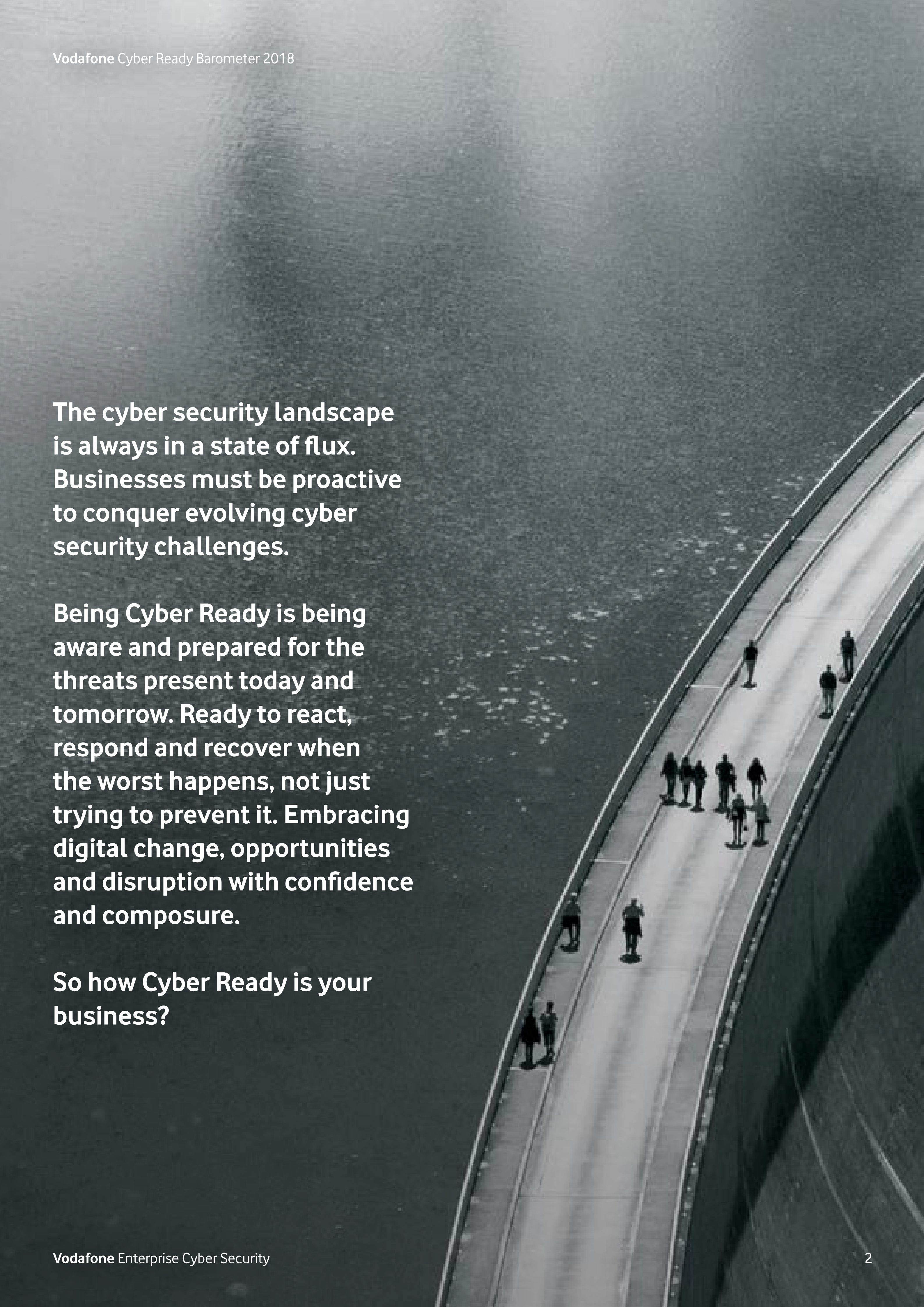
The Vodafone Cyber Ready Barometer 2018

A detailed investigation into levels of Cyber Security and Readiness in businesses around the world, including the relationship between security and success.

The future is exciting.

Ready?

vodafone



The cyber security landscape is always in a state of flux. Businesses must be proactive to conquer evolving cyber security challenges.

Being Cyber Ready is being aware and prepared for the threats present today and tomorrow. Ready to react, respond and recover when the worst happens, not just trying to prevent it. Embracing digital change, opportunities and disruption with confidence and composure.

So how Cyber Ready is your business?

Introducing the Vodafone Cyber Ready Barometer

Vodafone's series of Barometer research reports take an in-depth measurement of some of the most significant changes and trends affecting the business technology landscape and the impacts they are having on you.

Based on the findings of our primary research, the Vodafone Cyber Ready Barometer report investigates how Cyber Ready businesses really are in 2018 and the relationship between readiness and business performance.

What will you learn from this report?

The research explores the trends and changes in attitudes across the cyber landscape over the last year and scores businesses on the Cyber Ready Index.

Source:
Oxford Dictionary

barometer
/bar-om'et-[.e]r/   noun

1. An instrument measuring atmospheric pressure
2. Something which reflects changes in circumstances or opinions

Find out...

How the levels and maturity of Cyber Readiness vary between different businesses – but there are some persistent overarching trends across country, size and sector

Learn...

How being Cyber Ready helps you succeed – the readiest companies are already gaining a competitive advantage through improving cyber security

Discover...

How contrasting attitudes between large and small businesses, their employees, and the consumers who buy their services, highlight some significant opportunities that are being missed.

In 2018 cyber security has reached a tipping point. Cybercrime is big business, the annual cost has rocketed to $600 billion worldwide*, overtaking the global drugs trade.

The scale, frequency and variety of cyberattacks has continued unabated from 2017, as hackers grow increasingly sophisticated. New technologies, such as blockchain, have the potential to disrupt markets. Privacy has taken equal billing alongside cyber breaches. The ethics and business models of the likes of Facebook and Google are being questioned, as data privacy and data security are thrust into the spotlight. GDPR legislation has left businesses scrambling to comply and consumers bemused by a barrage of re-consent emailers. All of this impacts directly on a business's reputation.

Traditionally, cyber security has been thought of as a defensive strategy. Building walls against known vulnerabilities to prevent future attacks and using forensic technology to clean up in the wake of breaches. Investment in cyber security was viewed as a necessary evil in the digital age. But our 2017 research report, **Cyber Security: The Innovation Accelerator**, uncovered a clear link between organisations with strong cyber security and greater business success. This countered the generally accepted narrative.

In fact, those businesses who took a proactive approach to cyber security predicted financial benefits, greater customer loyalty and competitive advantage. We felt that this demanded investigation, so in 2018 we set out to question decision makers to see whether they realised those benefits and to corroborate this link between cyber and business success. People are one of the most decisive factors in strong cyber security – but how much do we really know about their attitudes and approach to security? We surveyed employees within businesses of all sizes to find out more about their perceptions of security. To gain a fully rounded perspective, we also reached out to consumers to ask about their attitudes to cyber security and its effect on their buying preferences.

Ultimately we aimed to discover if the most 'Cyber Ready' businesses, those who acknowledge the evolving threats faced but take proactive measures, are really seeing a business advantage over the cyber laggards. The Cyber Ready Barometer has taken a pressure reading on the level of cyber readiness in the market. We're excited to share some stunning insights and highlight not only the evolution of cyber attitudes, but also how winning organisations are harnessing cyber security to drive growth and trust. We would like all organisations – large and small – plus individuals and their families to ask themselves "How Cyber Ready am I?"

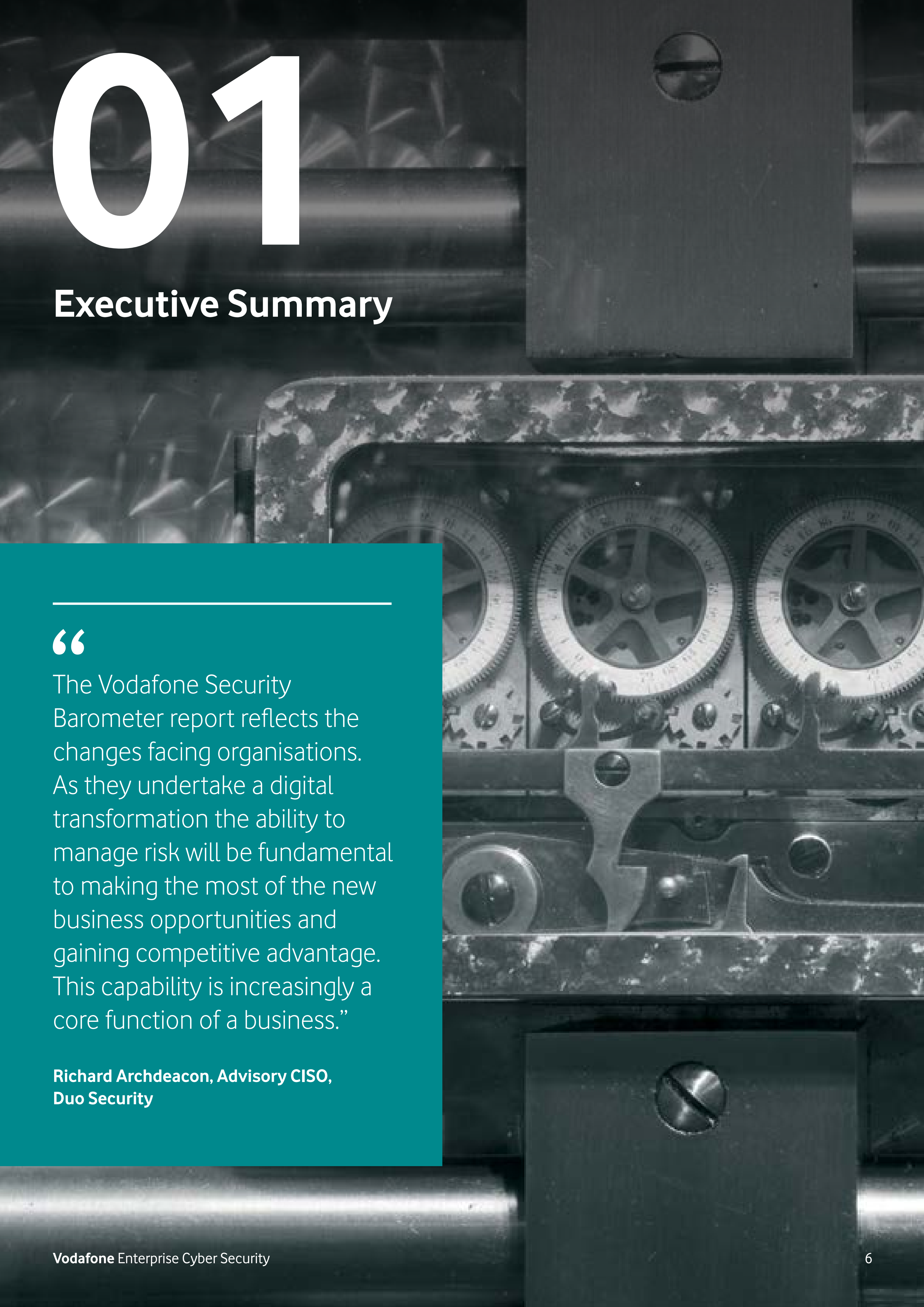
Thank you for reading our report. We look forward to working together to help businesses and people become ever more Cyber Ready.

Maureen Kaplan
Vodafone Enterprise Cyber Security Lead

* Source: McAfee with the Center for Strategic and International Studies Report, 2018

Contents

If you have any questions about these findings - or how you can increase your own Cyber Ready initiative, please contact us at: **cybersecurity@vodafone.com**



01

Executive Summary

> “The Vodafone Security Barometer report reflects the changes facing organisations. As they undertake a digital transformation the ability to manage risk will be fundamental to making the most of the new business opportunities and gaining competitive advantage. This capability is increasingly a core function of a business.”

Richard Archdeacon, Advisory CISO,
Duo Security

1. Executive summary

Becoming more Cyber Ready in the face of the shifting cyber security landscape and widespread digital transformation is increasingly essential for all businesses.

The objective of this research was to assess the levels of security readiness and resilience across businesses worldwide, gain an understanding of the factors that contribute towards being Cyber Ready and how it affects business success.

To achieve this, we created the Cyber Ready Index. The Index assesses businesses 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 as **Basic**, **Reactive**, **Developing**, **Proactive** or **Advanced** – with the latter two being classed as **Cyber Ready**.

We investigated the contrasting perspectives between business decision makers, employees and consumers and the extent to which a business's success and its ability to innovate is affected by its Cyber Readiness.

We also compared the data against our 2017 research findings - Cyber Security: The Innovation Accelerator - to assess how trends are developing year-on-year.

Here are five key findings.

A word on our contributors...

We have worked closely with a number of industry experts from a range of organisations and functions to provide their valued additional perspective on the research findings in this report.

Many thanks to all of our contributors:

Ovum

RUSI www.rusi.org

Huntsman®

DUO

BAE SYSTEMS

iisp

NEXOR®

University of BRISTOL

#1

Few businesses are truly cyber ready and many are not adequately addressing cyber concerns

Only a quarter of businesses are classed as Cyber Ready. On average, businesses achieved a score of just **46**/100 on our Cyber Ready Index. Smaller businesses (with less than 100 employees) were the least ready, scoring **42**/100, with **20%** demonstrating the lowest level of readiness 'Basic'.

Overall, businesses ability to understand security risks rated highly. 'Understanding Risk' is one of the six criteria of the Cyber Ready Index, it evaluates a business's security confidence, consideration, awareness and skills. Encouragingly **34%** of all businesses achieved the highest readiness level 'Advanced' here.

Despite this, confusion about who can help handle security challenges is actually increasing. 46% of businesses agreed that they are unsure of who can help with information security challenges – up 5% in the year since our 2017 research.

Understanding their potential Digital Footprint is a struggle for most businesses. 50% of all businesses demonstrating low readiness when assessing of the 'gap' between the IT and employee view of use of technology and working practices within the business.

#2

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

The digital footprints for both businesses and consumers are increasing in size and complexity. Increasing adoption of new technologies such as cloud services (**83%**), IoT devices (**48%**) and growing numbers of remote workers (**46%**) is creating new business security challenges. The average consumer home now currently uses **9** different connected devices and **11** different online services. Newer devices are proliferating and bringing fresh security concerns for consumers, with **60%** worried about their voice assistants and **53%** about smart home controls.

Businesses are spending more of their IT budget on security. 55% stated that the increase in security threats was driving greater investment in information security, **43%** felt that minimising risks to their reputation was the key driver, while greater adoption of cloud (**43%**) and IoT (**34%**) technologies are also factors.

Despite greater investment, business confidence in the face of these security challenges is low. Only **29%** of business decision makers feel their organisation is ready for the future. Only **43%** of respondents surveyed in April 2018 say they are both aware of and have taken measure to comply with GDPR.

#3

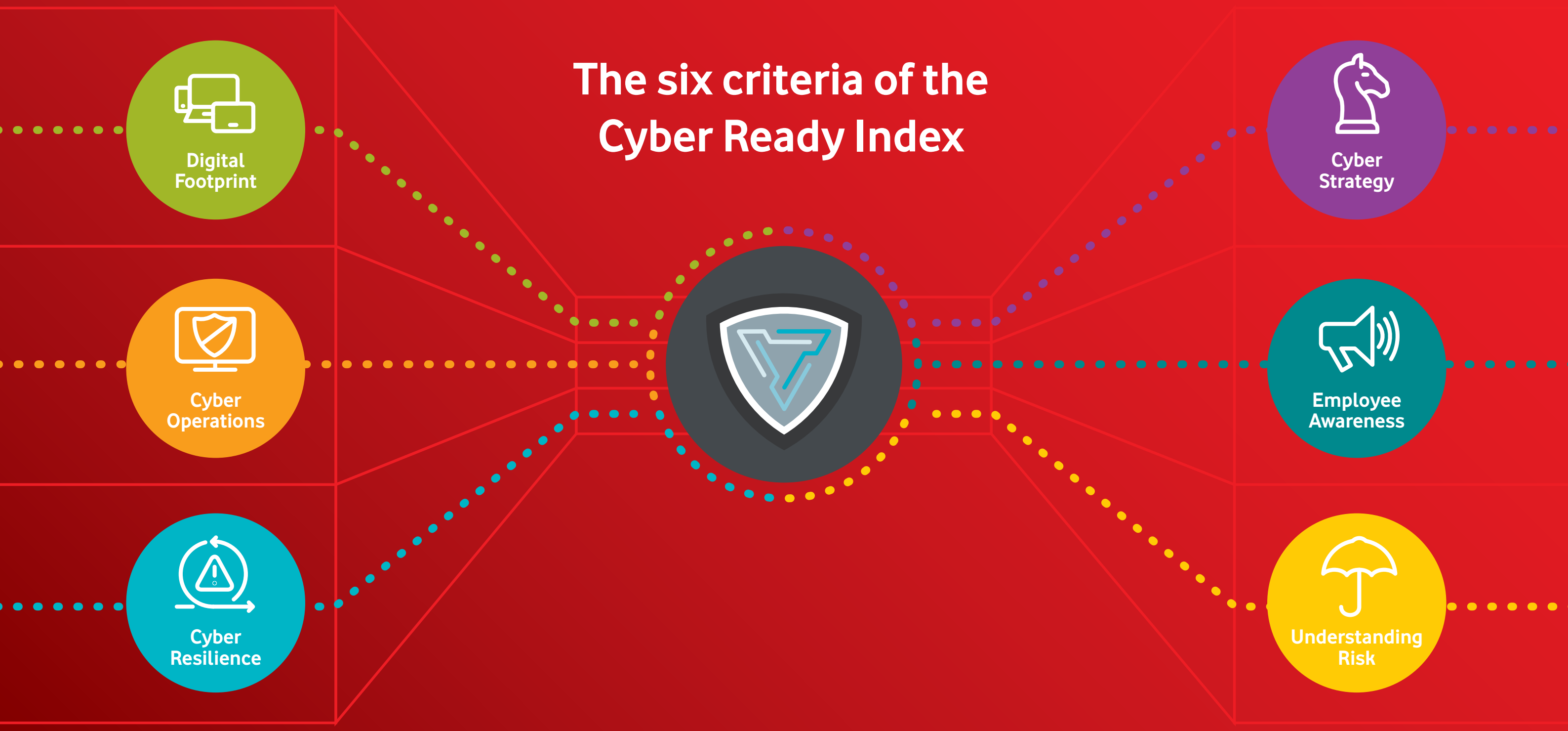
There are divergent security behaviours between business decision makers and employees, creating greater risk, breaking processes and undermining security

Low employee knowledge of policies, lack of compliance and high cynicism contradicts the business view. Only **47%** reported that official policy or process is followed by all staff, while **39%** think that information security is just a "box ticking" exercise. Only **52%** of employees' report receiving regular and specific information security training.

