BT Means Business

The Cyber Agile Organisation:
Financial services

Transforming security into a platform for growth

business.bt.com

Contents

Foreword

The financial services industry has undergone a technology-fuelled transformation in the last two decades; what started with progressively better digital experiences became a flywheel of opportunity with new ways to leverage rapidly evolving technology. Smartphones, artificial intelligence and machine learning, combined with a dynamic regulatory environment, are providing customers with a vast array of upgraded services.

But this change comes with challenges. For obvious reasons, cyber criminals tend to target businesses whose stock-in-trade is money, making financial services businesses particularly vulnerable to risk. To complicate matters, the digitisation and distribution of devices, software and services, as well as increased collaboration and integration, means a broader attack surface for criminals who want to disrupt the system for their own financial gain.

It goes without saying that companies in the financial services industry need the best cyber protections available, on top of grown-up strategies, formal training and water-tight security protocols. But it doesn't stop there. Today, there's an opportunity to blend cyber security into enterprise-level strategies, making it a cornerstone of plans for growth.

Security is the bedrock of business performance, a platform upon which organisations can do more, faster and better. It facilitates secure, well-governed change, allowing institutions to respond quickly to their market, customers and competitors.

This is the key benefit of what we call '**cyber agility**', the highest level of cyber preparedness combined with efficient systems that allow businesses to seize each new opportunity as it comes; to experiment, innovate and execute plans with confidence, even in an industry that is heavily regulated with high cyber risk.

Foreword

Time to get agile

A Cyber Agile Organisation proactively adapts to cyber regulation and reporting, implements the best security software, regulates supply chain risk, conducts regular and effective training, and employs credible strategies for responding to incidents.

These protocols help financial services enterprises deliver better products and services, receiving in return higher levels of trust and loyalty from customers confident their money is in safe hands. At the same time, employees can collaborate securely in line with evolving regulations, plus develop new skills and knowledge using tools like artificial intelligence in a safe environment.

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 from organisations across eight markets and eight industries (including the financial services industry).

Respondents were split into two groups:

- **1,275 IT C-suite technology leaders**, including 174 from the financial services industry.
- **1,225 other C-suite leaders**, including Chief Executives, Chief Operating Officers and Chief Compliance Officers, including 188 from the financial services 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.

