Help your business address the Cyber Ready challenge

Executive Summary

Highlighting the findings of Vodafone's 2018 Cyber Ready Barometer research and three key lessons.

The future is exciting.

Ready?

vodafone

Download the full report

The cyber security landscape is continually shifting. The scale, frequency and variety of cyberattacks continue to grow, as hackers become increasingly sophisticated.

Privacy has taken equal billing alongside cyber breaches in the news agenda. The ethics and business models of the likes of Facebook and Google are being questioned, further thrusting data privacy and security into the spotlight. GDPR legislation has left businesses scrambling to comply and consumers bemused by a barrage of re-consent emailers. All of this can have a direct impact on a businesses' reputation.

Traditionally, cyber security has been a defensive strategy, building walls against known vulnerabilities and using forensic technology to clean up and fix weaknesses in the wake of breaches. Investment in cyber security was considered a necessary evil to secure your business. But this attitude is changing. The findings of our **2018 Cyber Security Barometer report** show a clear link between strong cyber security and greater business success, countering the generally accepted narrative.

Investigating Cyber Readiness worldwide

Our 2017 research report **Cyber Security: The Innovation Accelerator** uncovered that businesses with a more proactive stance on cyber security investment expected greater financial benefits, more customer loyalty and competitive advantage. In the Cyber Ready Barometer 2018, we set out to corroborate this link, questioning decision makers to see whether they have realised the business benefits they predicted.

Ultimately, we wanted to better investigate this supposed advantage enjoyed by the most 'Cyber Ready' businesses, those who acknowledge the evolving threats they face but equip themselves to survive and thrive. We're excited to share some stunning insights into the evolution of cyber attitudes, and how winning organisations are harnessing cyber security to drive growth, trust, and ultimately revenue.

When considering cyber readiness and resilience, the people within a business are one of the most decisive factors in determining how secure you are – good practice is a huge advantage, but poor behaviour can create major risks. But how sure can you be of their attitudes and approach to security? We surveyed employees to find out their thoughts about their employers' security, and also reached out to consumers to discover the impact of cyber security on their purchasing preferences. Speaking to decision makers, employees and consumers offered a unique chance to compare and contrast attitudes and gain a rounded perspective of cyber security posture.

The Cyber Ready Barometer is designed to give you food for thought to assess and test your own internal readiness; highlighting areas to focus your resources and investment on. Are your employees confident in your security measures or do they feel it's hampering them and look for workarounds? Is your training really sinking in or could more be done to engage staff? How sensitive to cyber readiness are your partners, clients and citizens? Is your business perceived as a secure supplier?

We hope this report prompts all organisations – large and small – as well as individuals and their families to ask themselves "How Cyber Ready am I?" The full report can be found **here**. We look forward to working together to help businesses and people become ever more Cyber Ready in the months and years ahead.

The Vodafone Cyber Ready Barometer 2018

Get the full report

This paper is just a snapshot of the barometer's findings. **Download the full report now**

Download the full report

Introducing the Cyber Ready Barometer

We questioned **4,809** IT and security decision makers, employees and consumers to assess their attitudes to, opinions of and knowledge about cyber security and specifically cyber readiness.

From this, we created the Cyber Ready Barometer. The Barometer indexes businesses by assessing them across six criteria contributing to readiness levels and assigns an overall readiness score out of **100**. This score is then used to categorise each respondent's level of Cyber Readiness which can be **Basic**, **Reactive**, **Developing**, **Proactive** or **Advanced** **–** with the latter two being classed as **Cyber Ready** (See page 8 'Calculating the Cyber Ready Index' for more detail.).

We define a Cyber Ready business as one that is effectively prepared for the challenges and opportunities of cyber security – able to bounce back quickly from a breach and embrace disruption and change with confidence due to their secure foundations.