There is a divergence between IT's perception of working practices and employee reporting across the board. Perception of where people work and the devices they use differ substantially. For example, employers reported **43%** of staff use their own device for work, while **63%** of employees stated they do so.

Business have some work to do to align their security policies with their employees' requirements and expectations. 42% of employees view their organisations security policies as either a slight or significant hindrance to their efficiency.

The six criteria of the Cyber Ready Index



#4

The more Cyber Ready the business, the better the competitive advantage

Cyber Ready businesses exhibited a high degree of trust and greater revenue growth. Businesses classed as Cyber Ready on the Index scored **4.3** out of 5 for reported stakeholder trust (customers, employees and regulators); while **47%** reported annual revenue increasing by more the **5%** in the last year.

Businesses who show Advanced readiness sit at an inflection point where outcomes accelerate rapidly. Advanced businesses (the top 5% and highest performing group on the Index) show a significantly higher growth rate than the rest, with **58%** reporting an increase of revenue of more than 5% in the last year and they enjoy very high levels stakeholder trust scoring **4.8** out of 5.

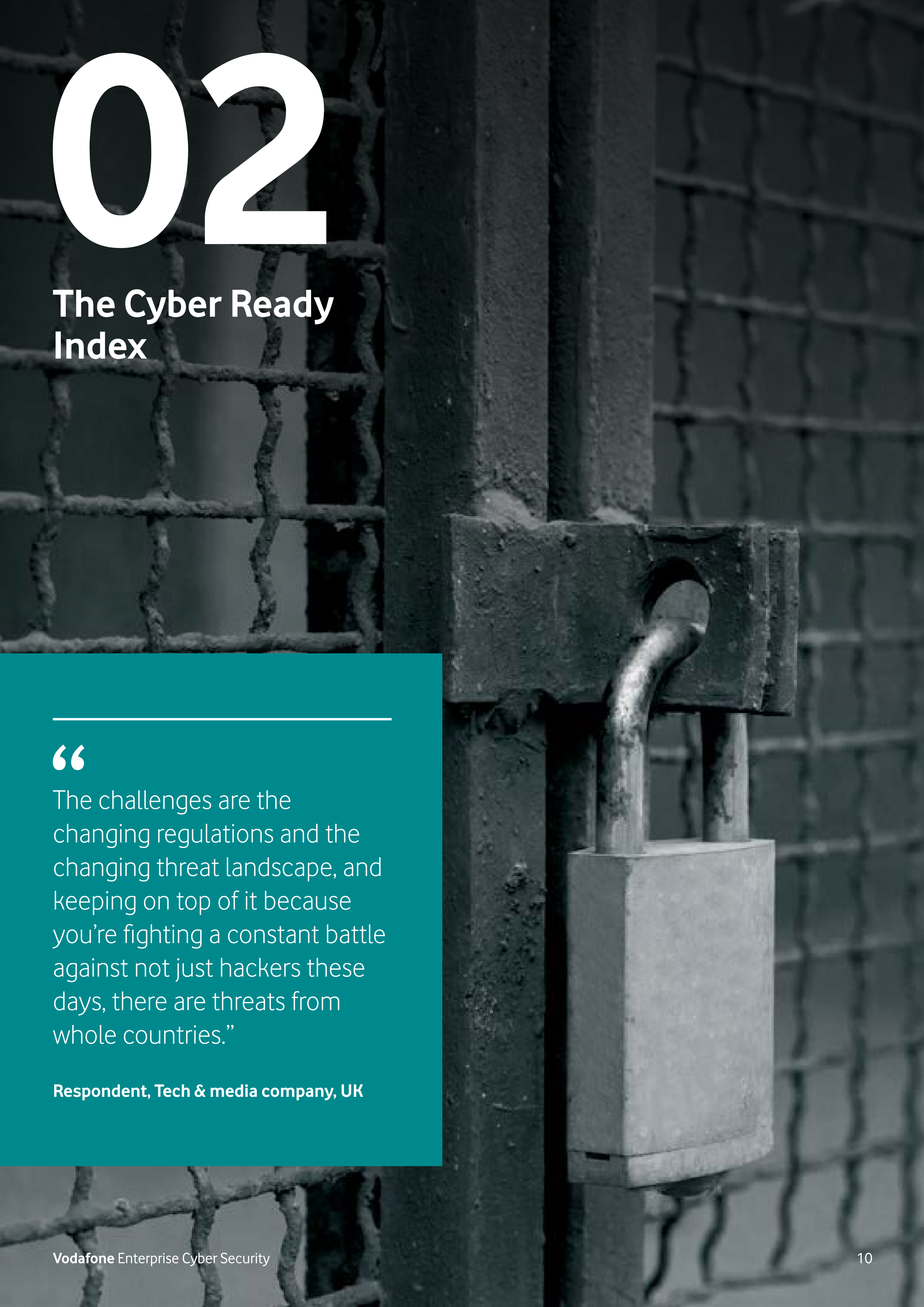
Conversely the least cyber ready organisations (Basic readiness, <25), often didn't achieve the same levels of trust and growth: Stakeholder trust drops to **3.1** out of 5; while only **22%** reported annual revenue increasing by more than 5% in the last year.

#5

Worried consumers feel at risk online and will pay a premium for peace of mind – but businesses have been slow to capitalise

Consumers feel under attack and are being selective around who they deal with as a result. 34% of consumers say they are increasingly aware of security threats being discussed in the media. **70%** consider themselves to be at risk of a cyber-attack or online threat, while **63%** have stopped using at least one online service due to security concerns and **43%** don't trust the security of companies they still use.

"Monetising" security is a potential differentiator, but businesses lag behind consumer attitudes here. 59% of consumers agreed that they are 'willing to pay extra for a higher level of security for the devices and services I use' - but only **29%** of businesses see there are significant financial benefits from 'being able to charge a higher price for our products/services due to increased confidence of customers doing business with us.' This is a significant opportunity for Cyber Ready businesses to capitalise on.



02

The Cyber Ready Index

> “The challenges are the changing regulations and the changing threat landscape, and keeping on top of it because you’re fighting a constant battle against not just hackers these days, there are threats from whole countries.”
>
> **Respondent, Tech & media company, UK**

2. The Cyber Ready Index

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.

2.1 What does being Cyber Ready mean?

2017 was a watershed year which saw a deluge of high profile and exceedingly costly cyber-attacks make security big news in the public consciousness and in the boardroom. In 2018 things are only accelerating, with a diverse cast of inventive and unrelenting cyber adversaries exploiting technologies – both new and old – for a range of criminal activities to create an ever evolving threat landscape.

Greater public scrutiny and media focus, combined with changing regulations, create a complex and highly pressurised environment for businesses who need to secure their data, retain customer trust and differentiate from the competition.

Against this backdrop, businesses must become Cyber Ready to win

We define a Cyber Ready business as one that is effectively prepared for the challenges and opportunities of cyber security - able to not just survive but thrive. As the cyber landscape evolves at pace, businesses and decision makers must too – adopting a more proactive, attacking approach to securing their information, people, places and things.

With the massive increase in the number and variety of cyberattacks, it's not enough to simply build up your perimeter defences anymore. Instead CISOs and other IT & c-level decision makers need to be more dynamic, preparing for both the inevitable attacks and emerging trends. Putting their business on a ready footing, where resilience and recovery are seamless and lessons are quickly learnt and acted upon.

This raises a huge number of questions including:

1. **Do you understand and have clear visibility of your digital footprint and where your data goes?**
2. **Have you invested in cyber security to adequately protect your data, devices and places?**
3. **How quickly can you recover and resume normal operations after a security incident - do you have effective processes in place to communicate with regulators and customers?**
4. **Do you have a clear cyber strategy that everyone has bought into – including the board?**
5. **Have you put in place training and effectively communicated security policies to help educate your staff?**
6. **Do you have the right cyber skills and knowledge in place to keep your business running and support growth and transformation initiatives?**

A truly Cyber Ready business can answer these questions confidently.

2.2 Calculating the Cyber Ready Index

The Cyber Ready Index is the result of our in-depth survey of IT and security decisions makers and business employees. Employees are defined as those consumers who are working, use IT and technology frequently in their job roles and they were asked additional questions during the research.

The Cyber Ready Index creates a statistical measure of cyber readiness that can be applied across all respondents. 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

3. The average score is calculated across all six criteria to create a **Cyber Ready Rating out of 100**.

The Six Cyber Ready criteria

Digital Footprint

Assessing the 'gap' between employer and employees reporting of their organisations' Digital Footprint. This includes factors such as awareness of mobile/off-site working and use of BYOD within organisations of the same size and sector.

Cyber Operations

This focusses on an organisation's confidence in its ability to secure their sensitive and personal data, whether in the cloud or on mobiles. It also looks at the level of investment in information security.

Cyber Resilience

This assesses whether a business has in place and tests relevant security policies and looks at the company's ability to identify, contain and recover/learn from an attack.

Cyber Strategy

Here we assess whether there is support and buy-in from senior management for improved security measures. It also digs into the extent to which the business understands that a strategic approach to security can differentiate in the eyes of customers.

Employee Awareness

Looking into whether the company has plans and policies that specifically address the security behaviour and actions of employees (such as a remote working policy) and whether there is dedicated security training for staff.

Understanding Risk

What is the level of awareness and consideration of security issues in the company, especially when implementing new initiatives or working with partners?

The Cyber Ready Index

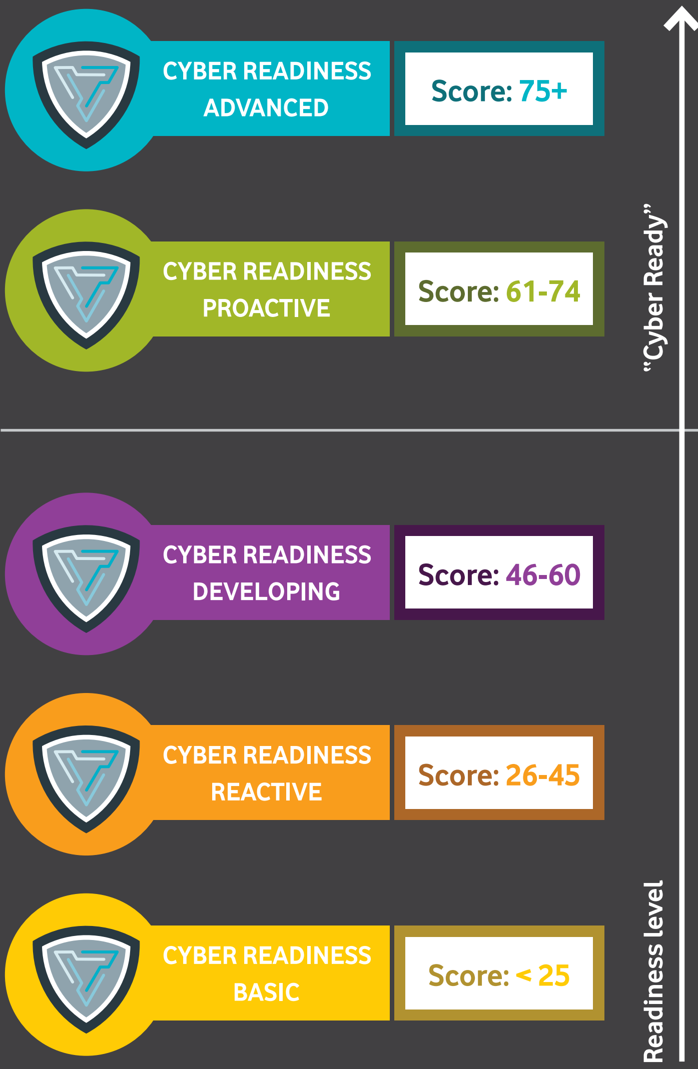
Scoring levels of readiness (out of 100)

The Cyber Ready Index is relative across different business types and accounts for differences in company size – any business, large or small, can be Cyber Ready (or vice versa).

Based on this Cyber Ready score out of 100, we've classified five levels of Cyber Readiness.

✓ A Cyber Ready score was calculated for each respondent; we have defined a 'Cyber Ready' business as one scoring **61+**. Businesses who have achieved this score have demonstrated a reasonable degree of Cyber Readiness across the different criteria, although there is still room for improvement. A Cyber Ready business comprises of both the **Proactive** and **Advanced** readiness levels – with the latter being the readiest of all.

The five Cyber Ready levels



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"

Readiness level

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.

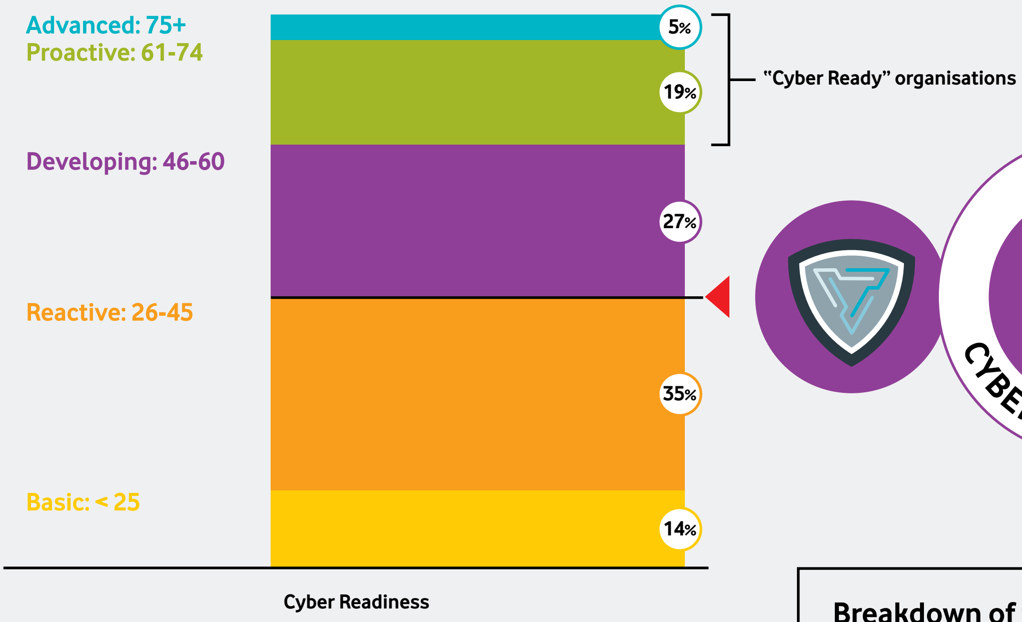
REACTIVE

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.

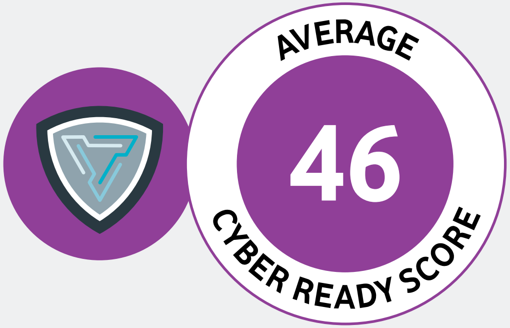
BASIC

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.

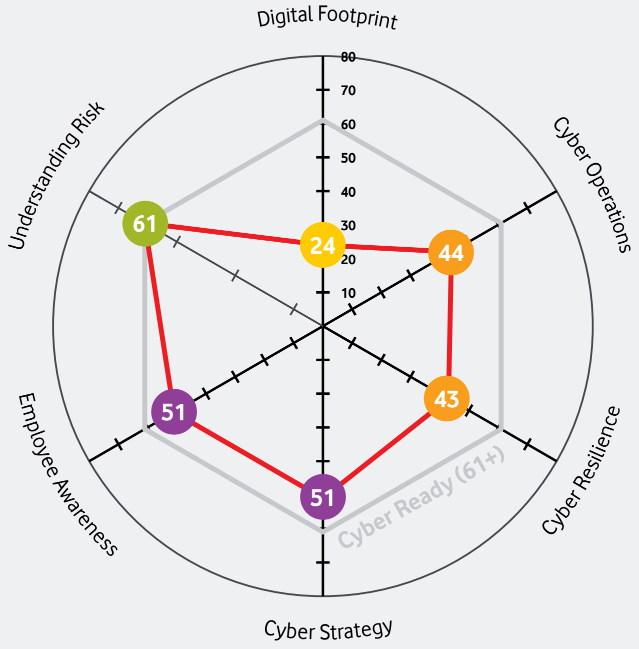
2.3 Assessing Cyber Readiness in 2018



Average Cyber Ready Index score (out of 100) and percentage levels across all businesses.