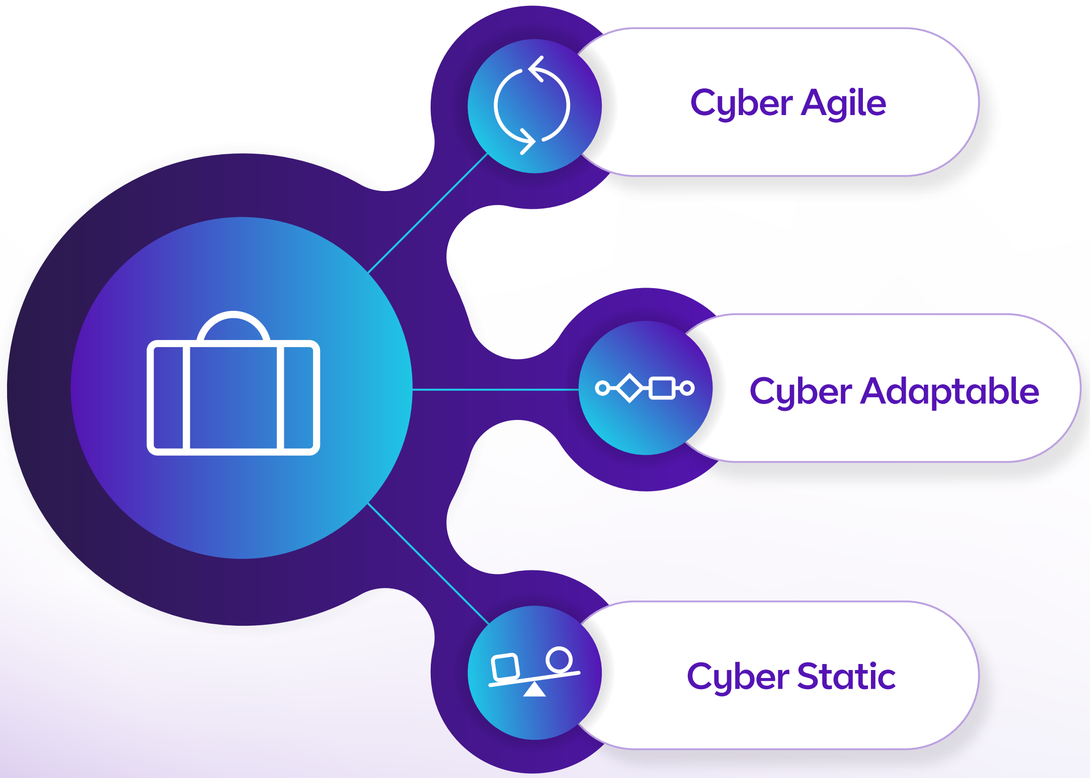
Innovation

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

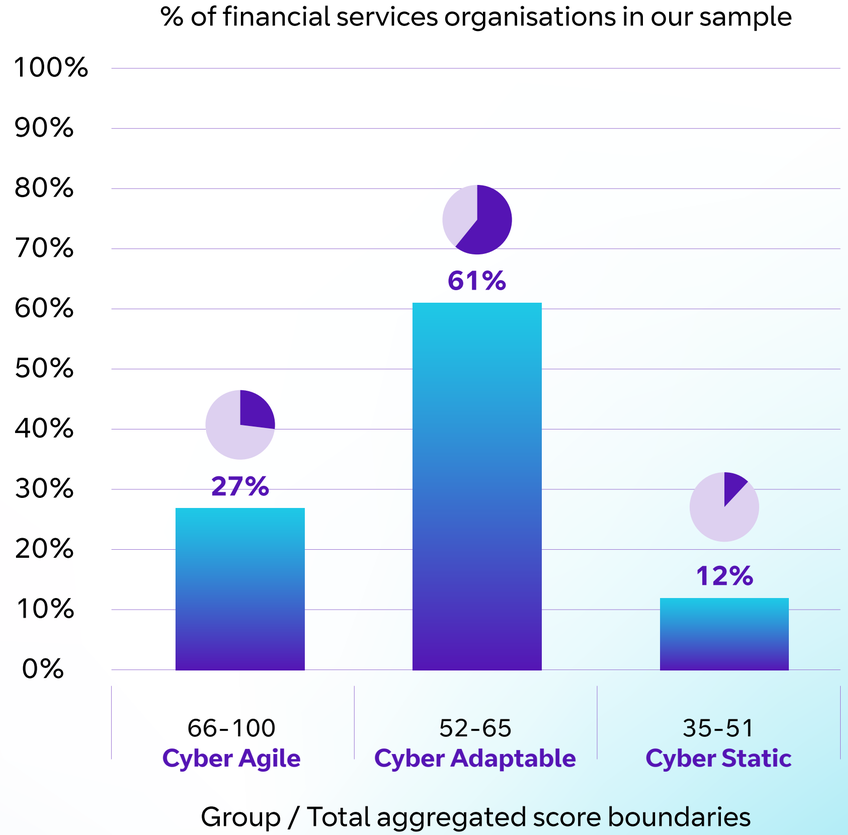
The cyber agility scoring system

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

Cyber crime is on the rise, with organisations in every industry reporting higher instances of attacks on their networks.

The financial services industry is far from immune: more than a third (**34%**) of financial services businesses involved in our study are experiencing 'high' or 'very high' cyber attack severity, with this rising to almost half of respondents in the sector (**47%**) expecting high or very high severity in the next three years.

34% of financial services businesses involved in our study are experiencing high cyber attack severity.

