BT Means Business

The Cyber Agile Organisation:

Energy and Resources

Transforming security into a platform for growth

business.bt.com

Contents

Foreword

As the energy and resources sector undergoes unprecedented transformation, connectivity and cyber security are becoming two of its most critical enablers. From the digitisation of traditional oil and gas operations to the rise of renewable energy, hydrogen, wind, solar and biomass as key players in the energy transition, protecting and connecting the systems that power our world has never been more important.

Cyber ransom hunters, rogue states and thrill seekers seek to exploit weaknesses in energy and resource systems for disruption, financial gain, intelligence gathering or IP theft.

Recent geopolitical conflicts have seen state actors disrupt each other's energy supplies through system subversion, posing a significant threat to large-scale infrastructure projects, particularly in solar and wind energy.

The potential impact of a coordinated attack is immense, from power outages and water supply interruptions to economic impacts and health implications. Recovery times can also be longer than in other industries.

To mitigate these risks, organisations in this sector must prioritise cyber security, employing the best people, tools and processes to protect against global threats. By enhancing their cyber security measures, these organisations can not only shield themselves from cyber crime but also create a foundation for innovation, collaboration and sustainable growth.

At BT, we refer to this approach as 'cyber agility'. A cyber agile approach goes beyond traditional cyber security by balancing threat mitigation with business success. Our study of companies in this sector identified the top performers as 'Cyber Agile Organisations', revealing the key ingredients to their success.

Want to learn more about these advanced organisations and how to 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 are from organisations across eight markets and eight industries, including 229 leaders from the energy and resources sector.

Respondents were split into two groups:

- **1,275 IT C-suite technology leaders.**
- **1,225 other C-suite leaders,** including chief executives, chief operating offers and chief compliance officers.

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

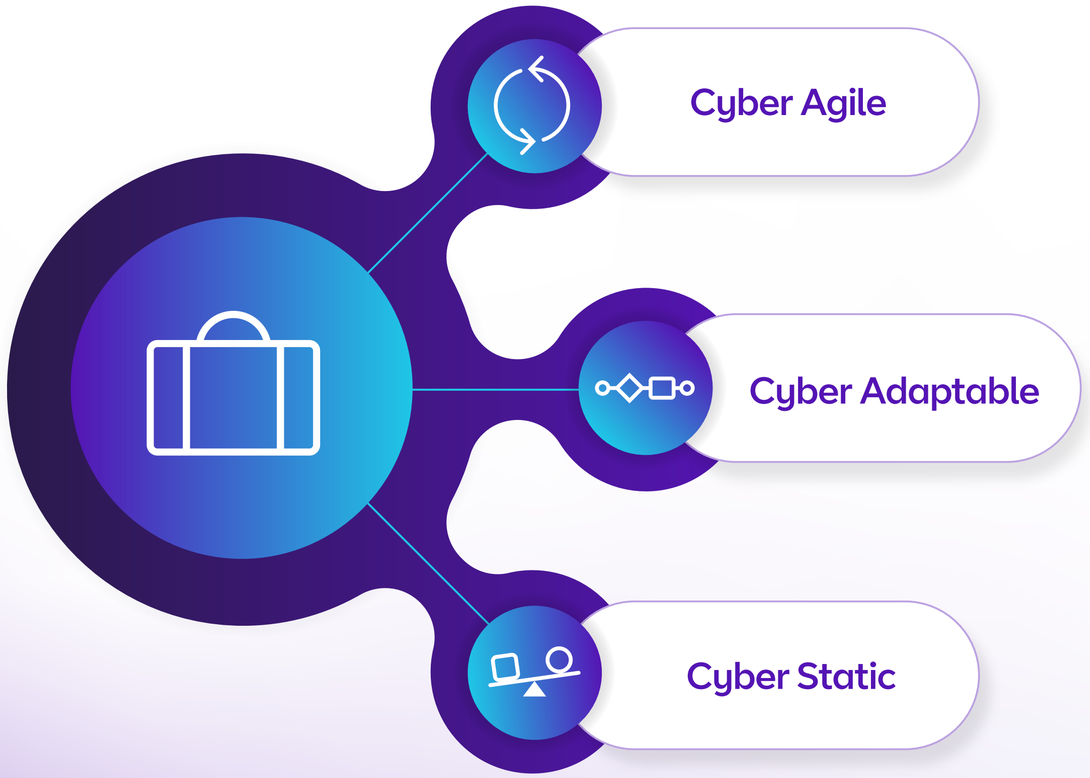
The extent to which cyber security is used as an enabler for innovation and broader organisational transformation.