What we discovered

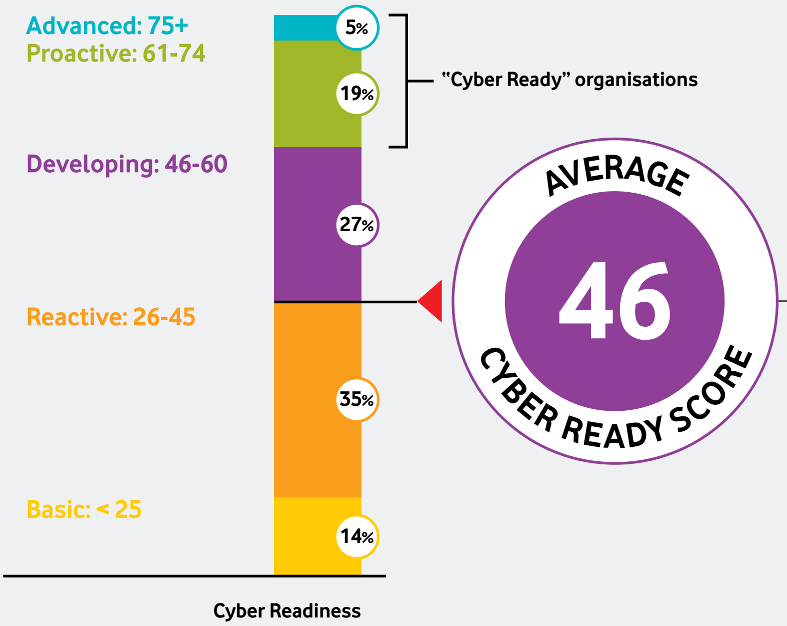
Few businesses are truly Cyber Ready and many are not adequately addressing cyber concerns.

Across all respondents, only **24%** can be classified as Cyber Ready today. The average Cyber Ready Index rating across all businesses, verticals and countries was **46**/100. Smaller businesses were the least ready, with **20%** demonstrating the lowest level of readiness Basic.

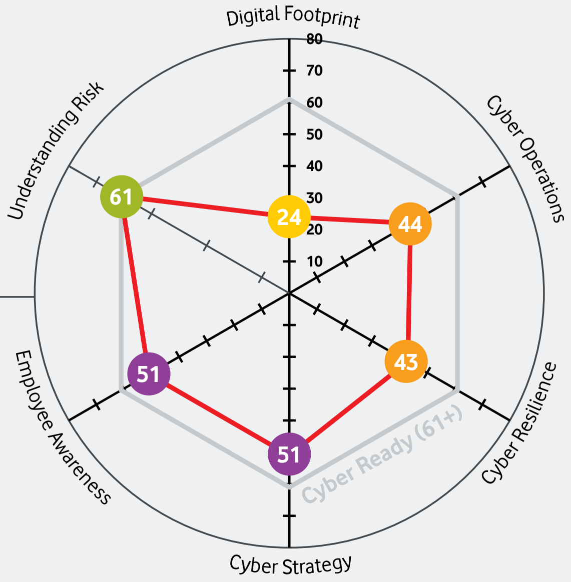
Cyber complexity is also creating confusion and uncertainty around who can help and where responsibilities lie. **46%** of businesses agreed they are unsure of who can help with information security challenges.