Cyber agility

Leveraging cyber security as a platform for innovation and growth

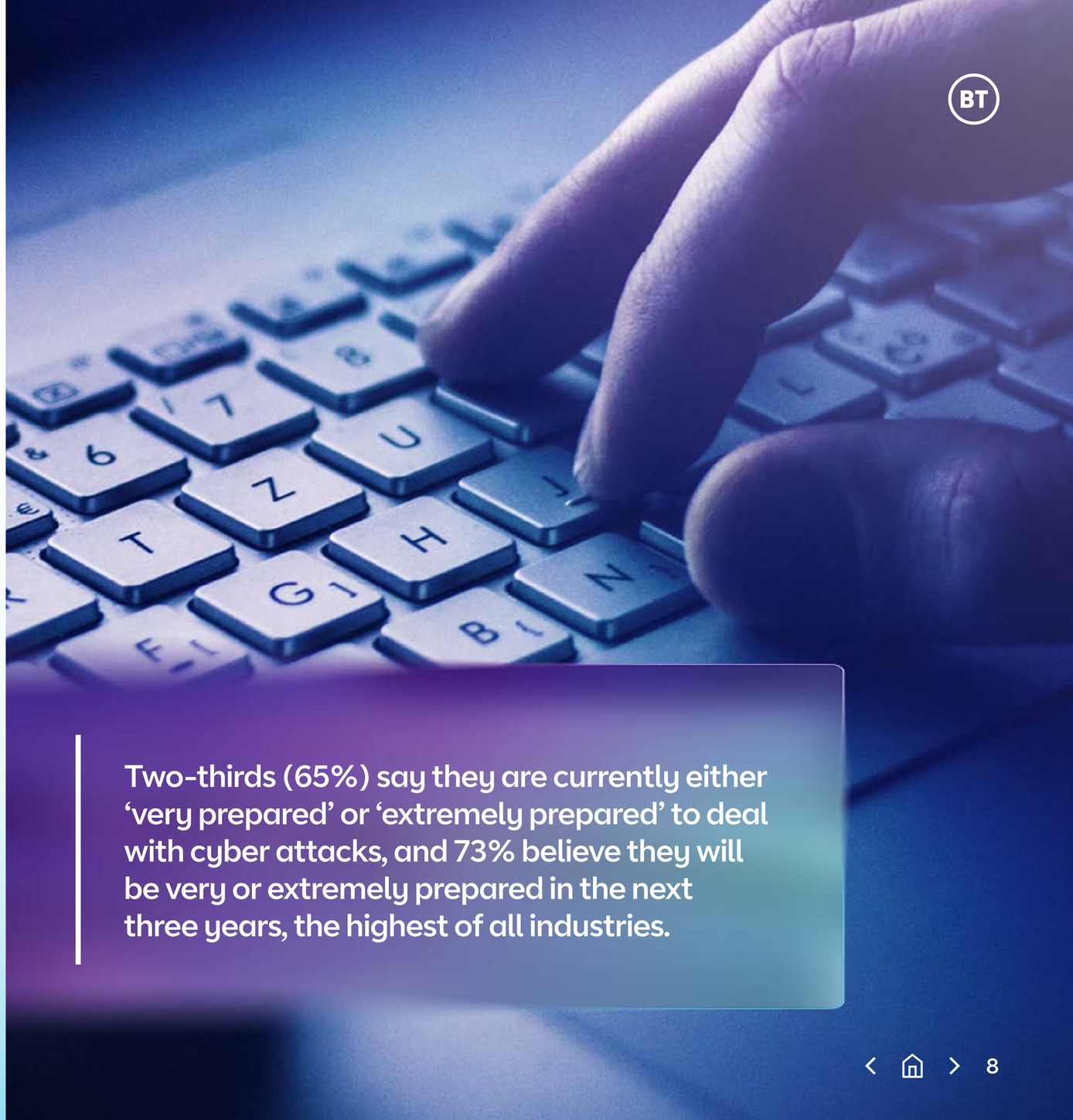
With so much malign activity happening around them, many financial services enterprises are concerned. More than six in 10 **(62%)** say that a major cyber attack is the main existential threat to their organisation.

62% say that a major cyber attack is the main existential threat to their organisation.

Prepared to protect

Financial services businesses are going to great lengths to insulate themselves from the maelstrom of destructive cyber activity.

At a fundamental level, **73%** of financial services businesses see a secure IT system as a prerequisite for doing business, and **82%** see this as essential to build trust with their stakeholders.



Two-thirds (65%) say they are currently either 'very prepared' or 'extremely prepared' to deal with cyber attacks, and 73% believe they will be very or extremely prepared in the next three years, the highest of all industries.

