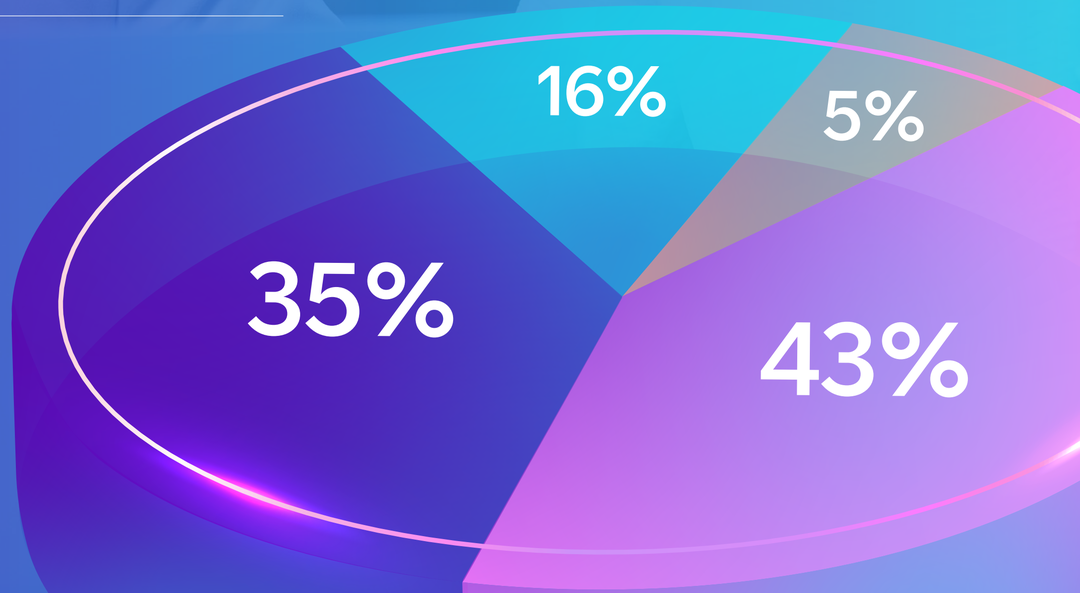
35%

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

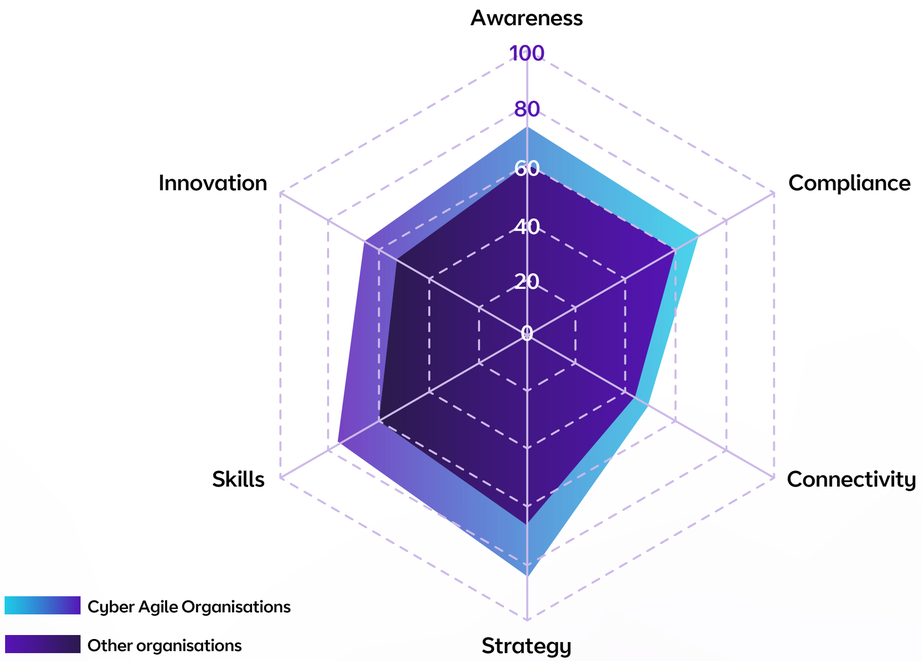
16%

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 professional services organisations.




| Dimension | Cyber Agile Organisations | Other organisations |
|---|---|---|
| Awareness | 75 | 58 |
| Compliance | 67 | 60 |
| Connectivity | 48 | 43 |
| Strategy | 86 | 68 |
| Skills | 77 | 59 |
| Innovation | 60 | 52 |

## Cyber agility gaps

Of the professional services businesses taking part in our study, only **18%** qualify as Cyber Agile Organisations. We uncovered major gaps between these sector leaders and the chasing pack, particularly within the Awareness, Strategy and Skills dimensions – with the biggest divergence seen for Strategy and Skills.