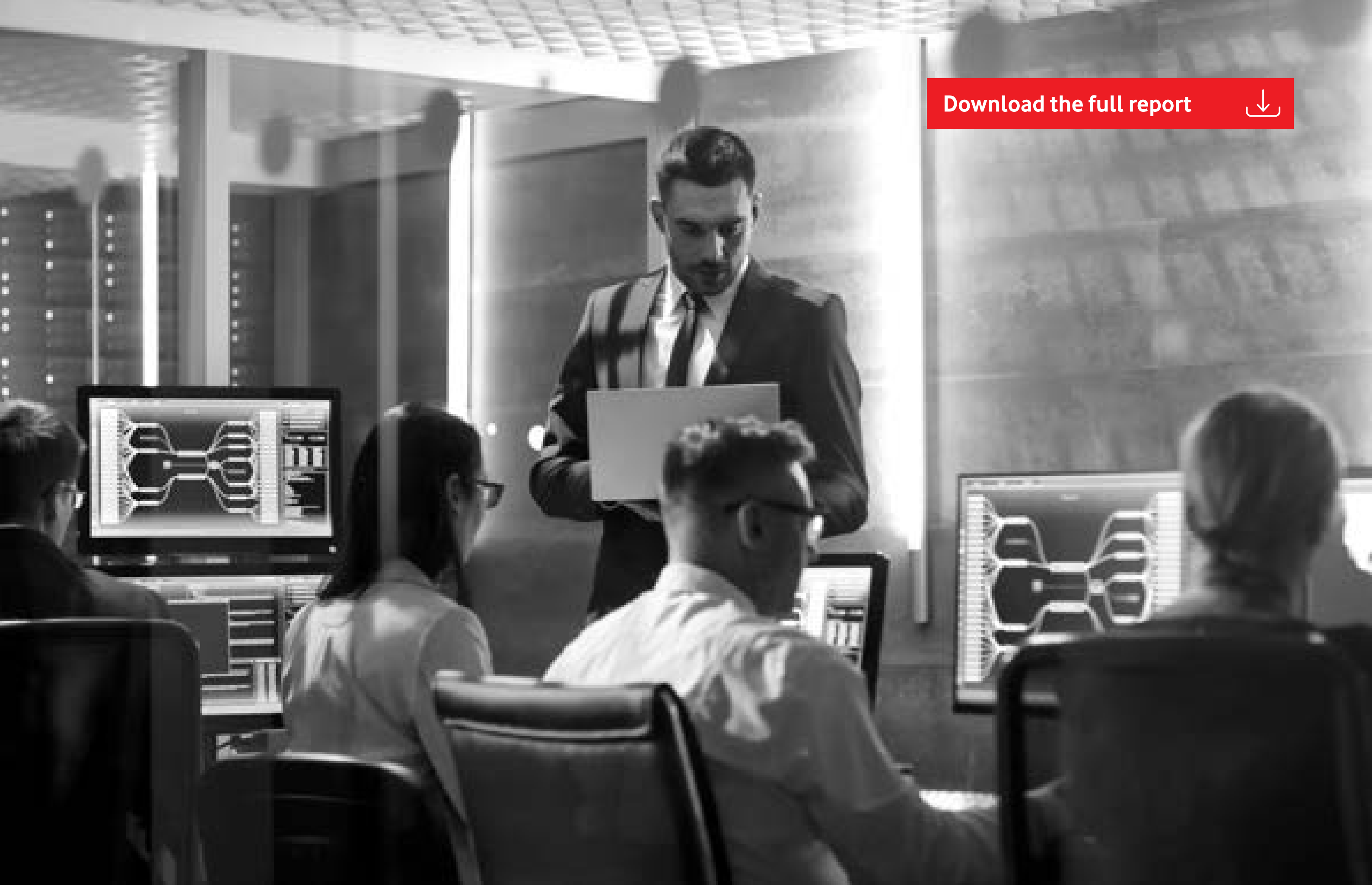
Overall though, **27%** of all businesses were classified as having Developing readiness. This shows that the security message is getting through, the right measures are starting to be put in place and with some focused efforts to improve, businesses can quite quickly progress and become Cyber Ready.

The breakdown of all businesses levels of Cyber Readiness



How did the average business score against the Cyber Ready criteria?





An evolving digital footprint and growing number of security threats are putting businesses under pressure.

50% of all business have only Basic readiness when it comes to having a clear overview of their Digital Footprint (including all the devices and potential access points to their IT environment) – only **3%** are Cyber Ready in this aspect. In fact, understanding of their Digital Footprint has consistently proved to be an area of concern across all business sizes, regions and verticals.

New security challenges are stemming from increased adoption of technologies such as cloud services (**83%**), IoT devices (**48%**) and more remote working (**46%**). However only **29%** of business decision makers feel their organisation is ready for the future. A **fifth** have no financial contingencies in place and lack the ability to identify complex incidents quickly.

The rise in security threats is a key driver of investment but **almost half** of businesses are investing to minimise risks to their reputation, influenced by the continual string of high-profile security stories in the media.

There are divergent opinions between business decision makers and employees on security and risk.

Businesses are confident that employee security policies are updated and communicated efficiently and training is delivered regularly. However, while businesses are bullish about having put policies and training in place, the effectiveness of their communication with employees may not be as robust as assumed.