Cyber security self-assessment

Maturity level for financial services 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

40%

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

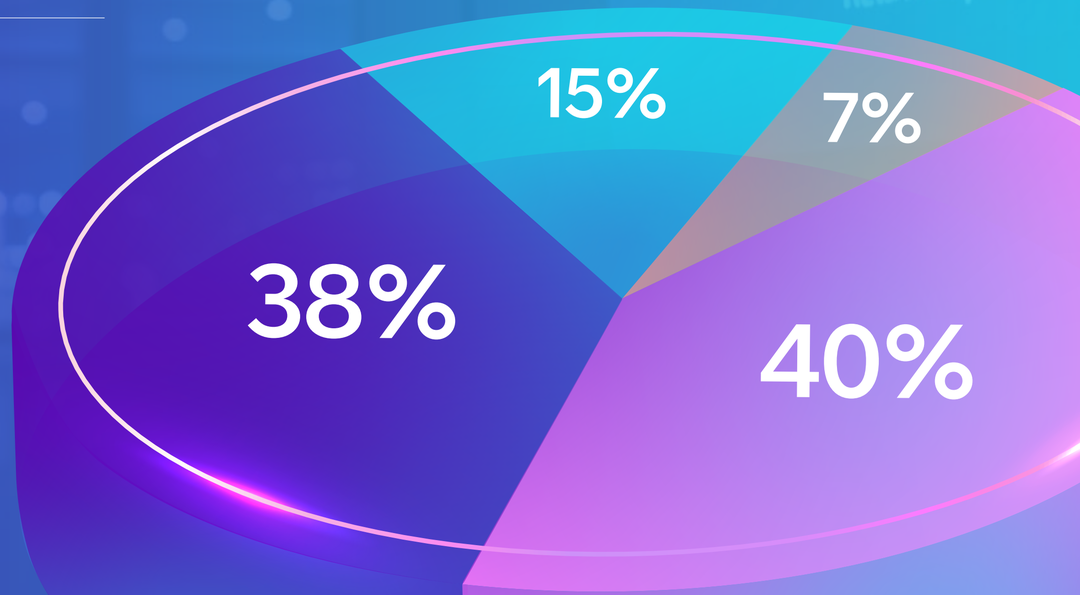
38%

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

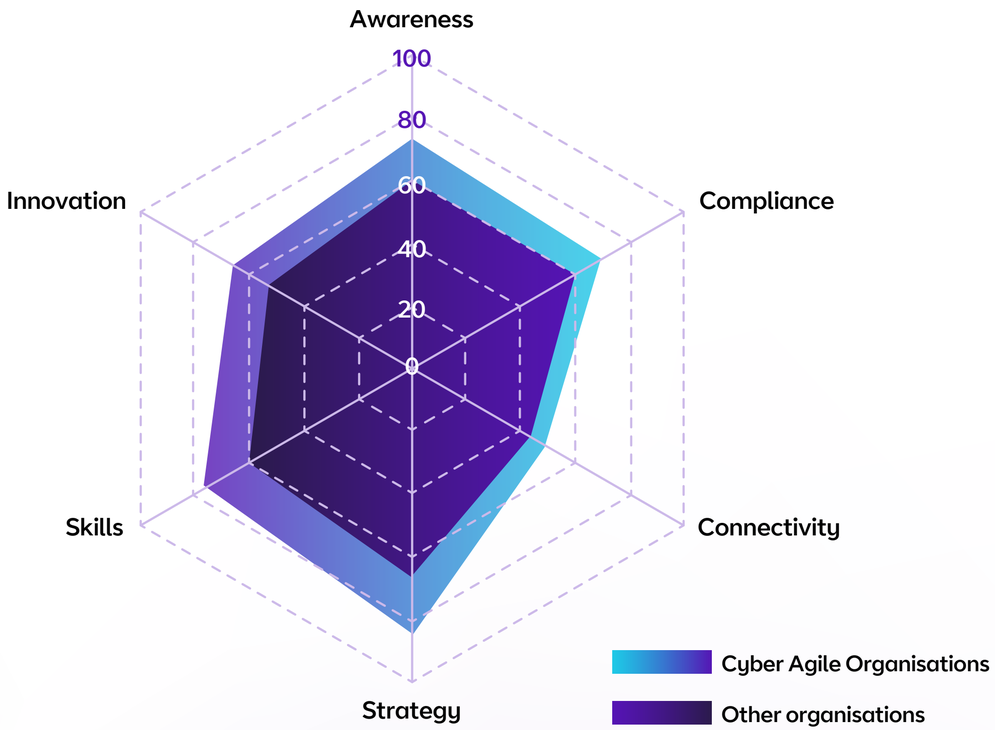
15%

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 financial services organisations.