Breakdown of the Average Cyber Ready criteria score for all businesses (out of 100).



The Cyber Ready Index identified a number of key trends amongst all businesses.

Only one in four businesses are classed as Cyber Ready

Across all respondents, only **24%** of businesses surveyed globally can be classified as Cyber Ready today (rating an average of 61/100 or more) – and just **5%** of this group qualify as having Advanced levels of readiness. The average Cyber Ready Index rating across all businesses, verticals and countries was **46**, which falls into the lower end of the Developing readiness level.

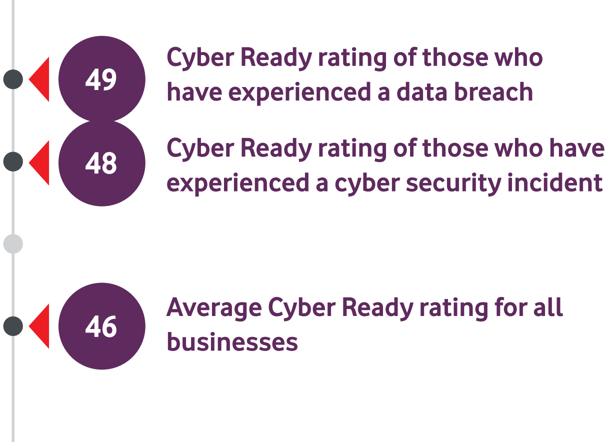
Overall, **27%** of all businesses were classified as Developing. This shows that the security message is starting to get through, the right measures are starting to be put in place and with some focused efforts to improve they can quite quickly progress and become Cyber Ready.

Over a third of all businesses fell into the Reactive category, while **14%** of businesses showed only Basic readiness and significant deficiencies across the Cyber Ready criteria today.

Businesses who have experienced a data breach are slightly more Cyber Ready

Those organisations who have reported experiencing a security incident or data breach in the past have a slightly higher than average Cyber Ready rating in the present – potentially demonstrating that they have learnt lessons from the experience.

Cyber Ready Index score by security incident experience



The strongest performing areas across all businesses are Understanding Risk and Employee Awareness

Encouragingly, all businesses scored highly in Understanding Risk with a score of **61**, which shows the increased awareness of and focus on cyber security when making key business decisions. Information security was consistently ranked as a top three consideration by businesses when thinking about implementing various growth and transformation initiatives, with cost management and increasing productivity being the other two.

Businesses are also confident that they are ensuring that employee-related security policies are updated and communicated (including offering training) regularly, with an Employee Awareness average of **51** (stronger performance is classified as 51+).

Cyber Ready IT specialist on Employee Awareness

> “Training that happens every 14 days is organized by our IT department and sometimes by external IT advisors ... with their signature employees also agreeing that they have been made aware of [security issues], therefore we did our part and they did theirs.”

Pharmaceutical firm, Germany, 249-999 employees, Proactive readiness

Employee Awareness effectiveness

However, while businesses are bullish about having put policies and training in place, the effectiveness of their communication for employees may not be as robust as assumed.

When questioned, employees had a much lower understanding of security policies and practices than their employers believe. Some employees knew of the existence, but not the details, of policies:

> I know there are formal processes in place but I'm not sure I'm fully aware of the content."

While others were simply not aware of policies at all:

> I don't think there are any policies in place. I'm not sure but it's not something that I'm personally aware of."

Security is often viewed as the responsibility of other people and departments within the organisation, so clearly there is some additional work required here. We will explore this disconnect further in Chapter 6.

Half of all businesses have significant work to do

Half of businesses were classed as only meeting the criteria for Basic (**14%**) or Reactive (**36%**) readiness. This means they currently have low readiness scores across several of the Cyber Ready criteria and significant improvements are required in order become ready and protect their businesses effectively.

The expert view

> Vodafone's research shows what many of us in the industry knew, suspected or feared... that cyber security is still a gap in companies' risk management strategies all too often. The revelation that few businesses are truly "cyber ready" reflects that fact that actually there is a striking asymmetry between defenders and attackers when it comes to their respective objectives."

Piers Wilson, Director, Institute of Information Security Professionals (IISP)

Gaining a clear understanding of their Digital Footprint is a universal challenge

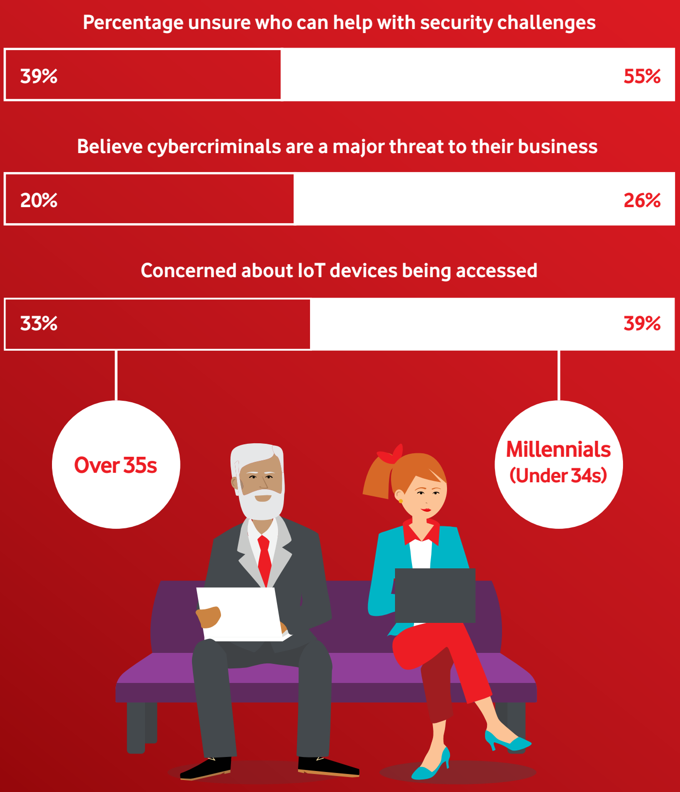
With a score of only **24/100** overall, Digital Footprint was the area where most businesses were shown to be struggling badly.

A low Digital Footprint score highlights a number of inconsistencies between the businesses and employee reporting of the different device types in use and their working practices including mobile working. **50%** of all business have only Basic readiness when it comes to Digital Footprint – while only **3%** of businesses are Cyber Ready in this aspect.

Understanding of their Digital Footprint has proved to be consistently an area of concern across all business sizes, regions and verticals. Use of non-approved IT solutions by employees also remains commonplace and creates risks.

> “We’ve got standard work applications like Office 365 and Onedrive and the like. But we’ve all been using workarounds. Up until fairly recently we were all having to share stuff and even now, amongst ourselves we will quite possibly use Google Drive to share stuff.”
>
> **Employee, Education, Rep. Ireland**

Cyber Ready by age



There is not a large “generational divide” when it comes to Cyber Readiness between millennial decision makers (up to 34 years old) and their older peers (35+) – but the younger age group are slightly more ready. The average millennial scored Developing readiness (**46**/100), while the 35+ group on average had Reactive readiness (**44**/100).

Millennials are more aware of the need to operationalise security, scoring **48** for Cyber Operations compared to **39** for 35+ year olds. This figure drops to **35** for the over 55s who are potentially further removed from the day-to-day concerns. However, the millennials’ greater operational understanding is accompanied by the growing confusion of who can actually help to solve increasingly complex security challenges.

Older decision makers have a better appreciation of the risks that their Digital Footprint brings, scoring an above average **26** compared to **22** for the under 34s. This was the only criteria where the millennials rated less ready than their older peers, potentially due to more awareness and concerns about new device types like IoT. Younger decision makers are more likely to see information security as an enabler of, not a barrier to, new opportunities with **71%** strongly agreeing with the statement versus **62%** of those over 35.

2.4 What contributing factors are driving the need for Cyber Readiness?

Despite greater cyber awareness and spend, an increasingly complex digital footprint and low levels of resilience are putting traditional cyber security strategies under strain and driving the need for readiness.

So why is Cyber Readiness proving so elusive for many businesses? We identified a number of trends that put the Cyber Readiness challenge into context. The changing cyber threat landscape and evolution of both business and consumer digital footprints are both major factors that are creating new challenges.

Meanwhile despite greater awareness and focus, business confidence in readiness levels of these threats is low and confusion on who can help with security has actually increased.

Businesses are feeling the pressure, as one respondent from a large UK Financial Services company summed it up:

"There have been so many cases, particularly in the financial industry, of data being compromised, that it's something we're all conscious of."

Businesses digital footprints are evolving fast

The adoption of newer technologies and working practices has created a rapidly changing digital footprint which is growing in size and scope. While this is unlocking exciting new opportunities and efficiencies for businesses, it brings new risks and considerations too.

Having the necessary resources, skills, tools and systems to understand and secure their digital footprint is a task that is becoming ever more complex for IT and Security decision makers, while providing new potential opportunities for cyber attackers.

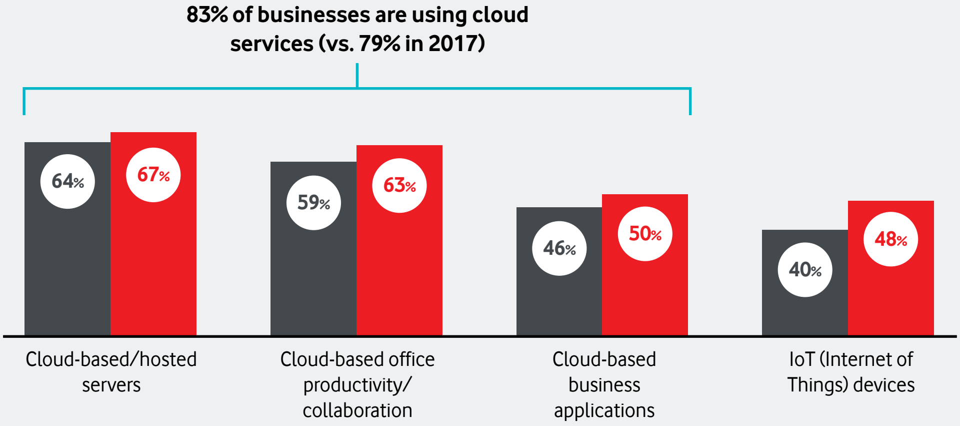
83% of organisations are using different types of cloud services (up 4pp from 2017)

48% of organisations are using Internet of Things (IoT) devices (up 8pp from 2017)

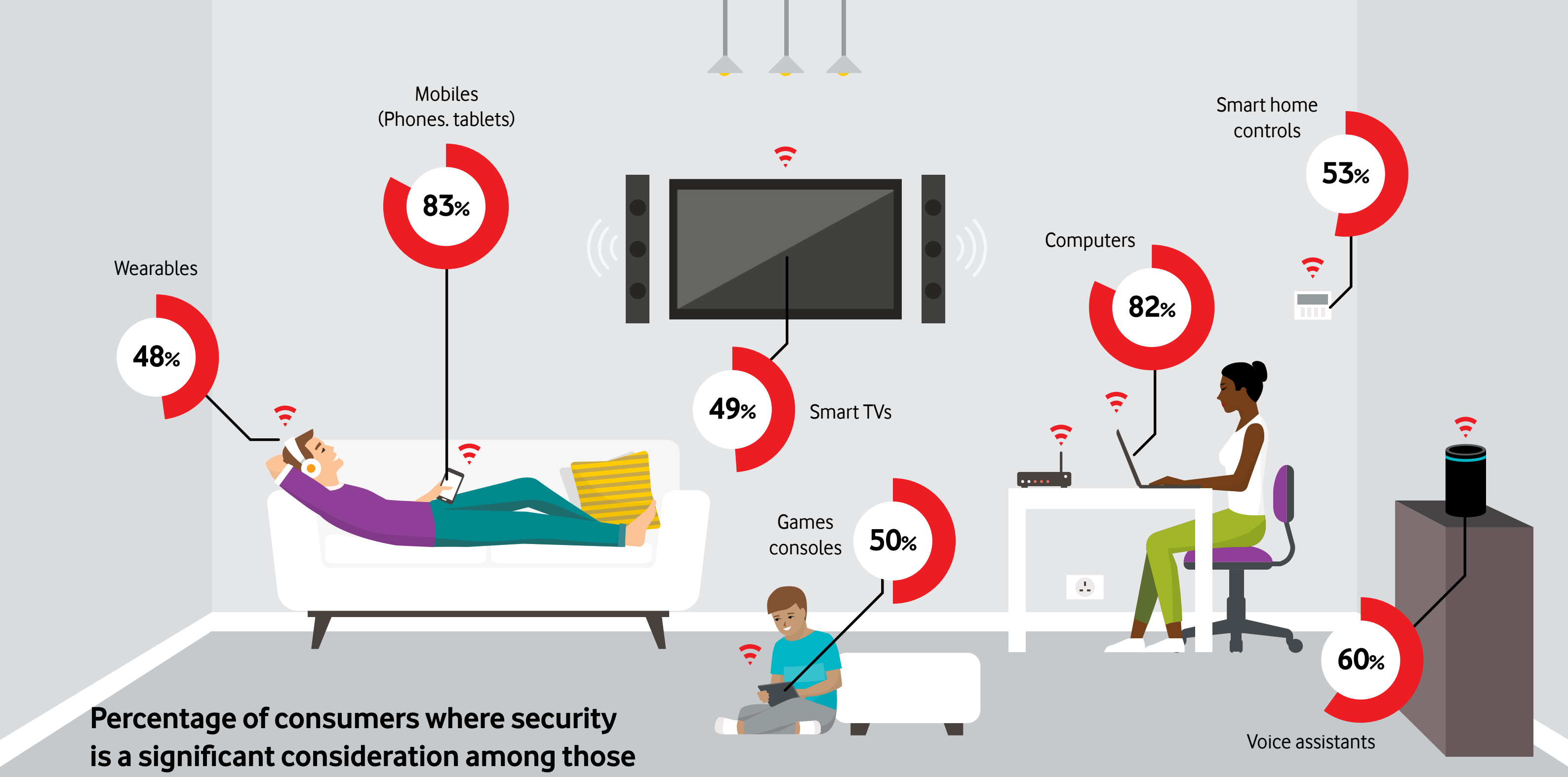
43% of organisations allow employees to BYOD (Bring Your Own Device)

46% of organisation report employees are remote working (for at least 30% of the time)

Percentage of organisation currently using the following systems or solutions



Businesses of all sizes are using more cloud-based servers, services, applications and productivity tools, the number of businesses using IoT devices has also increased by **8%** in the last year.



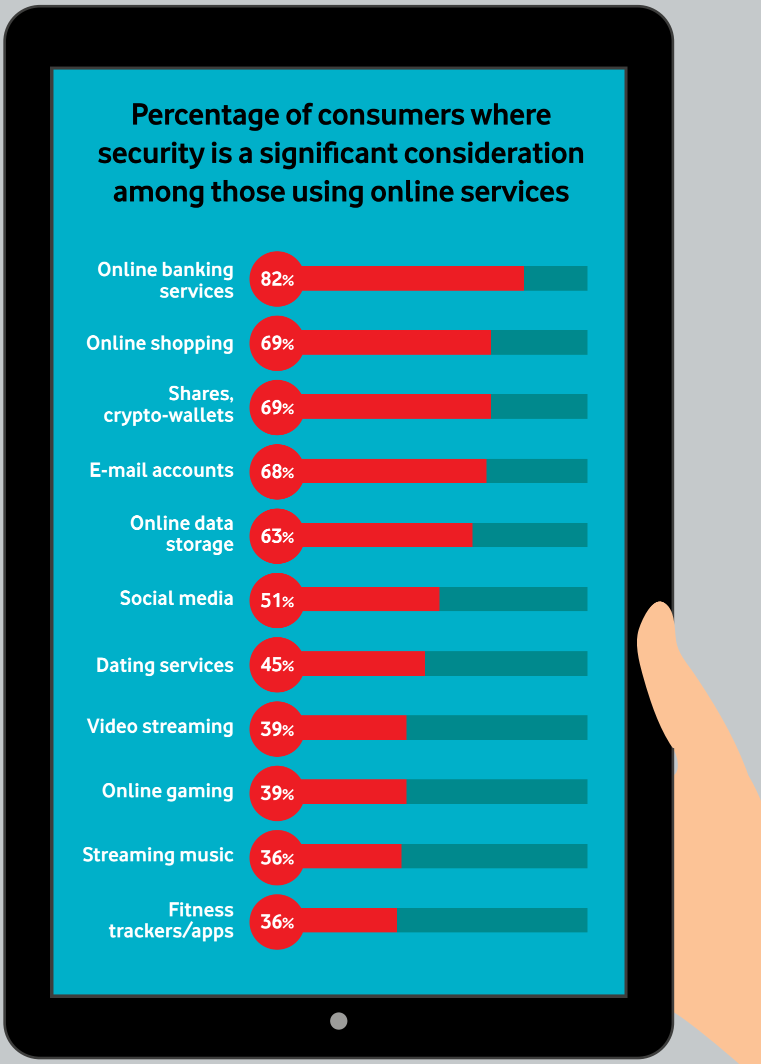
Percentage of consumers where security is a significant consideration among those using each device type