Less than half of employees reported that official policy or process is followed by all staff, while **39%** view cyber security as a "box ticking" exercise that hinders their efficiency. Only **52%** regularly receive specific security training.

The inability to accurately assess how many employees work remotely or use their own devices for work purposes creates potential risk – **63%** of employees admitted using their personal smartphones for work, while only **43%** of business decision makers stated that they allow BYOD. This points to a crucial mismatch between IT's perception of working practices and the employee-reported reality.

Download the full report

The more Cyber Ready the business, the better the business outcomes

There's a notable correlation between Cyber Readiness and business performance. This relationship accelerates as businesses move up the Readiness Index with those classified as Advanced experiencing a marked positive impact on stakeholder trust and business performance. **58%** of Advanced businesses reported an annual revenue increase of more than 5% last year, compared with only **22%** of Basic organisations.

These Advanced companies that have baked security into their values, products, services and messaging are capturing market share. The solid foundations required for strong cyber security, readiness and resilience create a high level of confidence throughout the business. For example, two-thirds of Advanced businesses were bullish about their ability to become 'more customer-centric'.

The tangible link between being more Cyber Ready, improved performance and competitive advantage can enable organisations to make a clear business case - investing in security considerations and initiatives with clear financial consequences.

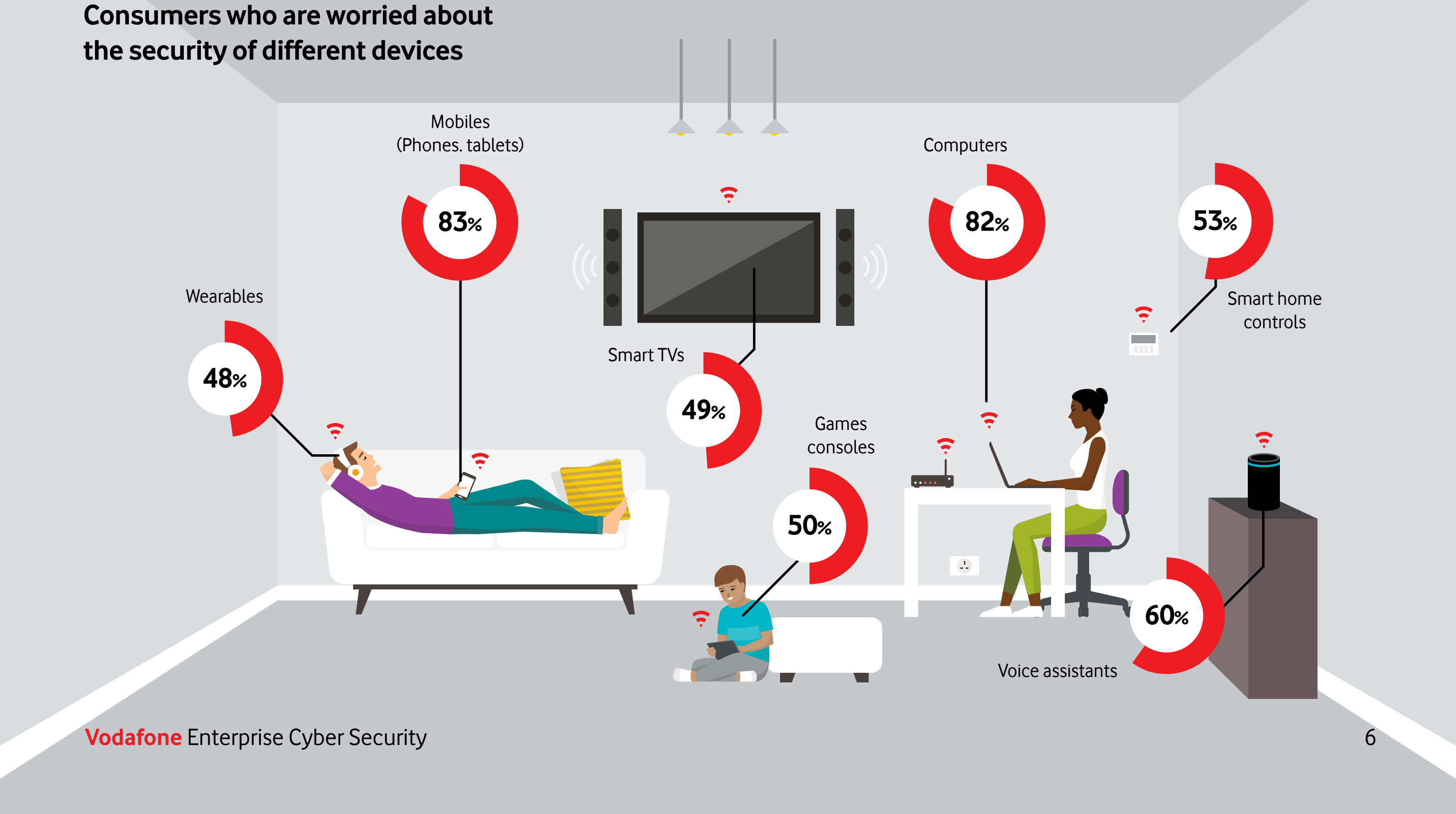
Worried consumers will pay a premium for peace of mind – but businesses have been slow to react.