Connectivity is a critical area of focus

The Connectivity dimension sees the lowest scores across all organisations, with only a small gap between Cyber Agile Organisations and others. As network infrastructure continuously evolves, leaders must focus on enhancing visibility and adapting safeguards to keep their ecosystems secure.

Readiness

Financial services companies' readiness to fend off threats was reinforced by the fact that more than a quarter (27%) of organisations qualify as Cyber Agile Organisations – the highest proportion for any sector in the study. However, significant gaps remain between sector leaders and their peers, particularly within the Awareness, Strategy and Skills dimensions – with the biggest divergence seen in Strategy.

Not only are Cyber Agile Organisations more secure and more confident about their readiness, but they are also experiencing a boost in metrics not traditionally associated with cyber security. Most notably, over the last three years, Cyber Agile Organisations in the financial services industry achieved **17% higher growth rates** than other organisations from the sector.

If all other businesses across the eight markets covered in this study matched this growth rate by improving their cyber agility, this could unlock an additional **£12 billion in revenue** and **£6 billion in gross value added (GVA)**[1] for financial services businesses and the wider economy[2].

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.

Learn more

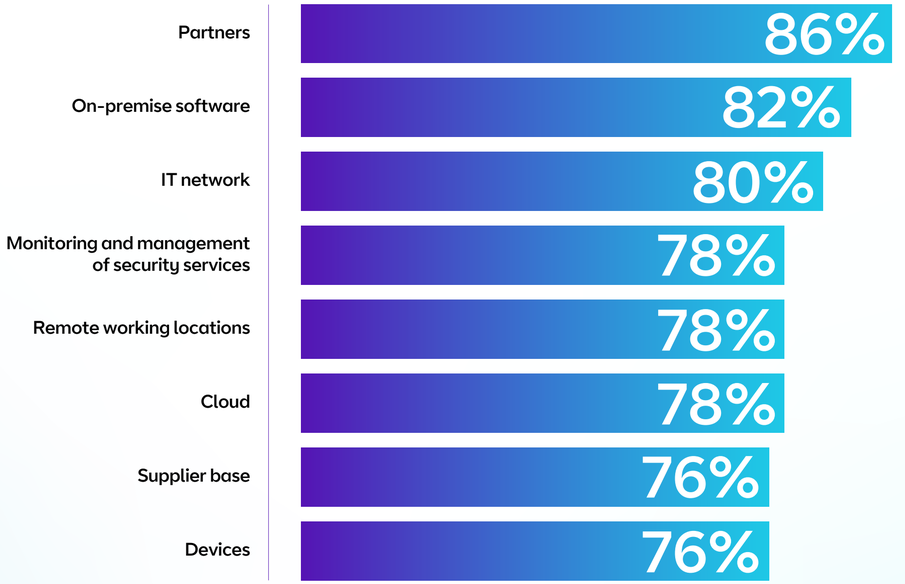
This financial boost could stem from the reported business-building effect of cyber agility. Financial services leaders recognise several significant benefits that improved cyber agility would bring to their organisations, the top five being:

"In an industry where the loyalty of customers is particularly prized and can be a key differentiator between rival enterprises, building and maintaining customer confidence and brand reputation are crucial. With this in mind, cyber security becomes more than just a defence mechanism – it is a cornerstone of trust and a catalyst for growth"

Lee Stephens, Director of Security Advisory Services, BT

US spotlight

US-based organisations are the top performing across four of the six dimensions of cyber agility: Awareness, Compliance, Strategy and Skills. However, they have one of lowest scores for the Innovation dimension. US-based finance organisations have a clear view of what's going on across their network.



Seven in 10 leaders in US-based finance organisations say their organisation is actively building a cyber security culture. And progress is strong: **62%** say every employee within their organisation knows they are responsible for IT security. **76%** of US finance leaders say their organisation will not work with suppliers that lack adequate security credentials.

The large majority of US finance leaders (**84%**) say IT transformation projects have increased their organisation's cyber security vulnerabilities. And **72%** say the explosion of generative AI and shadow AI in the workplace has made cyber security more important than ever.

Part 2

Becoming cyber agile: Key focus areas for financial services

According to our study, the majority of organisations in the financial services industry expect their cyber security budgets to increase by an average of **13%** by 2027. However, it's important that this additional investment is channelled into the right areas and used to ensure security becomes an enabler of growth.