A consumers’ digital footprint also presents an increasingly complex picture

The average consumer currently now uses **9** different connected devices at home and **11** different online services, but there are highly uneven attitudes to their security online. Concern is highest about the security of mobiles devices (**83%**) and computers (**82%**) – but newer devices like voice assistants (**60%**) and smart home controls (**53%**) are also a cause for concern. As different device types continue to proliferate, this will only lead to greater risks to personal data and more confusion should the worst happen. In the words of one respondent,

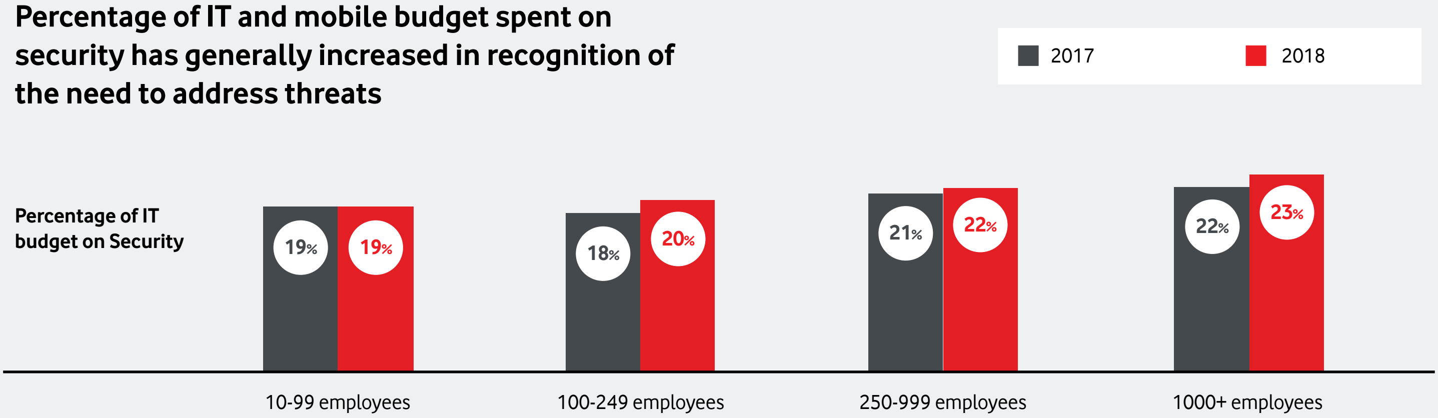
> **“I don’t have any idea who could support me in relation to cyberattacks. I would need support, whether it was advice, training, phone calls or anything.”**

Sharing their financial data online is the biggest consumer concern, specifically online banking (**82%**) and shopping (**62%**), yet only **51%** expressed concern about using social media and only **45%** online dating services. So while consumers are more educated and wary of the need for online security, perhaps they don’t yet appreciate the value to hackers of the sensitive and personally identifiable information (PII) shared within these types of services.



Percentage of consumers where security is a significant consideration among those using online services

Percentage of IT and mobile budget spent on security has generally increased in recognition of the need to address threats



Factors affecting increased spend on information security

Internal Factors

- 43% Greater use of cloud computing
- 36% More mobile devices to secure
- 35% More mobile/flexible working
- 35% To enable innovation
- 34% Increasing use of the Internet of Things (IOT)
- 34% New growth transformation inititiatives
- 34% More complex business processes/applications

External Factors

- 55% Increasing security threats
- 43% To minimise risks to organisation reputation
- 35% Industry/company specific risks
- 33% Requirements of regulators
- 33% Demands from customers/ shareholders
- 29% Media stories about security threats
- 28% Competitors have been impacted by security threats

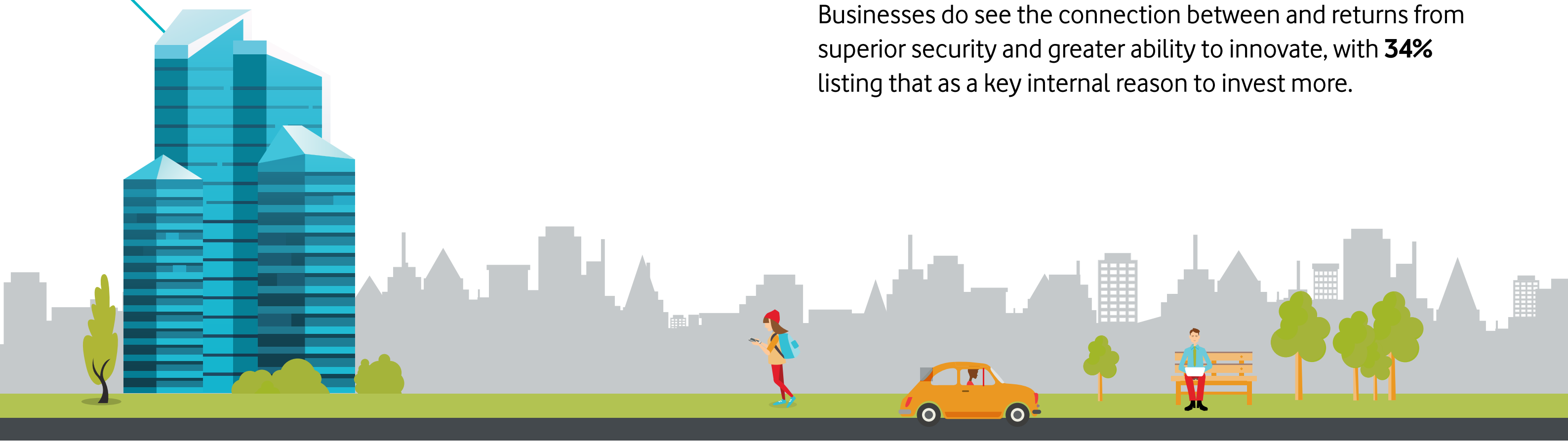
Businesses are spending more of their IT budget on security in 2018

Businesses are focusing a higher percentage of their IT budget on information security. Since 2017, all businesses with 100 employees or more report an incremental increase in terms of how much of their budget they allocate to security.

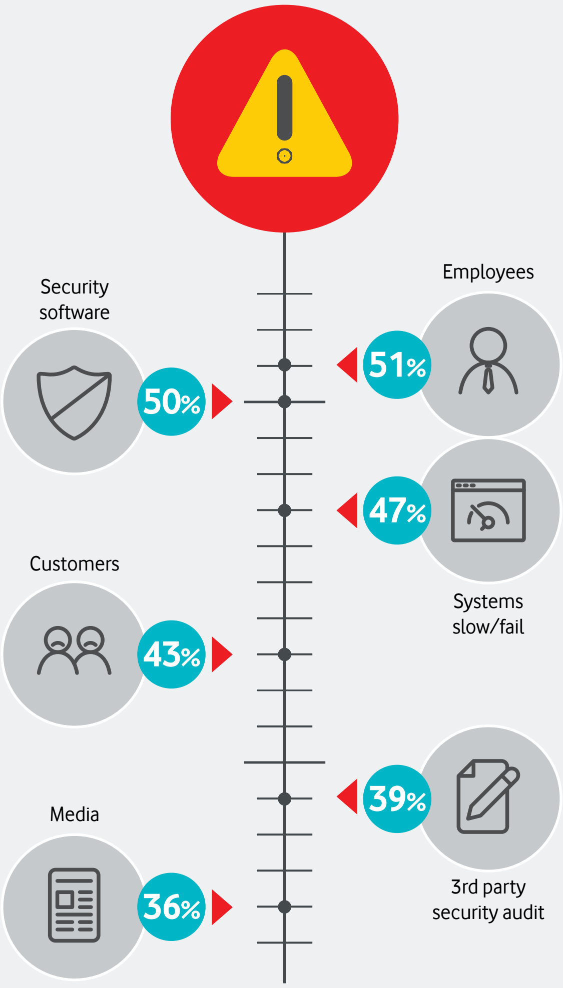
What's driving cyber security investment?

A range of internal and external factors are driving this increase in spending. Among those seeing a change in IT security budget, the main drivers of change are a perceived increase in threats (**55%**), concerns about reputation (**43%**), increased use of cloud-based (**43%**) and mobile working (**35%**).

There are a few notable increases in the last year, particularly the use of the Internet of Things (up **5%** since 2017) and also the concern about Stories in the Media (up **7%** since 2017). Businesses do see the connection between and returns from superior security and greater ability to innovate, with **34%** listing that as a key internal reason to invest more.



Security incidents are often discovered by sources outside of the IT and security team



When asked to list the various methods that decision makers have been made aware of a security incident, the methods most frequently cited by respondents often included being alerted by sources outside of IT including:

- Other staff within the business (51%),
- Being told by customers (43%) or
- Made aware via the media (36%).

The incident being detected first by their own security systems and software was only cited by half of respondents (50%).

The frequency of security incidents is underplayed within businesses – with staff and customers often reporting them first

Only **21%** of all business respondents report that they have experienced a security incident, although this figure rises to **26%** amongst businesses of 1000+ employees. However, despite this, the increase spending and the acknowledgement of the various internal and external threats; worryingly many organisations admit to only becoming aware of security incidents when they are reported to them by people outside the IT function including staff, customers and even the media - as shown in the image on the left.

Business readiness and resilience to cope with attacks is under scrutiny

Despite greater awareness of cyber threats and more investment, only **29%** of business decision makers strongly agreed that their organisation is 'ready for the future'.

The majority of staff also have some doubts – only **32%** felt 'very confident' in their organisations ability to respond to a cyber threat or attack.

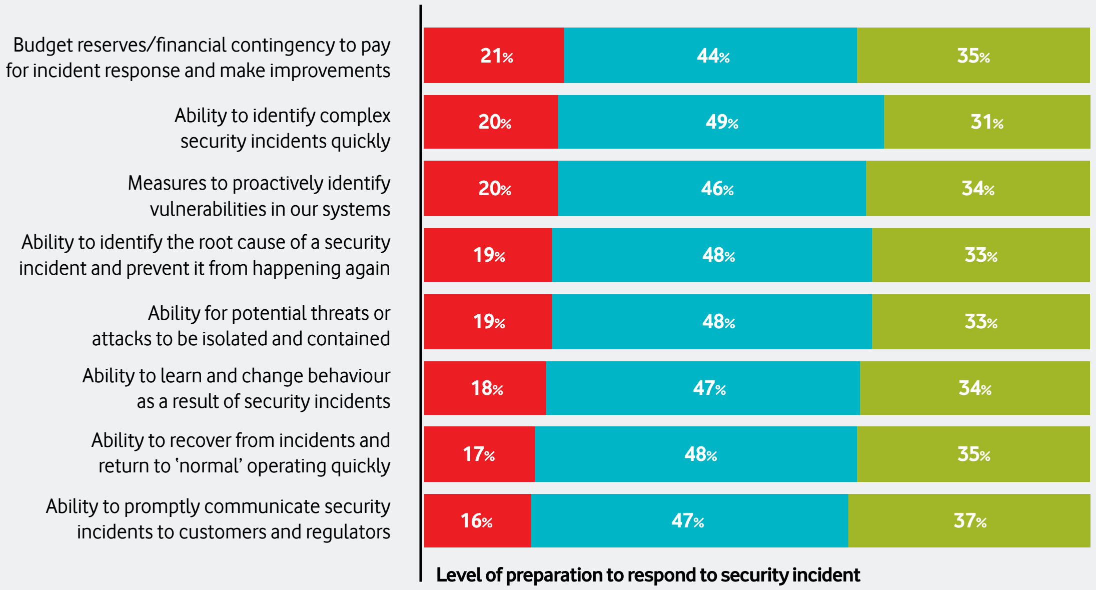
Businesses resilience levels in the event of a security incident are variable. We assessed preparation levels across multiple necessary incident response measures (the systems and processes in place to aid recovery), and found **25%** of all businesses consider themselves unprepared for three or more of these critical actions. Although many businesses consider themselves very well prepared in certain areas, such as ability to promptly communicates incidents externally (where **84%** are quite or very well prepared), few were primed across the board:

21%	**of businesses consider themselves unprepared in terms of having a financial contingency to pay for incident response and make improvements**
20%	**lack the ability to identify complex security incidents quickly**
20%	**don't feel they have the measures to proactively identify vulnerabilities in their system.**

See chart overleaf for a complete breakdown.

Most businesses have gaps in their security preparation

🟥 Not prepared 🟦 Quite well prepared 🟩 Very well prepared



51% are not prepared for one of these incident responses

25% are unprepared for three or more of these critical incident responses.

Cyber complexity is creating growing confusion

Despite the increased focus and attention on cyber security, confusion about who can actually help to handle security challenges is actually increasing amongst businesses. In addition, businesses who have use a wide array of IT and technology vendors feel this makes it difficult to identify who is responsible for resolving different types of incident.

46% of businesses agreed that they are unsure of who can help with information security challenges, an increase of 5pp since 2017

44% agreed that they use so many IT vendors that it is difficult to understand where security responsibility lies, up 4pp in the last year

34% do not feel well-informed about information security solutions, up 5pp since 2017

The expert view

> “The defence against cyberattack needs to take account of a growing technology footprint and attack surface; more systems, more devices, more ways of delivering IT through on-premise and cloud; and a greater expectation from staff, business partners and customers that technology-led services and interactions (digital transformation) will predominate.”

Piers Wilson, Director, Institute of Information Security Professionals (IISP)

03

The Cyber Ready Index impacts business performance

“

The Vodafone Barometer offers an invaluable method of seeing how organisations in general anticipate and adapt to change. Whether change is reflected in terms of ‘products’ or perceived threats, there are all too evident factors that constrain an organisation’s willingness to explore plausible change, and proactively adjust to it.”

Randolph Kent – Director, The Futures Project, The Royal United Services Institute for Defence and Security Studies

3. The Cyber Ready Index impacts business performance

Around the world, business decision makers increasingly realise the positive impact of improved information security on future growth and transformation initiatives; and the potential financial gains better security can bring. Meanwhile, the research findings clearly identify a strong correlation between how Cyber Ready an organisation is and their level of business success.

3.1 Cyber Readiness drives revenue growth and increased trust

9 out of 10 decision makers see the link between cyber security and business success

There is a clear expectation that improving cyber security will help businesses unlock a range of financial benefits. A high proportion of business decision makers believe improving security standards will deliver either 'some' or 'significant' benefits when asked about a numbers of positive business outcomes including:

92%	Making our business more efficient
90%	Improved staff productivity
90%	Reduced costs from downtime
89%	Better reputation within our market potentially attracting new customers

Businesses spending a higher percentage of their IT budget on security are reaping the rewards

Businesses of all sizes who spend a higher proportion of their IT budget on security are more likely to consider their business to be over-performing against competitors in multiple areas.

When asked to self-report on their level of performance against their peers across a number of business outcomes, businesses who are currently spending 20% or more of their IT budget on security felt they had a strong competitive advantage across the board.

65%	Building a digital advantage
66%	Becoming more customer-centric
63%	Being focussed on innovation
62%	Being prepared to deal with the risks to our business and markets

A high level of Cyber Readiness has a positive impact on trust and business performance

The Cyber Ready Index rating shows a clear relationship between the success levels enjoyed by the businesses at the different levels - the more Cyber Ready the business, the better the business outcomes. For example, there is a staggering **34%** difference between the number of Advanced businesses and Basic businesses reporting high revenue growth.

In order to investigate the relationship between an organisation's degree of readiness and its success (or lack of it), we statistically tested each group of businesses in the five levels of the Cyber Ready Index against multiple dependent variables from the research data. The aim was to identify the impact of each respondent's Cyber Readiness level on selected 'measures of business success'.

The businesses outcomes that the Cyber Ready Index groups were tested against included:

- Stakeholders trust levels in an organisation's security measures (including employees, consumers and regulators)
- Changes in organisation's revenue in past 12 months
- Comparison of current performance against similar competitors, across a number of areas

The results show this clear correlation between an organisation's level of Cyber Readiness and positive business outcomes.

Cyber Ready businesses exhibited a high degree of stakeholder trust (amongst customers, employees and regulators) of **4.3** out of 5; while **47%** reported annual revenue increasing by more than 5% in the last year.

Conversely the Basic organisations, the least Cyber Ready, revealed significantly worse business outcomes - stakeholder trust (amongst customers, employees and regulators) drops to **3.1** out of 5; while **22%** reported annual revenue increasing by more than 5% in the last year.