Consumers understand the severity of the threats facing them and increasingly look to services providers for protection. The average consumer home now has **9** different connected devices and **11** different online services. Newer devices are bringing fresh security fears for already concerned consumers, with **60%** worried about their voice assistants and **53%** about smart home controls.

Crucially, almost **two-thirds** of people are willing to pay a premium for a higher level of security. Yet only **29%** of businesses believe that they can charge higher prices for their products and services due to the increased peace of mind of doing business with them.

Cyber Ready companies should draw on their reputation to differentiate from their competitors and tap into the security conscious consumer market. Those who fail to address their customers' concerns risk losing customers and an increased churn rate.

Consumers who are worried about the security of different devices



Three steps to becoming Cyber Ready

This report identifies that the majority of businesses today are not fully equipped to tackle the evolving cyber threats and embrace the rapidly changing digital world. However, the clear correlation between Cyber Readiness and competitive advantage creates a strong business case and motivation for business to focus on becoming more Cyber Ready. Here are four areas of focus for businesses looking to become Cyber Ready.

1. Resilience is key and must be improved

In today's climate, a business will now be judged on its ability to withstand multiple and ongoing cyberattacks, while continuing business operations. It's important not just to focus on preventing attacks, but also to consider whether you have the skills, technology, processes and know-how to bounce back quickly and mitigate the impact of a breach or incident.

2. Get a handle on your digital footprint

The explosive growth of both business and consumer digital footprints, the rapid adoption of newer technologies like cloud and IoT and the evolution of working patterns and practices has left businesses struggling to maintain visibility and control.

3. Don't underestimate the importance of your people and try to understand all perspectives

Although the importance of cyber security is well understood by business leaders and employees alike, the actual practice of communicating security policy and following best practice is better in theory than reality. Businesses need to engage their employees and align their security priorities with how the organisation operates.

Ultimately, businesses want to deal with other companies offering assured security, and consumers are willing to pay a premium to ease their security worries. The most Cyber Ready companies need to explore these opportunities and better monetise their investment in security.

Get the full report

This paper is just a snapshot of the barometer's findings. **Download the full report now**

Download the full report

Calculating the Cyber Ready Index

The Cyber Ready Index creates a statistical measure of Cyber Readiness. It is calculated by the following method:

1. We identified and measured six distinct criteria which relate to how Cyber Ready a business is.

2. All respondents were assigned a score out of 100 against each criteria, based on a number of relevant variables from the research data

The average score is calculated across six criteria:

The Six Cyber Ready criteria

Digital Footprint

The 'gap' between employer and employee perception of Digital Footprint. Awareness of mobile working and BYOD.

Cyber Operations

Confidence in the ability to secure sensitive, personal data, in the cloud or on mobiles. The level of investment in IT security.

Cyber Resilience

The relevance of security policies. The company's ability to identify, contain and recover/learn from an attack.

Cyber Strategy

Support from senior management. How well the business understands that security can be a differentiator in the eyes of customers.

Employee Awareness

Company plans and policies that address the behaviour and actions and training of employees.