Preparedness:
Securing connectivity

Both the rapid proliferation of devices – managed and unmanaged – and the increasing power of the apps they handle pose opportunities and threats for businesses in financial services.

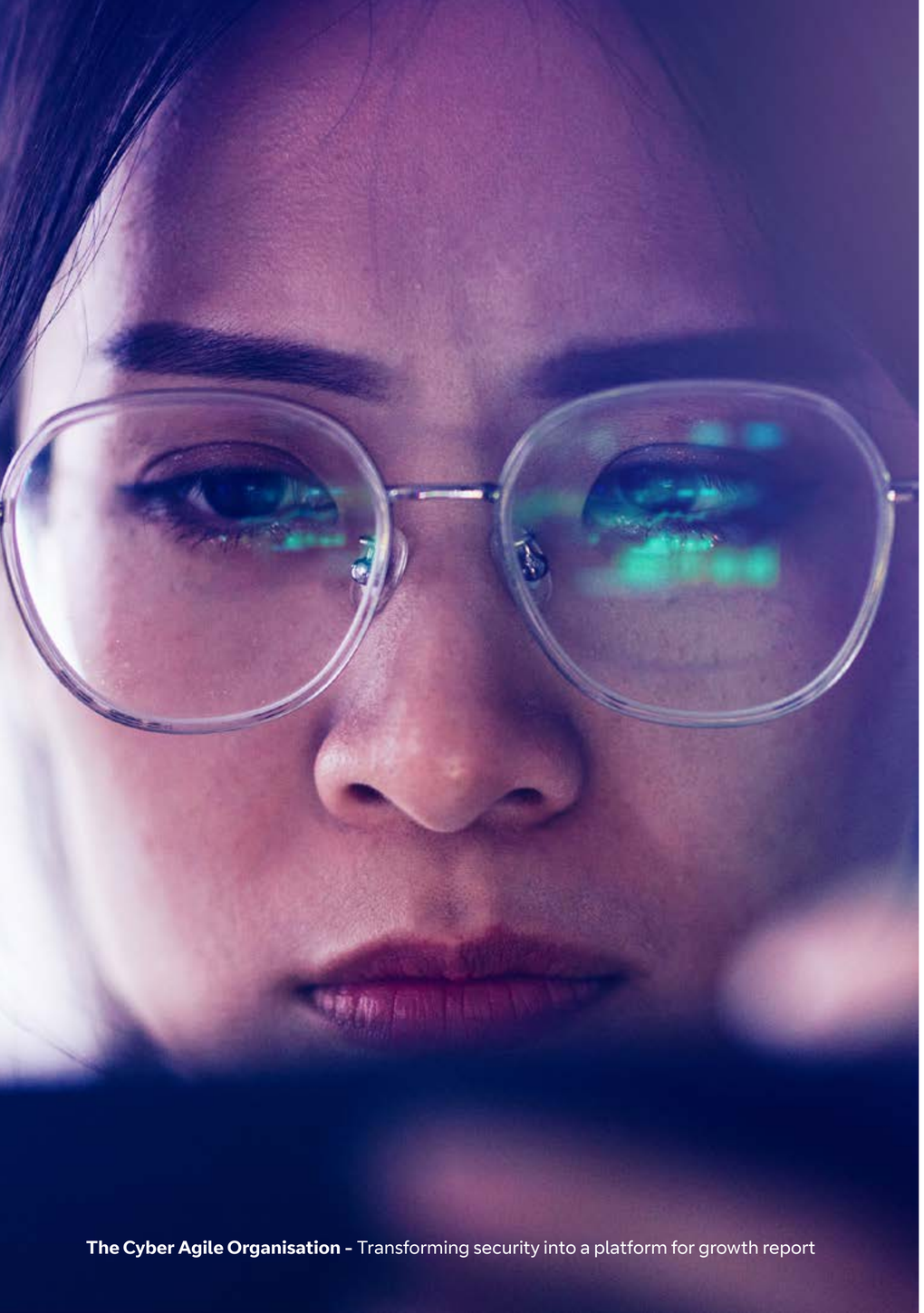
While added mobility and powerful digital tools help to strengthen product offerings and opportunities to collaborate, they also add new dimensions to the connectivity risk picture. So much so that leaders identify an increasing number of devices, use of public or insecure wireless networks and increased use of AI as the three most significant risks to their organisations' networks.