The cyber agility scoring system

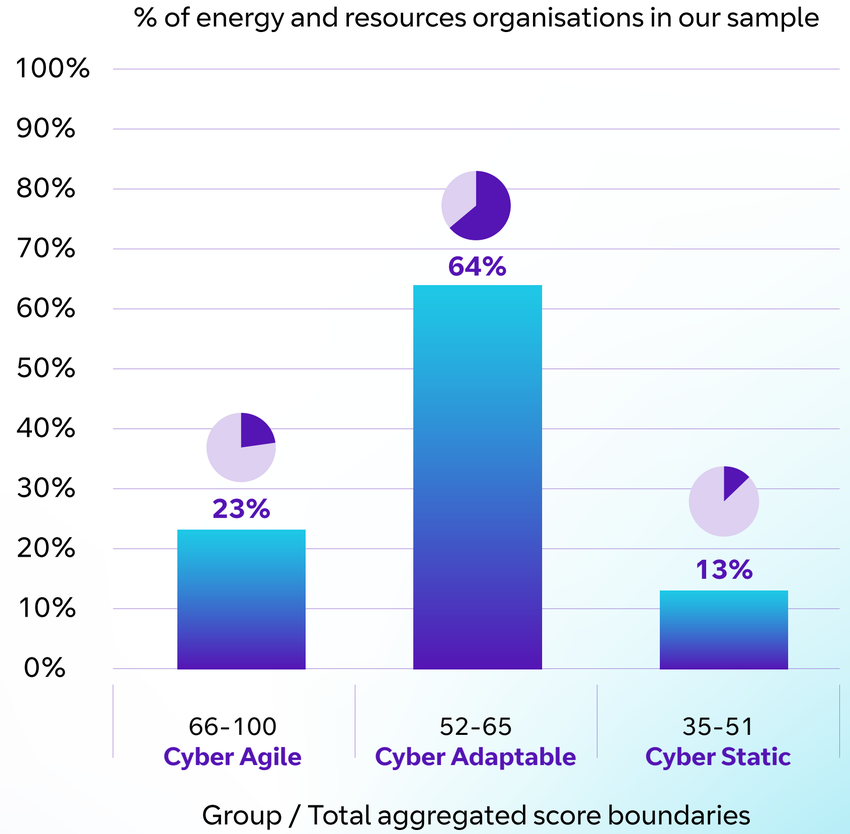
Cyber agility scores were based on performance in the six dimensions: Awareness, Compliance, Connectivity, Strategy, Skills and Innovation. Each dimension comprised a set number of questions from the opinion research which were attributed different weightings. In total, each dimension was valued at 30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

Soaring cyber threats

By leveraging advanced data systems, IoT, smart infrastructure and robust global networks, energy and resources organisations are driving innovation and reducing carbon footprints. However, these advancements come with heightened risks. Sophisticated cyber threats targeting operational systems, energy grids, and critical infrastructure are on the rise, requiring robust security and seamless global connectivity to maintain resilience and trust.

More than a third (**35%**) of energy and resources leaders in our study are currently experiencing either 'high' or 'very high' cyber attack severity. This figure rises to **53%** of businesses when asked about their expectations of cyber attack activity over the next three years. It's a particularly worrying trend given that two-thirds (**66%**) admit that a major cyber attack is the main existential threat to their organisation.

35% of energy and resources leaders report high or very high cyber attack severity.

66% see a major cyber attack as their organisation's top existential threat.