Cyber Ready levels compared to measures of business success

Cyber Ready = Growth & Trust

Cyber Ready rating	Stakeholder Trust (out of 5)	Revenue Growth (5%+)
Advanced	4.8	58%
Proactive	4.3	48%
Developing	4.1	32%
Reactive	3.6	27%
Basic	3.0	24%

+1.8

The gap between Advanced and Basic businesses for stakeholder trust is a substantial 1.8 out of 5

The Advanced advantage

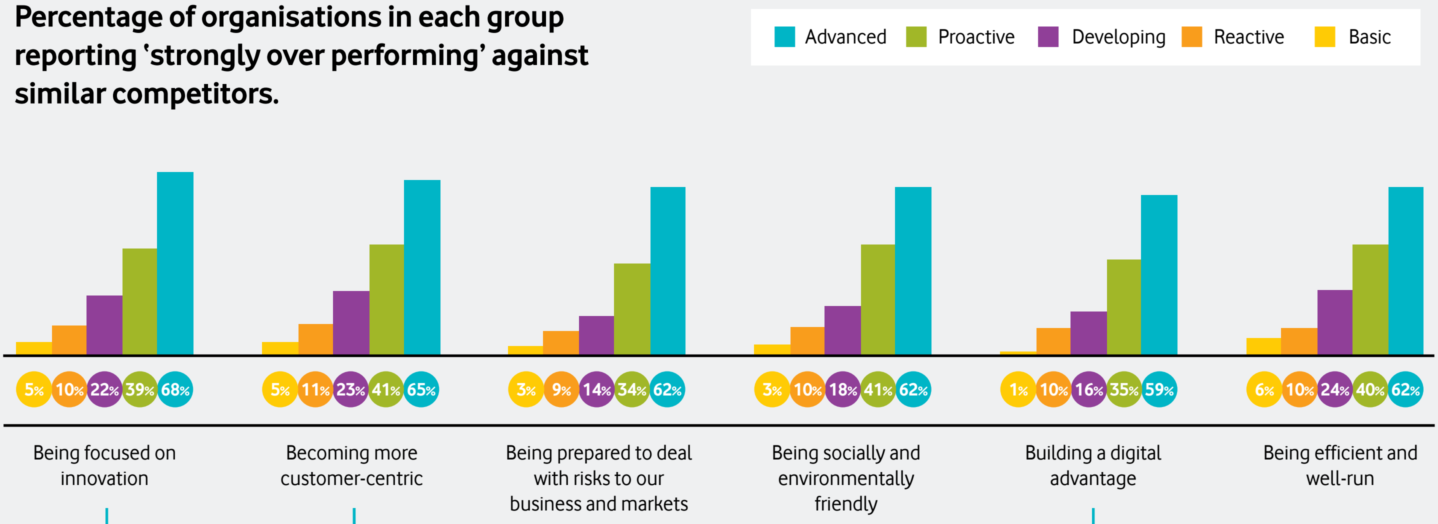
Those businesses who classify as Advanced sit at an inflection point where business outcomes accelerate rapidly.

Only **5%** of all Cyber Ready businesses demonstrate Advanced readiness. These exhibit a spike in business success compared to less ready rivals, even against the **19%** of Proactive businesses who also qualify as being reasonably Cyber Ready.

Advanced businesses show a significantly higher growth rate, with **58%** reporting an increase of revenue of more than **5%** in the last year – they also enjoy very high levels of trust among their stakeholder community scoring **4.8** out of 5.

The more cyber ready the business, the better the business outcomes.

Percentage of organisations in each group reporting 'strongly over performing' against similar competitors.



68%

of Advanced businesses believed they were more 'Focused on innovation' – 29% higher than Proactive businesses.

65%

of Advanced businesses were bullish about their ability to 'Become more customer-centric' against just 41% of Proactive businesses.

59%

of Advanced businesses felt they were strongly over performing in Building a digital advantage' – against 35% of Proactive businesses and only 1% of Basic businesses.

3.2 The Cyber Ready competitive advantage

Advanced companies report outperforming the competition in essential business KPIs

Companies who have security in their DNA, in their values, products, services, messaging are capturing marketshare. The solid foundations of strong cyber security, readiness and resilience seemingly creates a high level of confidence throughout the business.

Maintaining a high level of stakeholder trust requires security teams to speak the language of their business. Security leaders need to understand Board-level performance metrics and how security impacts those measures.

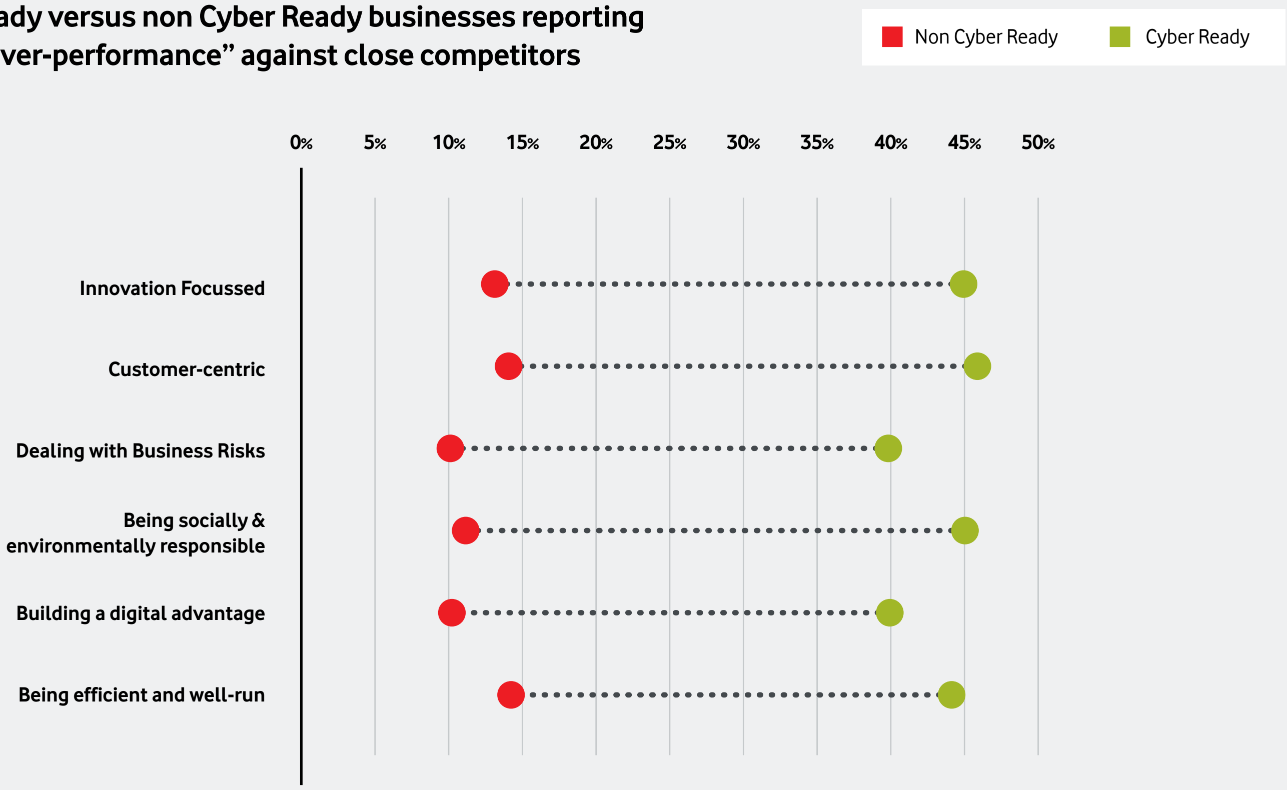
Here the Advanced group report a clear advantage in overall performance against the competition – particularly in the key areas of being able to be focussed on innovation, in building a digital advantage and in becoming more customer-centric.

When broken down by their Cyber Ready level, the percentage of organisations in each group reporting themselves as "strongly over-performing" against competitors showed a clear disparity between Advanced and the rest. Performance increases notably in line with Cyber Readiness; almost twice as many Advanced business reporting being at an advantage compared to those of Proactive readiness.

Among our average-scoring, or Developing, organisations only **14%** report strong over-performance in being prepared to deal with risks, and only **23%** over-perform in becoming customer-centric. Only **9-11%** of our largest group of organisations, the Reactive group, managed to over-perform in any of the 6 areas we measured.

The tangible link between being more Cyber Ready and a positive impact on business performance ultimately can enable organisations to make a clear business case for investing in security considerations and initiatives with clear financial consequences.

Cyber Ready versus non Cyber Ready businesses reporting “strong over-performance” against close competitors



Cyber Ready = Competitive Advantage

When you compare these indicators at the level of Cyber Ready vs Non Cyber Ready, it becomes clear that being Cyber Ready can be seen as a competitive advantage for organisations of all sizes.

On average, **12%** of Non Cyber Ready organisations report over-performance in any one of these 6 areas, compared to **43%** of Cyber Ready organisations.

The expert view

> “My interpretation of this finding is that a business that is efficient and well run has good business outcomes, and by virtue of being efficient and well run, it manages cyber security well – recognising cyber security is as much about people and process as it is technology.”

Colin Robbins, Principal Security Consultant, Nexor

04

Breaking down the six criteria of the Cyber Ready Index

> “
> Not facing cyber security challenges head-on puts businesses at risk of reputational damage and loss of revenue. This research reveals that many businesses have an appreciation of these risks and employees are coming to understand their importance in ensuring cyber security, hence there is a great opportunity for the cyber security industry.”

Dr Emma Williams, Vice-Chancellor’s Fellow in Digital Innovation and Wellbeing, University of Bristol

4. Breaking down the six criteria of the Cyber Ready Index

Although there was remarkable consistency in overall Cyber Readiness trends across all respondents, we identified a number of interesting findings when assessing the results across the six individual Cyber Ready criteria.

Broadly they fall into two groups:

Improvements needed
Digital Footprint, Cyber Operations and Cyber Resilience

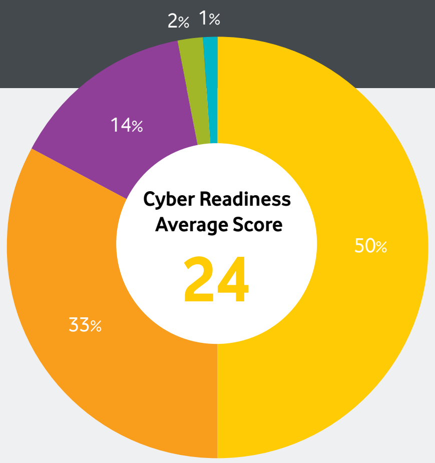
The stronger performers
Cyber Strategy, Employee Awareness and Understanding Risk

Key for following charts

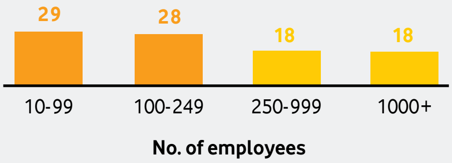
🟦 Advanced 🟩 Proactive 🟪 Developing 🟧 Reactive 🟨 Basic

Digital Footprint

Persistently the area where businesses were the least ready



By Company Size



Key finding

Half of all businesses were rated as having only Basic readiness, defined as the employer under-estimating the degree of remote working and use of employee owned devices within the organisation.

Overall only **3%** achieved a Cyber Ready score of **61+**, meaning they have accurately assessed or overestimated remote workers or employee owned devices.

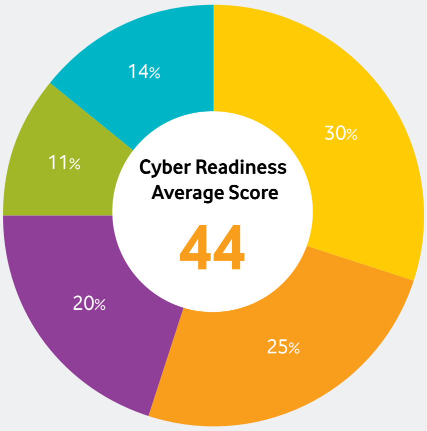
New technologies are creating rising levels of apprehension - the number of people concerned about remote access to connected systems in larger businesses (1000+) is growing:

- **42%** are concerned about IoT devices, 9% higher than in 2017.
- **17%** are concerned about connected vehicles, which is a 7% increase since 2017.

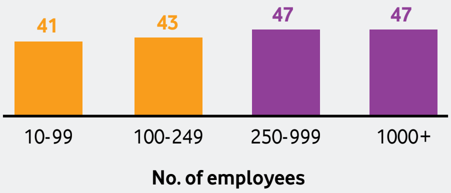
What did we measure?

Assessing the 'gap' between employer and employee reporting across:

- Volume of remote & mobile working
- Propensity of employees to use personal devices for work purposes



By Company Size



What did we measure?

- Confidence in the business's ability to protect personal identifiable and company data
- Confidence in the business's ability to secure its data in the cloud
- Confidence in the business's ability to support mobile and flexible working
- Percentage of IT budget spent on security.

Cyber Operations

Larger firms are at an advantage

Key finding

One in four businesses' Cyber Operations were classed as Cyber Ready – meaning that they are confident in their ability to secure their mobile and cloud-based data and allocate a high proportion of IT budget towards security.

30% of respondents' Cyber Operations ranked in the Basic group - demonstrating a lack of confidence in their ability to secure their data and low investment in their business' information security.

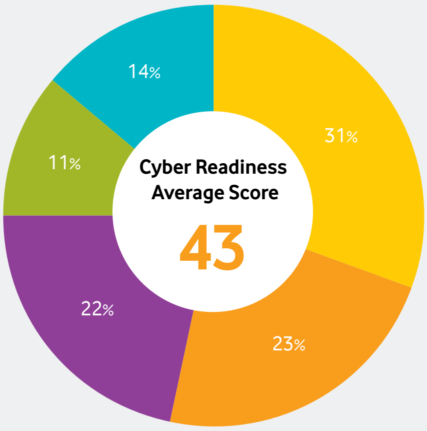
But encouragingly there is evidence that things are improving. Business confidence in the security measures they have in place to support various growth or transformation initiatives is increasing:

- **43%** are very confident in their security when implementing digital technologies (up 22% from 2017)
- **39%** are very confident in their security for their digital collaboration between employees (up 24% from 2017).

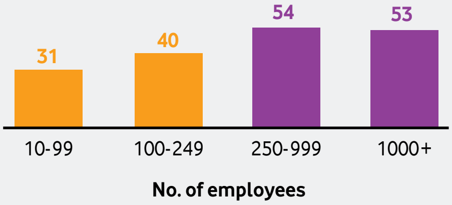
Larger firms (from 250+ employees) recorded a higher than average Cyber Operations score **47** out of 100; whilst the smallest businesses of 99 employees or less saw this score drop to **41**.

Increased overall confidence in security measures has also led to a decrease in businesses who view security as a blocker to new innovation or transformation projects. Since 2017, less people also perceive security as a barrier to rolling out new business initiatives such as:

- **30%** see security as a barrier when implementing digital technologies (down 7% from 2017)
- **29%** see security as a barrier to selling to or supporting customers online (down 5% from 2017).



By Company Size



What did we measure?

- Existence, extent and testing of security policies
- Ability to identify, contain and respond to a security incident (for example: existence of penetration testing, self-identified ability to identify contain and respond, employee education and communications).

How to respond and recover following a breach isn't always understood

Cyber Resilience

Smaller businesses are the least resilient

Key finding

Small businesses (10-99 employees) scored a worrying **31**/100 - meaning they are unlikely to have a full set of security policies in place and aren't resilient and able to withstand attacks while continuing business operations. A Reactive approach to resilience will quickly wear down any security team. However, larger businesses (250+ employees) scored a strong **53** on the Index.

26% of employees in small firms are less confident in the organisations ability to respond to a cyber threat or attack, compared to **19%** in businesses of 250+.

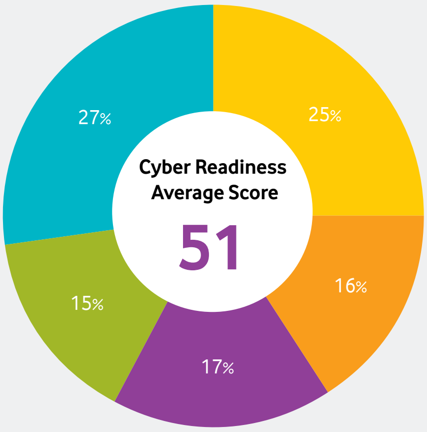
40% of all businesses believe it would take up to a week to respond to a breach and return to normal operations.

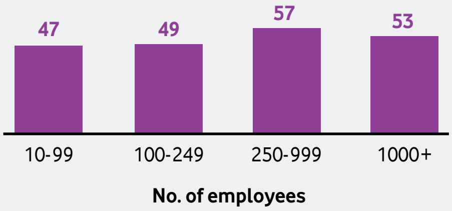
Larger businesses are more likely to have security policies in place AND regularly tested:

- Disaster recovery and business continuity policy in place and tested – SME **34%** vs **44%** larger businesses.
- Security incident/data breach action plan in place and tested – SME **33%** vs **43%** larger businesses.

> “The only thing that we've done is to make sure that our data is backed-up and that way, if something happened, we would be able to restore our data ... if information was actually stolen and then somebody started using our financial information or our customers (information), I'm really not sure what we would do to correct that.”

USA, Construction firm, 0-99 employees





What did we measure?

- Board-level support for cyber security strategy
- Stakeholder belief that information security is of high strategic importance for the organisation
- Recognition that cyber security is important for retaining and winning customers

Cyber Strategy

Most stakeholders recognise the value of a strong strategy

Key finding

The importance of cyber security is well recognised, **42%** of all businesses rate as Cyber Ready in terms of their Cyber Strategy with an average score of **51**.

71% of all businesses agree that "Senior management actively supports and encourages better information security measures".

78% of businesses who operate online view a 'good reputation for security' as a competitive differentiator and **75%** of employees agree, while this figure drops to **69%** when asked of all businesses.

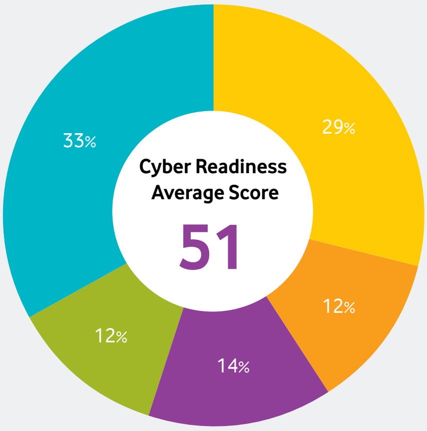
Technology & media are the most advanced industries in terms of their Cyber Strategy, with a higher than average score of **58**/100.