A secure IT network is a cornerstone of cyber security and, by extension, cyber agility. It makes sense, then, that **68%** of professional services leaders see a secure network as a prerequisite for doing business. In a hybrid-working world, the need for security extends beyond the office; a secure network safeguards users, devices and information across digital boundaries.

Cyber Agile Organisations achieved 24% higher growth rates over three years.

But cyber agility is more than a formality; it gives organisations a competitive edge. Over the last three years, Cyber Agile Organisations in professional services achieved **24%** higher growth rates compared to others in the industry.

## Boosting customer trust

The majority of professional services leaders in our study (**82%**) identify increased customer trust as a significant potential benefit that improved cyber agility would bring to their organisation. If made real, this would be a huge boost to any firm in the sector. Whether it's lawyers protecting client funds, consultancies handling M&A deals or accountancy firms managing sensitive data, trust is crucial for winning and conducting business effectively.

## Further potential benefits, as cited by respondents, include:

- 77% Improved overall business agility
- 76% Improved reputation
- 74% Improved collaboration
- 67% Reduced management time

Cyber Agile Organisations in the professional services sector see the connection between security and creativity: **86%** believe innovating their approach to cyber security helps them to become more innovative generally, compared to **75%** of other organisations.

“In an industry where reputation is everything, executives might not be worrying about the vulnerabilities and data protection risks that come with adopting cloud of AI technologies. But failure in these areas could cause reputational damage and ultimately hit bottom line earnings. Adopting a secure by design approach enables organisations to leverage the transformative benefits of these new technologies.”

**Michele Metcalfe,** Professional Services, Media and Communications Director, BT

# Part 2

## Becoming cyber agile: Key focus areas for professional services organisations

The majority of organisations in professional services predict that their cyber security budgets will increase over the next three years, by an average of 13%. But it's no good being flush with cash if you don't spend it in the right areas.

# Preparedness:
# Securing connectivity

## Network security backbone

In a highly competitive sector where trust and reliability are paramount, investing in comprehensive network security is not just a protective measure; it's the backbone of operational continuity. It ensures that critical systems, such as case management tools, financial platforms and client collaboration portals remain accessible and protected from disruptions.

Just below three-quarters (**71%**) of Cyber Agile Organisations in the professional services sector claim to have high visibility of their IT infrastructure and network and strong safeguards to keep them secure. This is compared to just **33%** of other organisations in the industry.

Professional services firms face critical challenges in safeguarding their networks given the rise in remote work, personal devices (BYOD), and connected IoT and collaboration tools. Insider risks and insufficient network segmentation, further expose systems to attacks.

Additionally, reliance on third-party vendors and cloud services demands secure data integrations and compliance regulations. A holistic multi-layered security strategy is essential to mitigate these risks and maintain client trust.

## Top 5 connectivity cyber risk factors for professional services organisations:

- **Devices connecting to public or insecure wireless networks**
- **Internet of Things (IoT) devices**
- **Increasing number of devices**
- **Unsanctioned use of personal devices**
- **Using multiple clouds**

So, how can organisations mitigate these risks to support seamless remote work, avoid uninterrupted service delivery and meet client expectations?

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

## 1

### Understand your cyber risk

Cyber security has become a board-level priority, but measuring risk remains a challenge. 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. Maintaining a 'live' threat analysis to track key risks and highlight emerging vulnerabilities will help keep your network secure, now and in the future.

## 2

### Watch your devices

Empower your people to thrive and capitalise on your investment in devices by protecting them from identity misuse, endpoint threats and data loss. Mobile device management and security applications can help to increase visibility. If it's essential that people use their own devices in your network, establish robust protocols for when, where and how they can be used. And keep security front of mind with regular reminders and updates.

## 3

### Keep track of regulation

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.

# Performance:
# Boosting skills

Demonstrating cyber agility isn't just about secure networks, endpoints and compliance; it's about equipping your workforce to protect themselves and the business. In a fast-paced work environment with constant communications on various devices and platforms, vigilance is key to protecting company and client information.

Over half (**52%**) of professional services leaders in our study say their team struggles to stay one step ahead of the cyber risk they face, while **65%** say human error is the biggest threat to their organisation's cyber security.

Employees are the first line of defence against cyber attacks, so it makes sense that more than eight in ten (86%) Cyber Agile Organisations report that they are actively building a cyber security culture, compared to **69%** of other organisations. In total, professional services businesses invested an average **$2.9 million** in cyber security training for employees over the last 12 months.

This is good news, but building a mature and holistic security culture requires employees at all levels to embrace their responsibility for IT security. Cyber agility must be embedded in the very DNA of an organisation, shaping its culture, streamlining operations, fortifying infrastructure and driving innovation.