Prepared to protect

Businesses in the energy and resources space are prepared to act in the face of cyber pressures to defend themselves against the worst possible outcomes. Currently, almost 6 in 10 (**57%**) consider themselves to be either 'very' or 'extremely' prepared to deal with cyber attacks. Looking ahead, two-thirds (**66%**) anticipate reaching this level of preparedness within the next three years.

Almost 6 in 10 (57%) say they are either 'very' or 'extremely' prepared to deal with cyber attacks

Cyber security maturity self-assessment for energy and resources organisations

Maturity level

Initial implementation

8%

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

35%

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

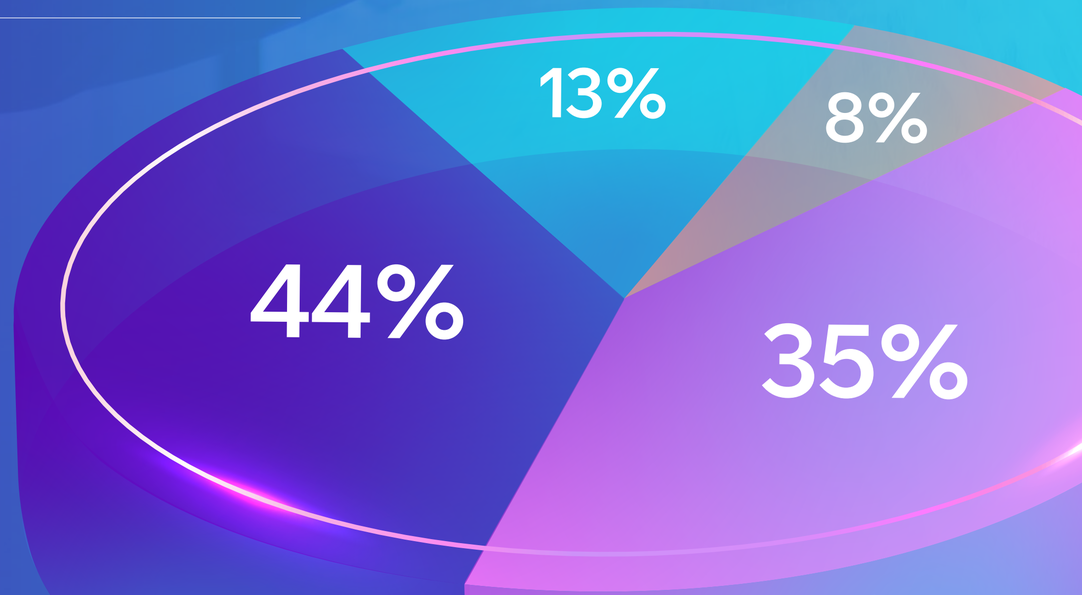
44%

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

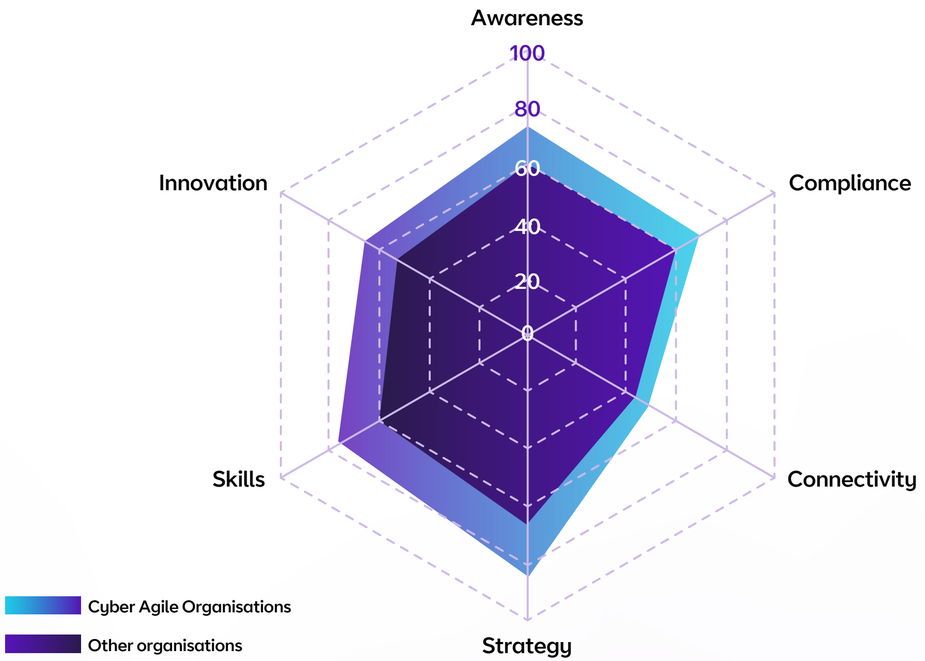
13%

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 energy and resources organisations.



Dimension	Cyber Agile Organisations	Other organisations
Awareness	73	60
Compliance	73	61
Connectivity	50	41
Strategy	85	67
Skills	75	59
Innovation	63	53

Of the energy and resources businesses taking part in the study, **23%** qualify as Cyber Agile Organisations, which puts the industry near the top of the sector rankings, just second to Finance and Banking.

But, despite this, there are gaps between sector leaders and the following pack, particularly within the Awareness, Strategy and Skills dimensions – with the widest discrepancy seen within the Strategy dimension.

Over the last three years, Cyber Agile Organisations achieved 27% higher growth rates than other organisations from the same industry – the greatest difference among all the sectors in our study.

With such a stark disparity between Cyber Agile Organisations and the rest within the energy and resources sector, it's perhaps surprising that a high number – **63%** – of businesses in this industry consider secure IT systems as a prerequisite for doing business.

Breaking down the benefits further, the vast majority, **77%,** see cyber agility increasing customer trust, while even more, **78%,** said it gave a boost to business efficiency and **79%** thought it improved corporate reputation.