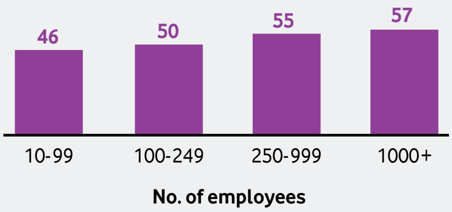
87% of businesses expect their information security budget to increase in the next three years, with a fifth predicting an increase of more than 50% of current levels.

The expert view

> "To ensure that the whole organisation supports a Cyber Ready culture, security must be democratised. Focus must be placed upon making security easy wherever possible."

Richard Archdeacon, Advisory CISO, Duo Security





Employee Awareness

Acknowledgement of the need to educate employees is high

Key finding

Acknowledgement of employees as a security risk is high - the implementation of security policies is seen as a key element of being Cyber Ready. Employee Awareness received a Cyber Ready score of **51** on average, which indicates businesses perceive high readiness – it was the second strongest performing of all the criteria.

71% of all businesses do have both security policies and training plans in place, although only **59%** of those businesses regularly test them.

Large businesses (1000+ employees) performed the most strongly in this area with an above average score of **57**. The smallest companies (10-99 employees) scored the lowest, coming in at **46**, five points below average.

Organisations in the Healthcare & Pharmaceutical (**57**) and Tech & Media (**54**) are leading the way in terms of strong employee engagement, while Retail (**44**) is struggling.

What did we measure?

- Communication of cyber security policy to employees
- Existence of remote working policy
- Existence of BYOD policy
- Employee cyber security training

The importance of Employee Awareness

Cyber Ready companies understand the stakes

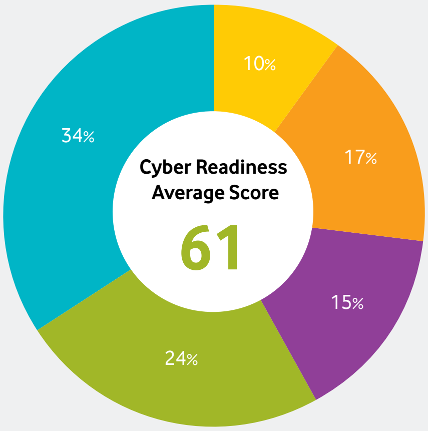
"Information security is totally mandated across everything; it's seen as a massively high priority. We take a compulsory tone to ensure everyone is aware of information security."

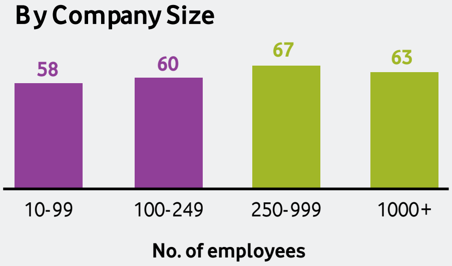
Tech. & Media, UK, 1000+ employees, Cyber Ready

While some employees think accountability lies firmly with IT

"I'm only middle-management so I'm not aware of anything that's formally in place. It's mainly down to the IT guys."

Employee





What did we measure?

- Existence and extent of cyber security criteria when commencing work with partner organisation
- Whether cyber security is considered for growth or transformation initiatives
- Whether the businesses are prepared to pay for cyber security support
- Whether the business assesses that they have the necessary cyber security skills in place

Understanding Risk

The importance of security in all aspects of business is well understood

Key finding

The importance of security in all aspects of business and the risks faced are well understood - even where other aspects of Cyber Readiness are lower. With an average score of **61**, over half of all businesses understanding of security risks consistently ranks them as Cyber Ready, with just **10%** of businesses ranking as Basic.

Information Security was ranked as a top 3 concern when assessing implementing new business growth and transformation initiatives – behind increasing productivity and cost management - when assessing implementing new business growth and transformation initiatives.

40% of all businesses were driven to consider security due to customer and partner demands; while **37%** felt potential loss of reputation across customers meant security had to be reviewed in-line with new initiatives.

GDPR is a concern, with almost two thirds of businesses still having work to do - as just **43%** of respondents currently say they are both aware of and have taken measures to ensure compliance, up from 29% in 2017. (Survey conducted in April 2018)

Increased security confidence has led to a change in attitudes towards risk by decision makers - **27%** of organisations agree that 'all new initiatives involve risks; we are accepting of risks to information security as well' – a surprising increase from 19% since our 2017 research, highlighting some possible complacency creeping in.

05

Cyber Ready Index trends assessed

> “
>
> I do believe many firms now realise that they need to understand their security posture (or Cyber Readiness), identify gaps, and the business risks involved, but are now looking for some help in prioritising their investment.”
>
> **Mike Sapien – Chief Analyst, Enterprise Services, Ovum**

5. Cyber Ready Index trends assessed

Cyber Readiness across countries, business sizes and sectors. Although there is generally a good understanding of Cyber Risks among most types of business, there are some pronounced differences between different countries, sizes and verticals when assessing other criteria of Cyber Readiness.

5.1 Cyber Ready by country

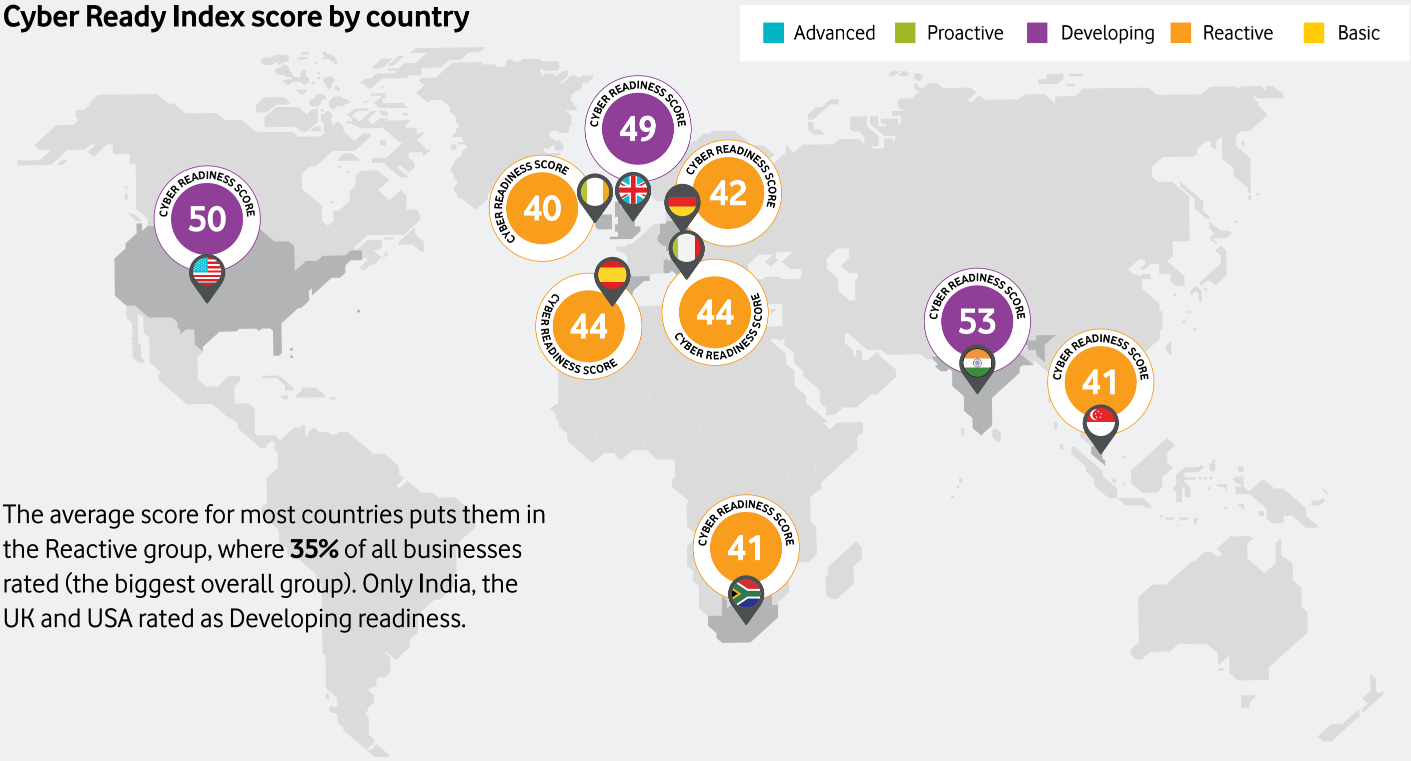
Readiness trends are consistent across countries, with the majority rating as Developing on the Cyber Ready Index

From the businesses surveyed, India (**53**), the USA (**50**) and UK (**49**) are more Cyber Ready than other countries; however, the overall trends are consistent by country – strong in Understanding Risk but low in understanding of their Digital Footprint.

The USA possesses an above average number of Cyber Ready businesses of any region at **31%**. India scored strongly across all areas of readiness, except for Digital Footprint (**20**), and Indian businesses overall score of **72** for Understanding Risk was the highest of any average score across all countries, sizes and verticals.

While collectively Europe's businesses were slightly below average (**44**), the Republic of Ireland (**40**) was the least Cyber Ready country based on those businesses surveyed. However, with a good rating for Understanding Risk (**52**) and reasonable one for Cyber Strategy (**46**), the Republic for Ireland has the foundations to improve quickly.

Cyber Ready Index score by country



The average score for most countries puts them in the Reactive group, where **35%** of all businesses rated (the biggest overall group). Only India, the UK and USA rated as Developing readiness.

In their own words

Customer and regulatory expectations are key drivers

“

Customers generally expect there to be a high level of information security in place - certainly on the government and public sector contracts we have, it’s an absolute necessity. On some of the private sector contracts and the smaller government ones, then cost is a potential issue ... we don’t tend to play on the risky side, **we would rather lose a contract on cost than win a contract and be exposed.**”

Technology & Media, UK

Regulated industries understand the reputational risk

“

I think my business is quite cyber ready, because I work in a bank. I think banks have higher concern about security, because if any information is leaked, then reputation will be at risk.”

Financial Services, India

Budget is still a concern for many businesses

“

Budget is a constant challenge. They want us to cut it, cut it and cut it but technology is going up, up, up and up so **we have to try and constantly strike a balance ... security is something that we don’t budge on**; our stance on that doesn’t change.”

Not for Profit, USA

5.2 Cyber Ready by business size

Medium-sized businesses rate as the most Cyber Ready

Medium-sized organisations (249-999 employees) are most likely to be Cyber Ready, scoring an average rating of **50** out of 100 with **27%** being classed as Cyber Ready. Only **9%** were rated as having Basic readiness, the lowest across all businesses, while **6%** have Advanced readiness. They scored particularly strongly in Understanding Risk (**67**) and in having in place a solid Cyber Strategy (**56**). But despite their overall rating being high, their Digital Footprint score was well below the overall business average (**18 vs 24**) – potentially due to their broader use of different technologies and the challenges of managing a larger workforce.

Smaller businesses frequently lag behind

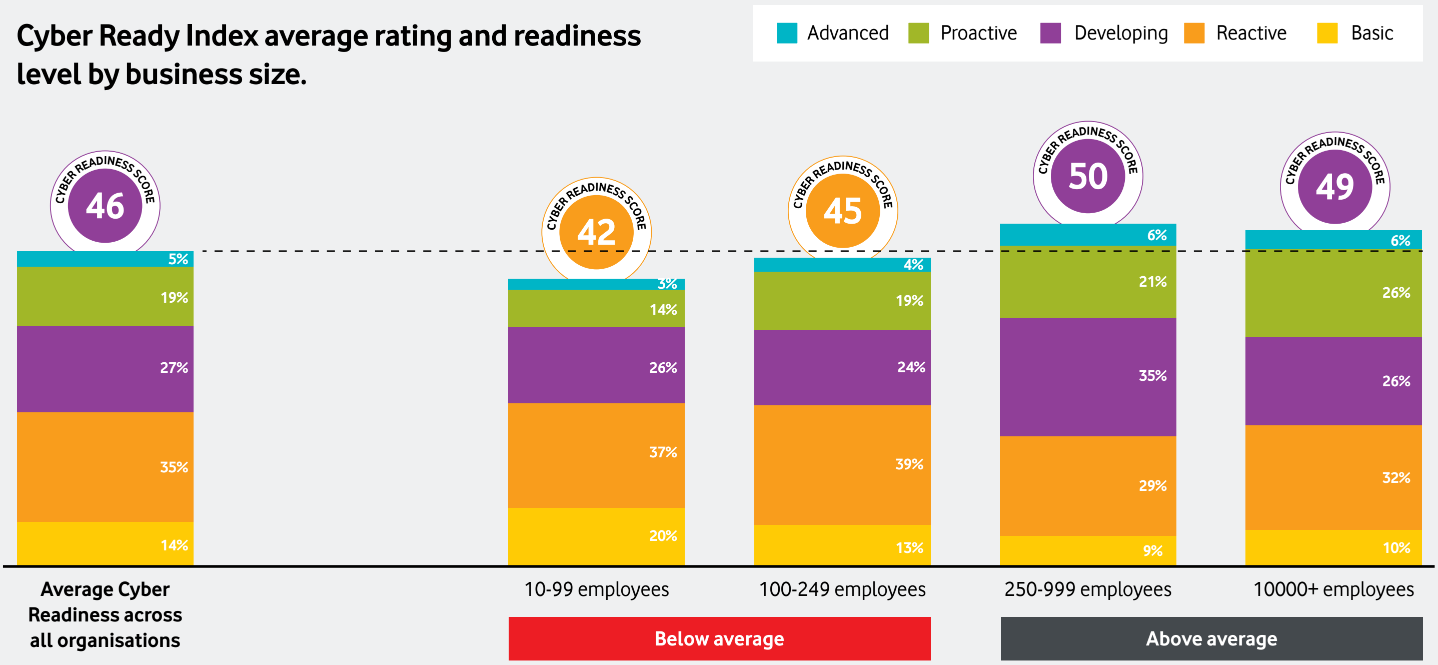
Smaller businesses (10-99 employees) proved to be the least ready with a below average Cyber Ready rating of **45**. Only **17%** of the smallest businesses qualified as Cyber Ready, with just **3%** of those classed as Advanced. Smaller businesses actually scored above all businesses in terms of understanding their Digital Footprint (**29 vs 24**), where perhaps they lack the complexity and challenges faced by larger businesses. Where small businesses were the least ready was in Cyber Resilience, where they were significantly below all businesses (**31 vs 44)**.

The largest businesses have headaches with their Cyber Operations and Digital Footprint

Larger businesses (1000+ employees) rated a slightly above average level of readiness, rating **48** out of 100. **32%** rate as Cyber Ready, the highest across all businesses, with **6%** showing Advanced Readiness.

They scored strongly in Understanding Risk (**63**), Employee Awareness (**57**) and Cyber Resilience (**53**) – but like medium-sized businesses they struggled to get to grips with their Digital Footprint (**18**), with heavier use of newer technologies such as cloud, combined with management and control across a widespread workforce likely to cause headaches if not effectively controlled and managed. Cyber Operations (**43**) also shows room to improve, with low confidence in their ability to protect their data and that their current investment in security (as a % of their IT budget) may not be getting the job done.

Cyber Ready Index average rating and readiness level by business size.



In their own words

Smaller businesses don’t always have security on the top of their minds

> “It’s not like we’re talking about information security all the time; it’s more on an ‘as and when it’s needed’ basis. It’s not a regular ongoing focus of discussion that we have.”
>
> **10-99 employees, Construction, USA**

Understanding the strategic importance of a reputation for good security in medium-sized enterprises

> “It is important that our customer knows that we as a company have a certain level of security that we can maintain ... that we can assure our customers that we are reliable and safe to handle their information.”
>
> **250-999 employees, Healthcare & Pharmaceutical, Germany**

Larger businesses are more likely to have plans in place – and have the resources to test them

> “We’re pretty high up there when it comes to responding to a cyber-attack. We’ve got more belts and braces, and the plan is tested regularly. We’ve always been pretty good at being able to respond to an attack – we’ve certainly been up there now in the last five or ten years.”
>
> **1000+ employees, Technology & Media, UK**

5.3 Cyber Ready by industry vertical

The Healthcare, Technology and Finance sectors are more 'ready' than others – while retail is struggling

When assessing the level of Cyber Readiness across all industries on the Index, several stand out as performing above average, notably the heavily regulated industries:

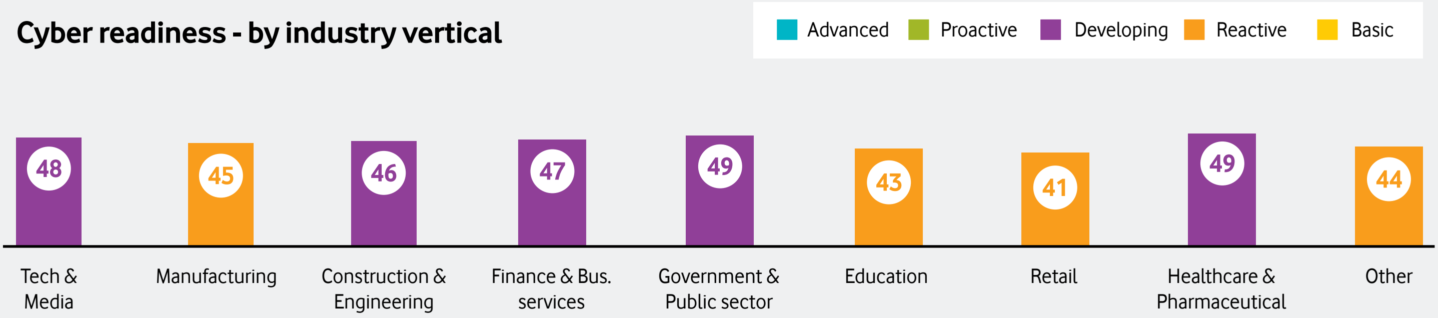
49	Healthcare	48	Public Sector
48	Technology & Media	46	Financial Services

Technology and Media companies in particular showed the highest awareness of GDPR legislation amongst respondents at **78%** and were also the most likely to have taken actions to comply with **54%** claiming to have done so.