**4 in 10**
**provide role-specific cybersecurity training**

More than half of professional services firms (**52%**) mandate regular cybersecurity training for all employees as part of their professional development. Some 4 in 10 provide role-specific cybersecurity training for key departments, such as IT and finance, while **24%** encourage security teams to acquire professional qualifications and participate in industry events.

Cyber Agile Organisations are more likely to have specialist cyber security professionals in place, with **71%** already employing a Chief Information Security Officer compared to **54%** of other organisations in the industry. Additionally, **62%** of Cyber Agile Organisations have a Cyber Security Architect, and **57%** already have a Security Operations Centre Analyst.

Currently, **44%** of professional services organisations are actively recruiting for AI and Machine Learning Security Specialists, and **41%** are recruiting for Threat Intelligence Analysts. All this highlights the diverse skill sets required to survive and thrive in the modern digital environment.

### Professional services firms' five greatest cyber weaknesses

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

“As firms rush to implement AI and machine learning to automate routine tasks, improve decision making and enhance client services, it will be important to integrate security measures at each stage. AI systems that rely on sensitive client data are prime targets for cyber criminals, making it essential for all team to prioritise data privacy and confidentiality to minimise the risk of unauthorised access.”

**Michele Metcalfe,** Professional Services, Media and Communications Director, BT

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

## 1

### Strengthen communication for cyber awareness

Clear, concise and accurate communication at all levels is critical for building a unified understanding of cyber risks and responsibilities. Regularly update employees on emerging threats, key policies and their roles in maintaining security, ensuring alignment between strategy and execution.

## 2

### Strategic budgeting for resilience

Cyber security budgets must be dynamic and comprehensive, incorporating the costs of technology, skilled personnel and proactive threat mitigation measures. Tailor your investment to reflect your unique risk profile, compliance regulations and the evolving threat landscape.

## 3

### Unlocking your human firewall

As cyber threats constantly evolve, we must stay vigilant. That means ensuring your people, from new recruits to veterans, keep up with the latest developments. Implement continuous, role-specific training, focusing on threat detection, secure practices, and incident response. Given the complexity of cyber threats, leveraging external expertise from Managed Security Service Providers can enhance your internal capabilities.

# Conclusion

## Evolution

**Like all industries, the professional services sector is changing under impetus from new technology, plus the thinking, strategies and processes underpinning every new era. But in the modern knowledge economy, clients still want expert, timely consultancy, advice and bespoke systems.**

## Resilience

As we have discovered, Cyber Agile Organisations have a better opportunity to deliver in these areas. Equipped with cutting-edge security tools, processes, systems and practices, client-facing professionals are empowered to work from anywhere, knowing their data, devices and people are protected. This enables organisations to stay agile, compliant and resilient in a world of growing threats and risks.

## Advantage

This amounts to an edge in a fiercely competitive global market where small details and trust really matter. Leaders in cyber agility know this – and have taken the necessary steps to position themselves for operational resilience and sustainable growth.

## Awakening

For everyone else, this should come as a wake-up call. It's not too late to begin on the cyber agile journey, by adopting the software and protocols needed to keep bad actors at bay and to recover when an attack occurs. With swift action, they too can join the cyber agility elite.

# BT's got your back

## We unify network and security expertise

Decades of experience protecting BT and our customers has equipped us with extensive knowledge of securing all network, connectivity and cloud layers – whether this be SASE, internet access, sites, supply chain or end users and endpoints. This expertise enables us to guide customers on their end-to-end transformation programs.

## We're always innovating

Our Cyber Assessment Lab delves into technology to uncover innovative new solutions. We invest in innovation to improve outcomes for our customers, and we are experts in understanding active defence solutions, keeping one step ahead to understand emerging technologies such as post-quantum cryptography and quantum key distribution. We are currently using AI and Machine Learning extensively to accelerate prevention, detection and response capabilities.

## We can help get your house in order

We offer governance, risk and compliance audits and Advisory services. We can help quantify your cyber risk using the SAFE methodology and support your people security strategy with training programs, policies and processes. Organisations can reduce management time with BT secure managed services, enabling them to focus on strategic and client-facing priorities. For field and frontline workers there's improved collaboration with our network and mobile security portfolio, enabling them to work from anywhere, on any device.

## We keep humans in the loop

Security isn't just about technology. We integrate human expertise into our end-to-end solutions, combining automation and semi-automation where appropriate to provide accurate, comprehensive, and cost-effective cyber security defence. This approach leads to stronger protection and better alignment with specific business needs. Our Security Operations Centres are available to support 24/7, 365 days of the year.

BT Means Business

# Get the conversation started

Talk to us

**Offices Worldwide**



JN: 1634561879