> "The energy and resources sector never stands still, so businesses need to be nimble and responsive to change. Cyber agility lets them forge ahead with plans and ideas without fear of security threats."
>
> **Lee Stephens,**
> Director of Security Advisory Services, BT

Cyber agility also plays a significant part in keeping communication channels open, facilitating teamwork in-house and via external connections with partners and suppliers. More than three-quarters (**76%**) of leaders in energy and resources pointed to improved collaboration as a significant benefit, while the same said it produced more secure connectivity.

Australia and Singapore market spotlight

Energy and resources leaders in Australia seem confident about their ability to deal with cyber threats. They are the least likely to expect the severity of cyber attacks to be high or very high over the next three years, with only **36%** anticipating this.

Across all industries, leaders in Australia also claim their organisation's skills and knowledge in various areas of cyber security are stronger than the global average.

But it's a different picture in Singapore, where energy and resources leaders are least prepared for an attack, with only **35%** believing they are either 'very' or 'extremely' prepared.

83% of Singaporean leaders avoid suppliers without security credentials.

It's no coincidence that, across all industries, **83%** of leaders in Singapore say their organisation will not work with suppliers who lack adequate security credentials, the highest percentage of all countries.

> **"It's clear that organisations with mature and cautious approaches to cyber security can rest easy at night, knowing their business is set up for safe, secure and sustainable growth."**
>
> **Lee Stephens,**
> Director of Security Advisory Services, BT

BW Group and BT - Case study

Discover how BT works with **BW Group**, one of the world's leading maritime groups, to tackle cyber risk and ensure uninterrupted business continuity. Our closed-loop threat management programme enables BW Group to identify, assess and prioritise vulnerabilities, track the results of actions taken, and feed learnings back into the system for continuous improvement.