However, despite their good overall rating, the Tech & Media industries struggle more than most with their Digital Footprint understanding with a very poor score of **13**, while Government and Public Sector have an excellent understanding (**54**).

Retail (**40**) was rated the least ready industry, performing poorly in Digital Footprint (**22**) and with further work to do in Cyber Operations (**38**) and Cyber Resilience (**40**).

Cyber readiness - by industry vertical



The expert view

> "This report does also align with the survey findings where Ovum sees many vertical industries investing more in security so they have more security maturity and therefore are more Cyber Ready. Financial Services and Healthcare were great examples of this investment difference. In many cases, security now is growing in importance with all customers, but these verticals had the budget to address them first AND had more critical assets to protect."

Mike Sapien, Chief analyst, Ovum

06

Divergent opinions – Businesses, employees and consumers

> “
>
> Workers expect empowerment. They are more choosy about their employment and its terms – demanding more flexibility in terms of when and where they work, how they manage their work and personal life and the technology they work with.”

‘Four key trends that will change your business’, Vodafone Trends Barometer 2018

6. Divergent opinions – Businesses, employees and consumers

Analysing the challenges and opportunities created by the divergence in cyber perspectives between business, the employees within them and the consumers they deal with.

To gain a more well-rounded understanding of the situation businesses truly face, we asked consumers how cyber security affects their lives and their buying decisions. For those in employment, we asked about their perception of cyber security in the workplace.

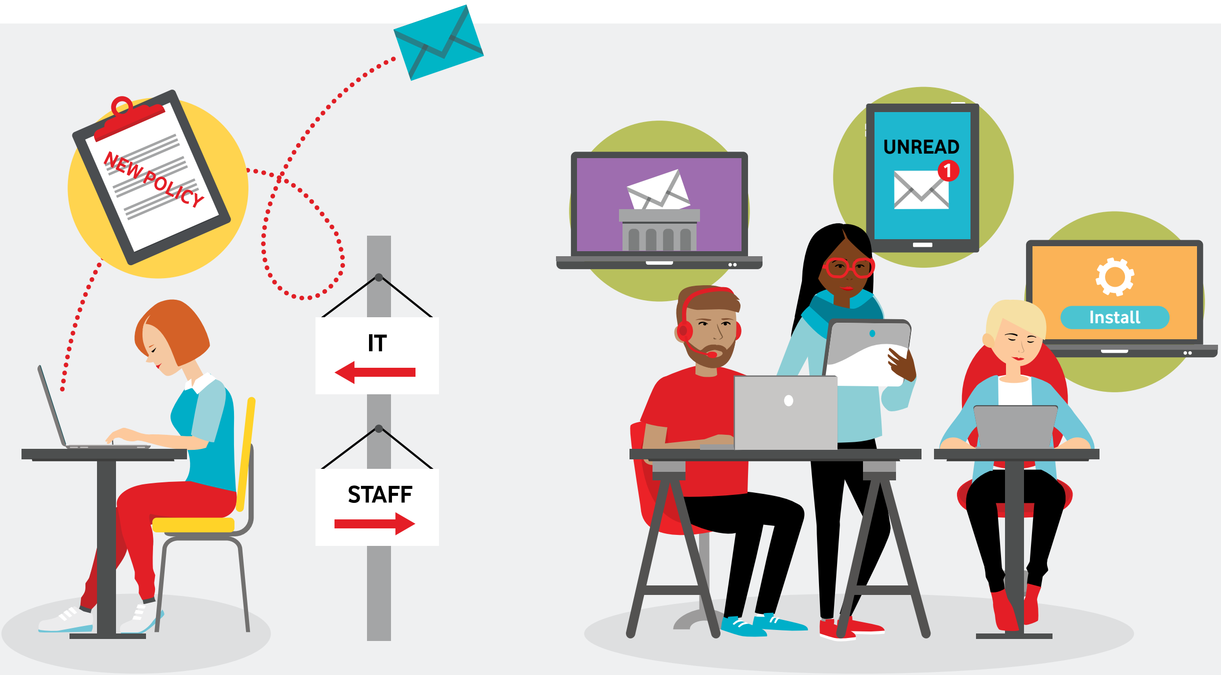
This provided an important comparison (and some interesting discrepancies) with how cyber security decision makers view cyber security within businesses of the same size and industry.

While only a quarter of businesses are truly Cyber Ready, there is significant opportunity to talk about steps that organisations can take to improve their readiness. This includes addressing key challenges with their people and a potentially missed opportunities with their customers.

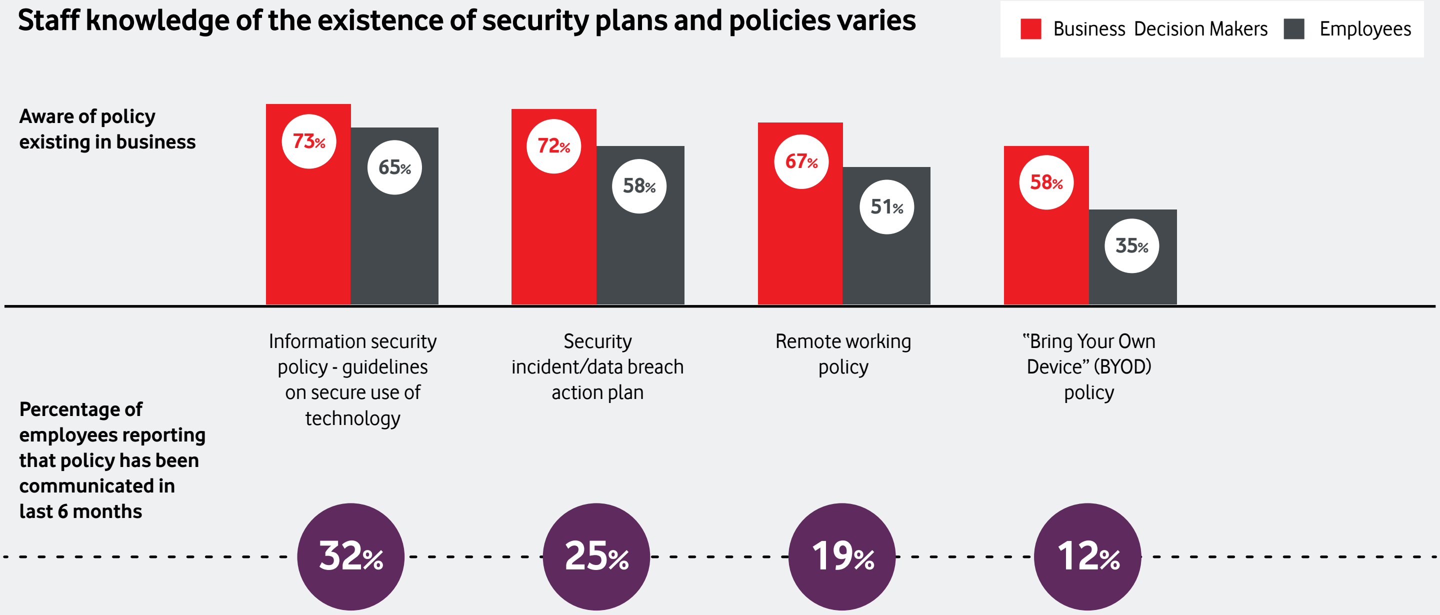
6.1 Employee engagement challenges – Friend and foe

When assessing how to improve Cyber Readiness, profiling a businesses' approach to employee engagement around security practices is essential. Employees are often cited as the biggest potential cyber security ally but also the potential weakest link.

The research identified several sharply contrasting viewpoints between cyber security decision makers and employees. These disconnects are potentially exposing businesses to greater risk and negating the effectiveness of cyber security measures.



Staff knowledge of the existence of security plans and policies varies



Low knowledge of policies, low compliance and high cynicism among employees can potentially increase business risks

Business and cyber security decision makers felt their organisations were performing strongly in terms of Employee Awareness (the average readiness score was **51** out of 100), with all of the appropriate security policies and training in place and understood by staff. However, when employees were asked about their knowledge of security policies it was significantly lower than expected by their employers.

This breakdown in the communication of security policies is especially concerning, with only half of employees (**51%**) aware of their business remote working policy and only a third (**35%**) aware of the BYOD policy. Even amongst those who are knew of the policies, only **19%** of employees were aware of having their remote working policy communicated and just **12%** remembered being told about the BYOD policy in the last 6 months.

The low levels of awareness and lack of (or ineffective) communications are also being exacerbated by low levels of security compliance amongst staff and businesses not providing mandatory security training for their employees.

47% **of staff reported that official policy or process is followed by all staff, with most reporting some type of "workarounds" being used.**

52% **of employees' report receiving regular and/or specific info security training.**

34% **of those who receive regular training say attendance is optional.**

Worryingly, roughly equal proportions of decision makers (**42%**) and employees (**39%**) agree that information security is just a "box ticking" exercise.

> "I know there are formal processes in place but I'm not sure I'm fully aware of the content. I'm there all the time but I'm not really aware of the details of the policies."

Employee respondent, Education, Republic of Ireland

In their own words

The employee disconnect

Cyber Ready companies tightly focus on the employee challenge

“The main challenge is people ... getting them to stick to the rules. Through HR and IT, we offer training to help equip them with the necessary cyber skills. We place a great deal of emphasis on being cyber-ready and so I would say we take the view that it is something that is compulsory and that everybody has to develop an awareness of it.”

Logistics, Singapore, 1000+, Proactive readiness

Less ready businesses are struggling to put measures in place

“The higher risk attacks now are the attacks which are disguised as valid emails and transactions that try to fool our staff into believing that they are valid ... we do have certain measures in place to combat these kinds of attacks but we can’t prevent our staff from clicking on a link or things like that all the time – we can only educate them so much.”

Wholesale, Singapore, 100-249, Reactive readiness

There is a disconnect between IT perception of working practices and employees reporting where they work and on what devices

One of the most startling contrasts between the cyber security and IT decision makers and employees was in the perception of the use of technology and working practices within their businesses. Although having a clear understanding of the business Digital Footprint was persistently scored as an area of low readiness on the Cyber Ready Index, the scale of the problem is perhaps worse than anticipated with significant gaps in understanding of what employees are using and where they are working.

Both employees and businesses were surveyed about the usage of various communications technologies and tools (smartphone, laptops, tablets etc.) and working practices (remote working, BYOD). The gaps were calculated by matching the company size and sectors of employees/businesses, then aggregating these findings across all respondents.

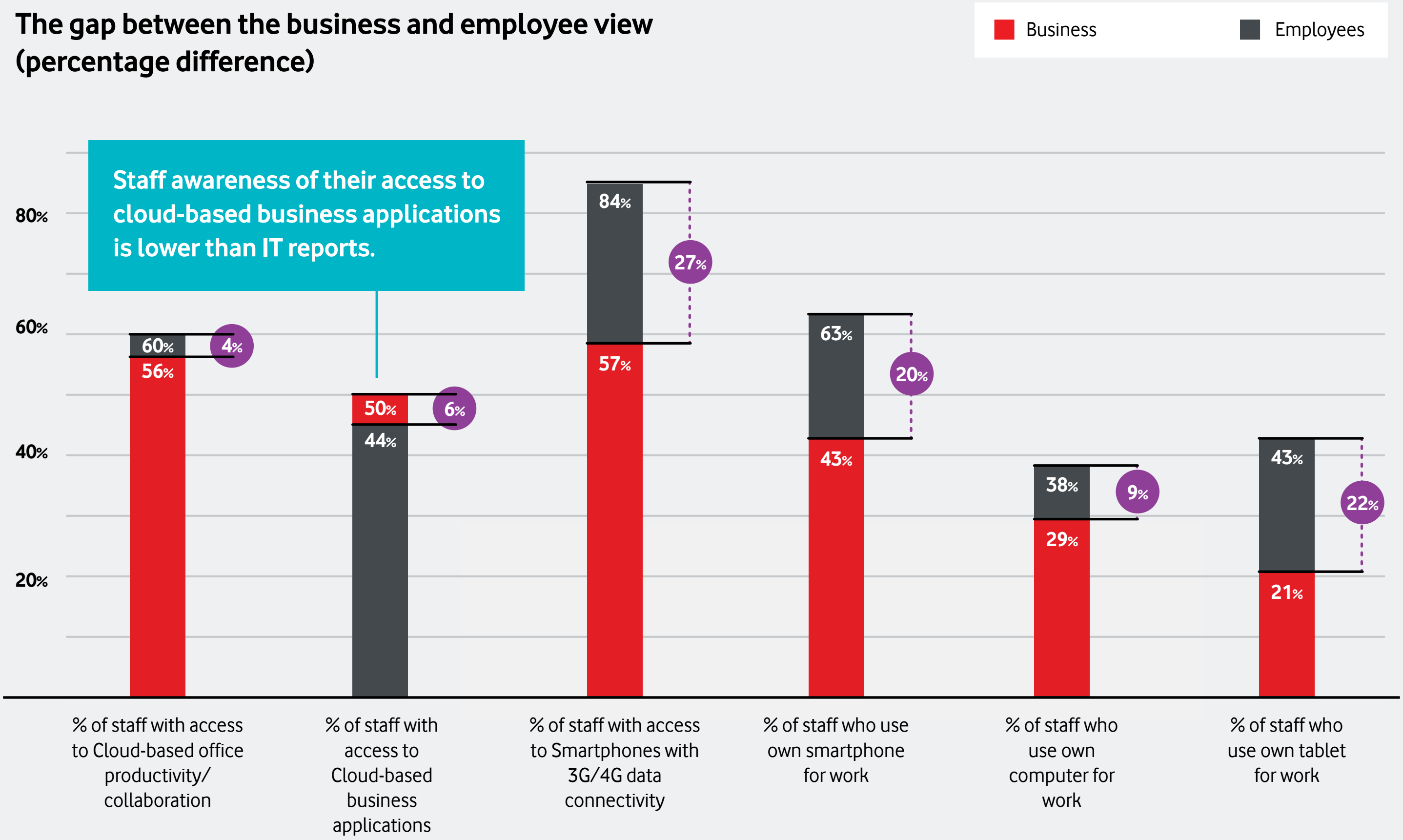
This highlighted some significant disconnects, blind spots and the potential for some unrecognised and unaddressed security risks.

- **46%** of businesses reported that they have remote working employees within their organisation. When employees were asked, **59%** reported that they sometimes worked remotely.

The proportion of staff who report using their own devices for work (BYOD), especially mobiles, is much higher than the perception of businesses:

- **63%** of employees use their personal smartphones, while only **43%** of decision makers believe they allow BYOD
- The discrepancy is similar for tablets, with **43%** of employees using their own against the decision makers' belief that just **21%** do.

The gap between the business and employee view (percentage difference)



Staff awareness of their access to cloud-based business applications is lower than IT reports.

Disconnect or differentiation?

Many businesses don't seem to have a clear understanding of these digital working practices and are therefore not enabling or securing them effectively. If people are the competitive differentiation in a digital economy – but your business isn't supporting or enabling them – you are impacting your competitive advantage and creating security risks. In response, organisations that are more Cyber Ready are likely to implement stricter no BYOD policies and ensure they provide the appropriate company devices:

> “We have a strong policy on that which means that we reduce the risk of exposure through employees using their own personal devices. Why expose ourselves to unnecessary risk? Employees who need to, can use company devices such as laptops and mobile phones.”

Logistics, Singapore, 1000+, Proactive Readiness

Less ready businesses see employee use of own devices as a significant threat, but especially smaller businesses understand it can be driven by frustration at the tools and services available to employees:

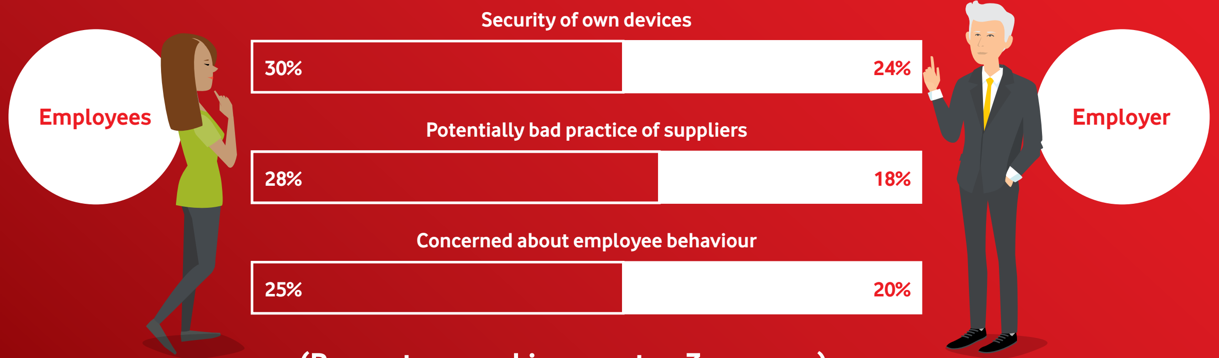
> “It's not encouraged, but we can't stop employees using their own devices. It's a grey area due to cost reasons. Not all the apps or software we provide give employees the full flexibility they need so some of them use certain outside apps and things like that to be more ambitious and effective. But since this is not part of the company software, we cannot ensure that all these apps are properly secure.”