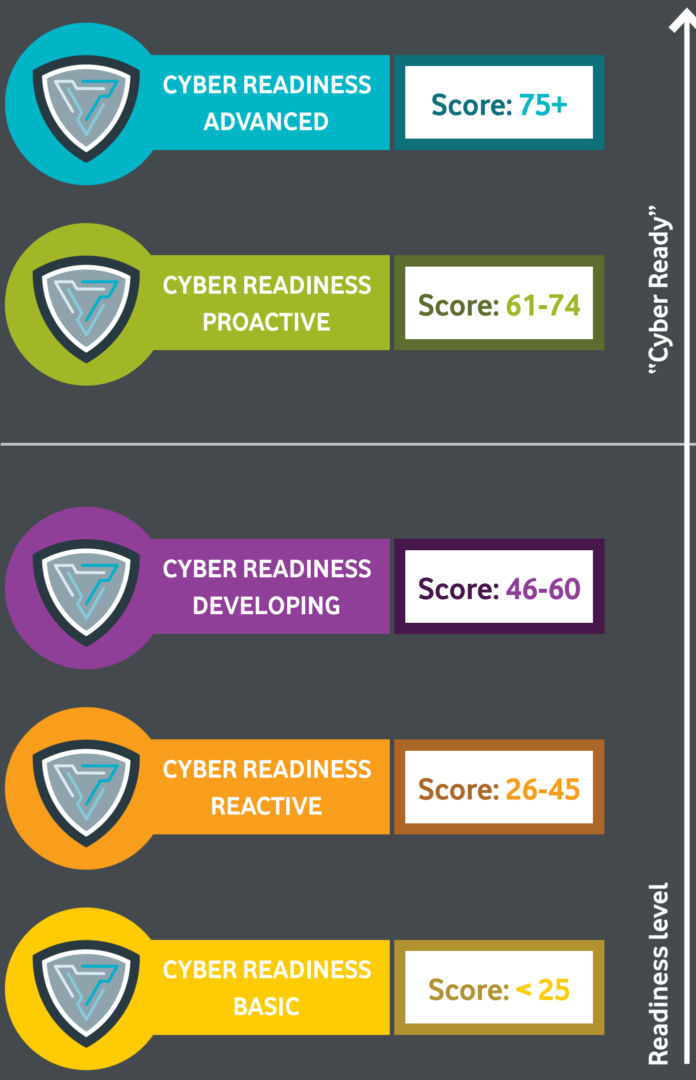
Understanding Risk

Awareness of security issues in the company, especially regarding new initiatives or partners.

Download the full report ⤓

The five Cyber Ready levels

Based on a score out of 100, we've classified five levels of Cyber Readiness. **We have defined a 'Cyber Ready' business as one scoring 61+**



“Cyber Ready”

Readiness level

CYBER READINESS ADVANCED	Score: 75+
CYBER READINESS PROACTIVE	Score: 61-74
CYBER READINESS DEVELOPING	Score: 46-60
CYBER READINESS REACTIVE	Score: 26-45
CYBER READINESS BASIC	Score: < 25

Cyber Ready: ADVANCED ✓

The leading subset of Cyber Ready companies - this group of businesses are leading the way in their approach to cyber security, readiness and resilience - and reaping the rewards.

Cyber Ready: PROACTIVE ✓

This group of businesses are Cyber Ready today, gaining a competitive advantage on their less ready competitors, but there is still potential for further improvement.

DEVELOPING

This group of businesses have shown they have achieved a good level of readiness across several areas, but still have gaps and threats to address if they are to become a truly Cyber Ready business.

REACTIVE

This group of businesses have taken some action to secure their business, but are generally on the back foot when it comes to cyber security. They have significant scope for improvement across the board.

BASIC

This group is lagging behind the rest, whether due to a lack of budget, skills or awareness, and it is leaving them at significant risk and at a distinct competitive disadvantage.

Discover more insight into the nature of Cyber Readiness and how it can potentially help your business differentiate from the competition in the Vodafone Cyber Ready Barometer research report. ⤓

www.vodafone.com/business/cyber-security **cybersecurity@vodafone.com** **+44-1635-813615**