Part 2

Becoming cyber agile: Key focus areas for the energy and resources industry

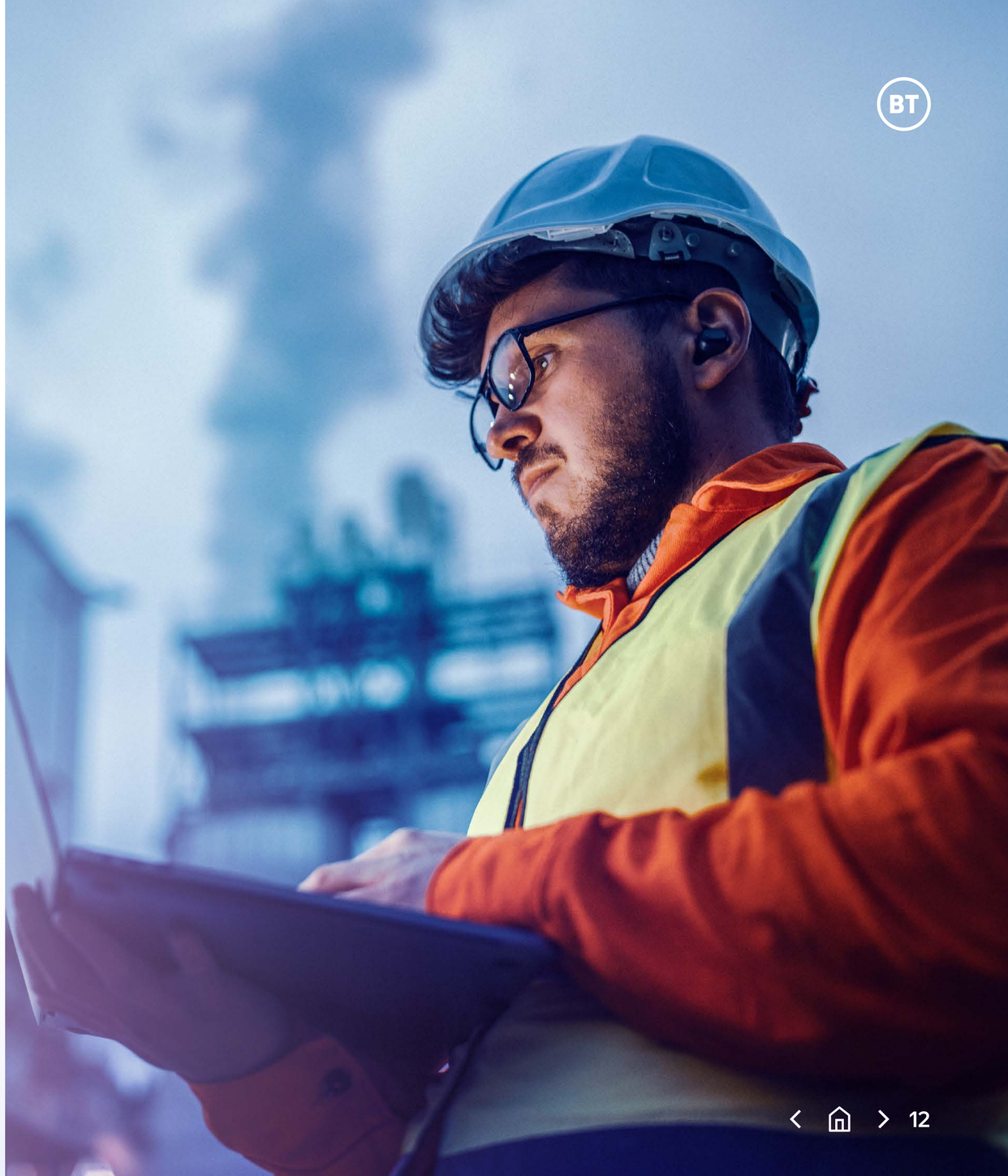
Becoming cyber agile: Key focus areas for the energy and resources industry

From fossil fuels to renewables, hydrogen to emerging technologies, the energy sector's evolution demands innovative thinking. The question is: how can these organisations unlock their potential while staying ahead of evolving cyber threats?

Most energy and resources businesses expect a 13% budget increase in the next three years.

A critical piece of the cyber agility puzzle is allocating appropriate financial clout to cover the organisation's security needs now and in the future. Most businesses in the energy and resources space expect budgets to increase in the next three years, by an average of **13%**.