Increasing number of devices

Devices connecting to public wireless networks

Sanctioned use of personal devices

This could be a key reason why more than two-thirds (**67%**) of leaders in finance Cyber Agile Organisations say their organisation has high visibility of its IT infrastructure and network, and strong safeguards to keep them secure, compared to only **30%** of other organisations in the industry.



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

1

Have clear frameworks and visibility

Ensure comprehensive frameworks and visibility to monitor your entire IT infrastructure, including operational technology and unmanaged devices. For example, utilising AI to not only secure your business but also to secure your customer's data. It's important to regularly assess cyber security risks and implement robust safeguards to keep your network secure, now and in the future.

2

Securing your end users and data

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

Getting ready for DORA

The Digital Operational Resilience Act (DORA) will apply to financial sector organisations operating in Europe from January 2025. This will require organisations to achieve oversight of their IT ecosystem, identify security risks and prove that they can withstand, respond to and recover from all types of IT-related disruptions and threats. Guided by the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA), the UK's strategy puts emphasis on the financial system's resilience and capability to deal with operational disruptions, adapting to and dealing with threats.

Performance: Driving innovation

Being cyber secure is only half the equation of what makes an organisation cyber agile; the other half is using that stable platform to become a faster, more dynamic and responsive business capable of grabbing opportunities as they arise.

Some **81%** of Cyber Agile Organisations in the financial services industry believe that innovating their approach to cyber security makes them more innovative overall. This is reflected in everything from the use of new and agile technology to maintaining uptime and staying connected to keep innovation processes going. For example, Cyber Agile Organisations are more likely to say their incident resolution and recovery process is extremely useful in mitigating the impact of cyber security threats (32% versus 21%), ensuring quick recovery and minimal disruption.

Showing that paradigm-shifting innovation is a two-sided coin, **73%** of all financial services leaders say the explosion of GenAI and shadow AI in the workplace has made cyber security more important than ever, but a similar proportion (72%) have either fully or partially implemented AI or machine learning technology for threat detection.

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

1

Keeping ahead of rapid technology evolution

When it comes to digital transformation, waiting is not an option. You must act now, taking steps to mitigate future threats such as transitioning to quantum-resilient cryptography and embedding secure, ethical AI frameworks into your operations. By taking a forward-thinking approach, you can be ready to address these challenges, using innovation to strengthen, not undermine, your security posture.

2

Securing your multi-cloud

A cloud-centric environment offers significant opportunities for scalability, cost efficiency and personalisation, but it also calls for a robust cyber security posture. Distributed cloud services need strict access controls, system isolation, and active network monitoring. By embedding these capabilities into your wider transformation strategies, you can unlock the potential of the cloud while ensuring that transformation efforts are secure, compliant and future-ready.

3

Invest in your skills strategy

As technology and complexity evolve, it is essential to stay ahead of potential threats by investing in your employees and their development. Skills strategies should focus on reskilling and upskilling, promoting diversity in recruitment, and outsourcing niche skills. As a financial services business, you must be capable of securing both current and emerging technologies. Implementing a continuous training program will help you to achieve this goal.