But, while it's good to know money is being made available, organisations must work hard to uncover the areas most in need of critical investment. According to the research, a major area of risk for this sector is the ballooning number of connected devices and how these are used.



Protection:
Securing connectivity

Secure connectivity is the backbone of the renewable energy transformation, but organisations face several challenges.

Increasing number of devices

Unsanctioned use of personal devices

Devices connecting to public or insecure wireless networks

The proliferation of devices complicates the job of gaining and retaining visibility over IT networks. Even so, some **63%** of Cyber Agile Organisations in energy and resources say their business has a 'high visibility' of its IT network and strong safeguards to keep them secure, compared to only **36%** of other organisations in the industry.

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

1

Get a clear picture

Carry out a comprehensive risk assessment of your entire IT ecosystem, integrating physical and cyber risk management, using a range of reliable information sources and creating an action plan to address problems raised.

2

Digital sovereignty

Take a proactive approach to operational resilience by ensuring you're adhering to data sovereignty regulations while monitoring the broader regulatory landscape and using this to shape your cyber security strategy.

3

Invest in resilience

Adopt a zero-trust architecture, conduct regular penetration testing, and ensure real-time threat detection. Develop incident response plans to ensure quick recovery capabilities in case of a successful attack.

Performance: Driving innovation

Without secure foundations for growth, it's hard to get people to innovate, but cyber security has a stronger bearing on innovation than simply providing its bedrock. Nearly four in five (**77%**) leaders within the energy and resources industry agree that innovative cyber security makes them more innovative overall.

Even seemingly separate elements such as incident resolution and recovery have an influence, with **32%** of Cyber Agile Organisations within the energy and resources industry saying their processes ensure quick recovery and minimal disruption, compared to **22%** of other organisations.

They are also more likely to channel innovation tools into their cyber security processes. While **74%** of energy and resources leaders worry the explosion of GenAI in the workplace has made security more important, **69%** have turned the tables and implemented AI or machine learning technology for threat detection.

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

1

Board-level oversight

Elevate cyber security to a strategic priority and align it to your organisation's 'true north' objectives to optimise people power, drive behaviour change, negate wasted effort and ensure your organisation is running at its efficient best.

2

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.

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.

Conclusion: Powering the future of energy

Sustainability

Businesses in the energy and resources sector have a key role to play in reducing carbon emissions and helping to limit global warming. They must adapt to become leaner and less polluting, while simultaneously facilitating ready access to the fuels and raw materials that can satisfy future needs.

Resilience

It's a tall order – and one the industry can only hope to fulfil if it is equipped with the best people, tools and procedures to get the job done.

Cyber agility is a major ingredient of this: keeping organisations secure and stable, giving them the confidence to plan, partner and develop, free from fear of hackers and data thieves.

Vigilance

With a healthy complement of Cyber Agile Organisations, the energy and resources industry can feel confident about its future. But this is no time to rest on its laurels; businesses should go on assessing, evaluating, investing and upgrading to ensure they're equipped to deal with the cyber threats of tomorrow.

Empowerment

At BT, our mission is to help partners embrace digital transformation with confidence, ensuring their systems are secure, connected and resilient.

Let's shape this future together.

BT: Your partner for cyber agility

End-to-end secure connectivity

At BT, we ensure the security of your operational technology (OT) at every touchpoint across your IT estate and down the supply chain. Leveraging cutting-edge technology, including artificial intelligence, we keep your data secure and confidential. Our advanced AI algorithms provide real-time threat detection and automated responses, significantly reducing the risk of cyber attacks.

Supporting sustainable transformation

Through our partnership approach, BT can guide your business through its digital transformation, embedding security at every stage. We are dedicated to helping you adopt and implement energy-efficient technologies and practices while maintaining robust security measures and ensuring compliance with global standards such as NIST, ISO 27001 and IEC 62443.

Collaboration, partnerships and ecosystems

With our extensive cross-vertical expertise, we offer comprehensive solutions to optimise your overall security posture.

Global reach, local presence

BT's unparalleled network coverage enables us to securely connect remote sites, offshore platforms, renewable facilities and data centres across continents.

BT Means Business

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