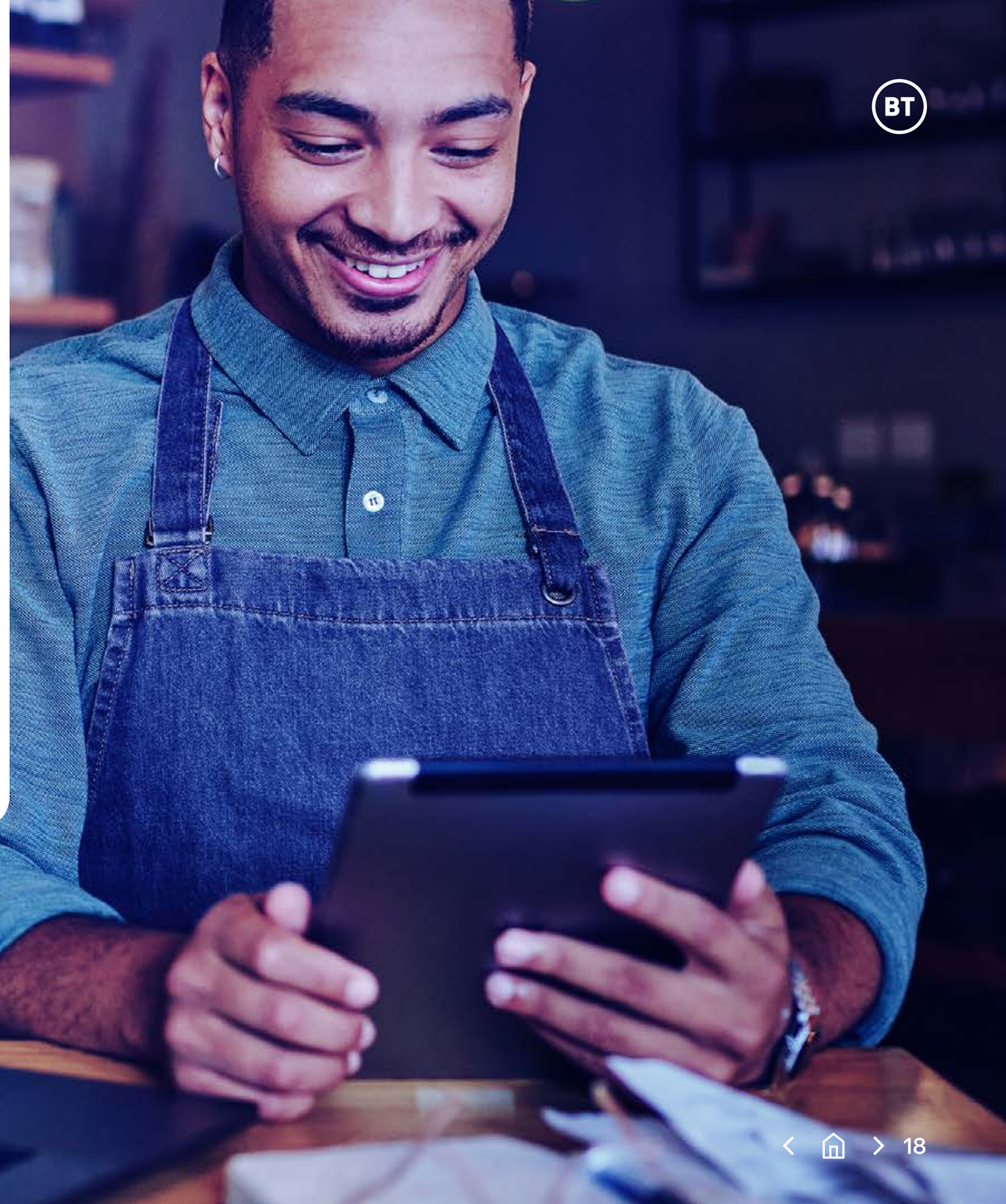
Conclusion

Cyber security has developed from its origins as a pureplay defensive tool to become a vital strategic asset for businesses wanting to grow without fear or constraint. This is perhaps better understood in the financial services industry – where reputations are built on keeping financial data safe – than in any other sector.

It's not surprising, then, that this sector has a high proportion of Cyber Agile Organisations compared to other industries – businesses prepared to safeguard themselves from cyber threats and leverage security measures to enhance wider business performance.

They understand that security is a business issue, not just a technology challenge or a problem to leave at the door of the IT team. Everyone should be involved in keeping the organisation secure – and everyone should reap the benefits of that security.

Customer trust, greater efficiency, improved reputation and more opportunities for collaboration are just a few of the advantages of becoming cyber agile. Cyber Agile Organisations have a better opportunity to do all this and more, while those in the chasing pack have some catching up to do.



BT's got your back

We're at the heart of financial services

For over 50 years, we've collaborated with financial regulators to shape policy and make sure our solutions deliver risk and compliance outcomes that are fair, explainable and auditable. This commitment has earned the trust of 78 of the world's top 100 banks, as we work alongside them to deliver bespoke solutions in an ever-shifting operational landscape.

We're global security specialists

Our experience in protecting critical entities – from governments to large corporations – from cyber attacks gives us a unique vantage point on evolving threats. Drawing on the expertise of our 3,000 security professionals, 350 highly-skilled consultants and our global security operations centre, we use quantum-safe networking services to help organisations detect and respond to threats in a Zero Trust world.

We have a renowned global network

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

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 and Security Operations Centre 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.

BT Means Business

Get the conversation started

Talk to us

Offices Worldwide

JN: 1634561879