Wholesale, Singapore, 100-249, Developing readiness

This disconnect, particularly in the use of personal smartphones and tablets devices for work purposes, highlights the challenges in securing a growing Digital Footprint in an area where security professionals already often lack resources and control.

Extra focus on strong identity verification and essential security controls across the organisation will go a long way to closing this gap.

Security priorities - employees are more concerned about staff and supplier behaviour than IT



(Percentage ranking as a top 3 concern)

Employers and IT decision makers perceive different challenges

When asked to rank what they felt were the biggest security challenges currently facing their businesses, decision makers and employees also held different opinions. There's common acknowledgement by both groups that ensuring data security is a major priority: 'Protecting sensitive company and personal data' was ranked as a top 3 concern by **40%** of businesses and **41%** of employees.

However, "on the ground" staff are disproportionately conscious of issues that might otherwise be hidden from management – namely the security of own devices and the potentially bad practice of suppliers (see chart above).

Both hold a perception of their businesses not being completely ready

One area where employees and business are aligned is in their perception of the majority that their companies are not fully prepared for the cyber security challenges they face – although employees actually held a higher regard for cyber security levels than the people in charge of it. **21%** of employees stated that they are very confident in the companies' ability to address all the top security challenges, compared to only **16%** of cyber security decision makers.

Businesses have some work to do to align their security policies with their employees' requirements and expectations

Businesses must work harder to gain employees trust and buy-in to their cyber security strategy. **42%** of employees view their organisations security policies as either a slight or significant hindrance to their efficiency – and this frustration is potentially what leads employees to adopt workarounds or use their own devices in breach of policy.

On the positive front for making improvements towards a creating a more Cyber Ready workforce, both employees and business recognise the importance of cyber security to the business and in terms of dealing with customers.

77% **of employees and employers agreed that 'Being confident in our security helps my organisation be ready for the future.**

80% **of businesses agree that 'Being secure is essential in our dealings with customers'**

85% **of employees also agree with that statement, possibly due to being at the sharp end of customer relationship management.**

Businesses need to ensure they get employees to understand that security is an issue and responsibility for everyone in the organisation, not just something for IT to deal with. Everyone needs to know what to do in the event of an attack or crisis in the digital workplace.

The expert view

The employee engagement challenge

“

Employee engagement in security remains a major issue and another smart area of focus for enterprises as there still remains many security breaches that can be spread, identified or curtailed by proper training of the employees in their use of corporate services and devices. One employee opening up an obvious phishing email can cause so much cost and disruption. Even with the best tools and services, employee training remains critically important”

Mike Sapien, Chief Analyst, Ovum

“

Being able to work with trusted access, from any place on any device, using applications in the Cloud or in-house, with simple user-friendly security controls, will be an employee expectation. Simple awareness and training will not suffice. The purpose and need for being Cyber Ready will need to be explained in the business context. This engagement will help to improve the overall employee attitude to being Cyber Ready going forwards.”

Richard Archdeacon, Advisory CISO, Duo Security

The expert view

The employee engagement challenge

“

Employees will often do the wrong things, for the right reasons. By that I mean we warn employees not to open suspicious emails, open unexpected attachments or click on links. However, we then provide security training by sending an email from an account outside of the corporate estate, instructing recipients to click on an unfamiliar link to find out more.

When factoring in the increasing trend for remote working and BYOD that result in further complicated guidelines, companies need to ensure they counter this employee disconnect by putting in place clear, simple and effective policies that don’t set out to demonise mistakes, but remove the obstacles that make cyber security difficult.”

James Hatch, Director of Cyber, BAE Systems

6.2 Cyber Ready Consumers – Putting a premium on peace of mind

Businesses perception of consumer attitudes to the value of security are lagging behind

Driven by the media and increased awareness of cyber, consumers feel at risk, look to the services providers for protection and will pay a premium as a result – something businesses can better capitalise on and Cyber Ready businesses are at an advantage.

Cyber security attitudes amongst consumers under the spotlight

When assessing the impact of security on business outcomes in 2017*, 89% of businesses believed that having a strong reputation for cyber security would enhance customer loyalty and trust. In the 2018 survey, **89%** of businesses still believed improving security would enhance customer loyalty and trust and **88%** felt it could create a better reputation within their market to help attract new customers.

To benchmark this, we surveyed over 3000 end consumers globally (employees respondents were also asked additional consumer-focused questions) to check their attitudes to cyber security from the companies they buy from and deal with – to see whether these aligned with businesses beliefs.

> “Customers are seeking to establish new trusted relationships and businesses are working harder than ever to build, and re-build, customer trust.”

Source - ‘Four key trends that will change your business’, Vodafone Trends Barometer 2018

Consumers feel under attack and are selective around who they deal with as a result

It’s clear that consumers acknowledge the severity of cyber security threats facing them – a third of consumers (**34%**) stated that the high profile attacks being discussed in the media has increased their awareness of the need for online security.

70% **of people questioned consider themselves to be at risk of a cyber-attack or online threat – with a quarter of people believing they are at significant risk**

66% **are very concerned about at least one security /privacy issue, such as Hacking of online accounts or Malicious software or viruses.**

67% **are very concerned about at least one privacy / online safety issue, such as Social engineering / phishing, Loss of personal data by companies, Use of personal data for ‘other’ purposes etc**

29% **agree that the number of threats to their online security is increasing significantly**

What’s more, consumers are acting on these concerns when choosing who to do business with and whether to conduct certain activities online. **63%** of consumers say they have avoided or stopped using at least one online service because of security concerns. Unsurprisingly, Financial Transactions (**55%**) and Communications & Data Sharing (**48%**) were most commonly what people were most worried about and had stopped using due to concerns. But interestingly Media & Entertainment (**40%**) and Lifestyle (**30%**) were also listed, showing security is a potential differentiator (or handicap) for businesses across a range of industries.

*Vodafone Cyber Security: The Innovation Accelerator report, September 2017

The majority of consumers firmly place the emphasis for protection at the service provider's door

While businesses exhibit increasing confusion over where to turn to for help in the face of highly complex security setups and multiple suppliers – consumers have a much clearer view.

When asked to list who bore the responsibility for managing information security and protecting them from online threats, **80%** of people listed the company providing the service as being amongst the top 3 culpable and **73%** felt it was the job of their internet and mobile data providers.

Digital opportunities & "monetising" security is a potential differentiator, but not an area where businesses yet feel they can make money

High levels of concerns amongst consumers are driving their behaviour when it comes to purchasing or using services:

93% **of consumers stated that the security of information held in online services they used was a significant consideration.**

59% **of consumers agreed that they are 'willing to pay extra for a higher level of security for the devices and services I use'**

43% **of consumers claimed not to trust the measures taken by companies they use**

So clearly, security is a key consideration in supplier choice and two thirds of consumers perceive better security as worth paying more for - in fact, **49%** expect superior security when paying for premium services. Meanwhile, almost half of consumers have little faith in the security of companies they currently use, leaving them ripe for being poached by a more Cyber Ready rival.

In their own words

Cyber security is a factor in consumer choice

“I would definitely consider looking at a company that had a reputation for providing strong cyber security services. It would come into my thinking, especially if you were doing something like changing your bank account. For example, there is a bank here that has a history of their accounts being hacked into and so I don’t think I would ever go near that kind of bank. Security is very important. ”

Consumer Respondent

Information security is a constant consideration; it’s at the back of my mind. If you’re buying something online you are thinking ‘OK well how secure is this site?’ I think if someone had a bad reputation, then that would dissuade me from considering them.”

Consumer Respondent

A reputation for providing a good level of security is a factor in terms of which providers I use.”

Consumer Respondent

Business attitudes need to catch up to concerned consumers

Meanwhile, businesses and employees are lagging behind consumer attitudes in the perception of the monetary value of security:

29% **of businesses see there are significant financial benefits from 'being able to charge a higher price for our products/services due to increased confidence of customers doing business with us'**

30% **is the discrepancy between consumers and decision makers who agree with charging more for better security**

24% **of employees agree that 'security is a significant benefit that helps us attract customers and win business'**

Security is a B2B differentiator

Security is essential and a potential differentiator when selling to or buying from other businesses. **61%** of employees with purchasing responsibilities at their company highlighted information security as being "very important" in supplier selection. And **69%** of decision makers agreed that they "are willing to pay for higher level of service for information security support" when choosing a partner or supplier.

The Cyber Ready opportunity

So for those companies who are highly Cyber Ready and can boast a reputation for strong security, there is the opportunity to use it externally to differentiate from less ready (or less aware) competitors and tap into the security conscious consumer market – while those who don't address their customers' concerns face a potentially high customer churn rate.

> "Cyber security is a positive thing in our company. That has been mentioned to clients as well. If you work with us, certain security is provided. We treat client information as confidentially as we can and we explain what solutions we can provide. In general, cyber security is a positive thing."
>
> **Employee**

07

About this report

> “Collaboration and knowledge sharing is critical in building cyber defences. To this end, Vodafone’s Cyber Ready Barometer will be useful for various stakeholders including businesses, government, cybersecurity professionals, and security software vendors.“

Dr Emma Slade, Lecturer in the Department of Management, University of Bristol

7. About this report

Read the Vodafone view on the report findings, how you can use this report to become more Cyber Ready and find out more about the research methodology and our contributors.

7.1 The Vodafone View

This report has identified that the majority of businesses today aren't Cyber Ready and 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. We highlighted three areas that we feel businesses should pay attention based on the findings:

1. Resilience is key and must be improved

In today's climate, a business will now be judged on its ability withstand multiple and ongoing cyberattacks, while continuing business operations. It's important not just to focus on preventing attacks, but also 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 people component of security and consider their 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 business operates.

You need to understand both partner and consumer views too. Businesses want to deal with companies offering assured security, 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.

What should you do with this report?

Use it to improve your security posture – The Cyber Ready Index 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.

Use it as provocation to understand your employees views on security – Are they 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?

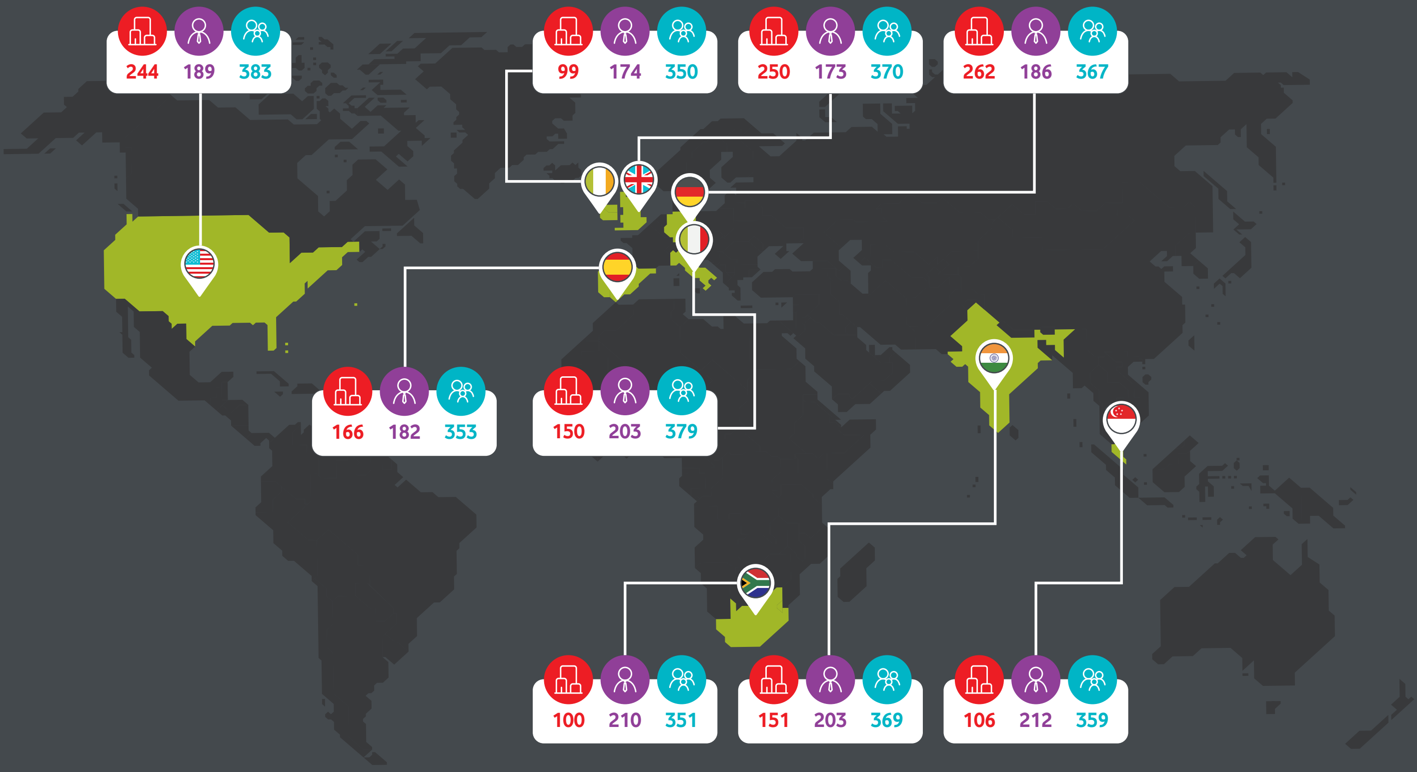
Use it to understand your customers – How sensitive to cyber readiness are your partners, clients and citizens? If you understand how they use and think about security, you'll understand how to position your business to circumvent challenges and uncover opportunities.

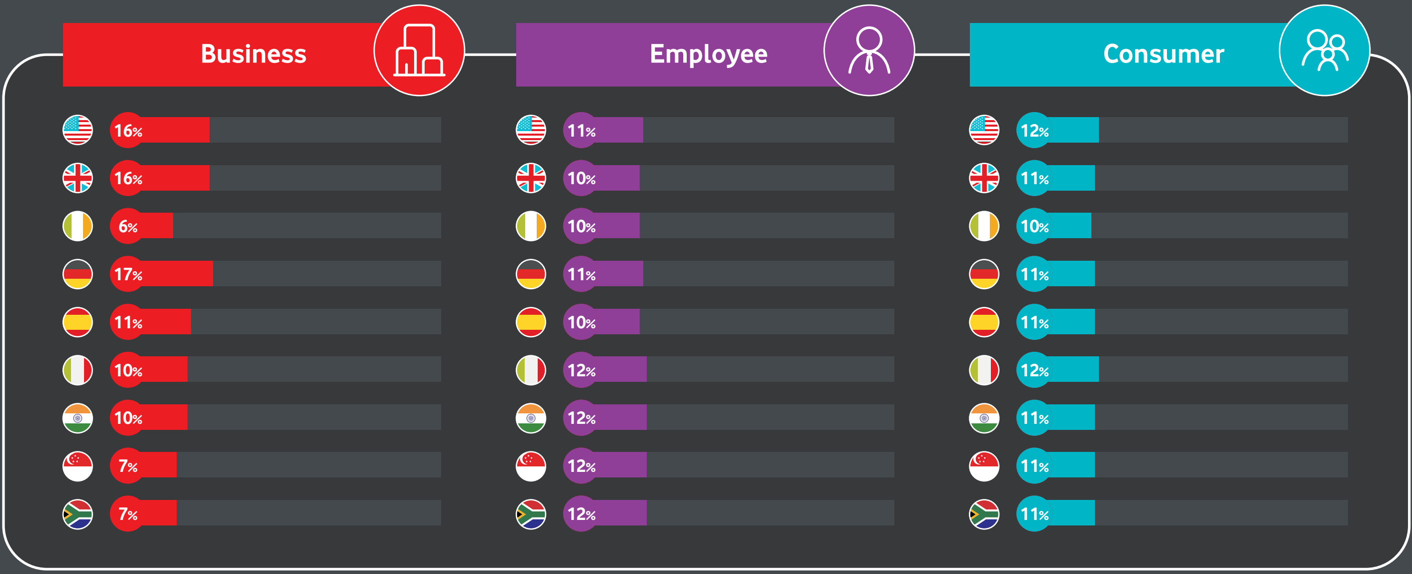
If you have any questions about these findings - or how you can enhance your own Cyber Ready initiatives, please contact us at cybersecurity@vodafone.com.

7.2 Research methodology

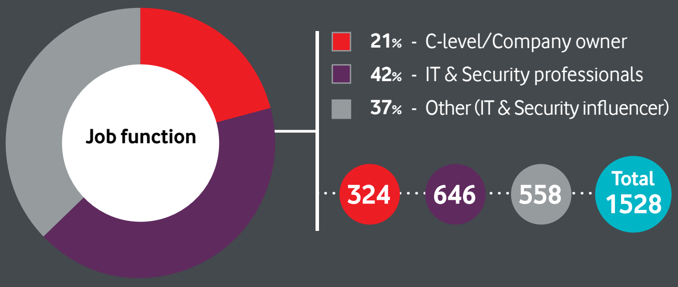
In April 2018 as part of a global security study, Vodafone interviewed **1,528** cyber security decision-makers and influencers in businesses and the public sector, and **3,281** combined employees and consumers, in nine countries around the world. This research was the foundation of this report.

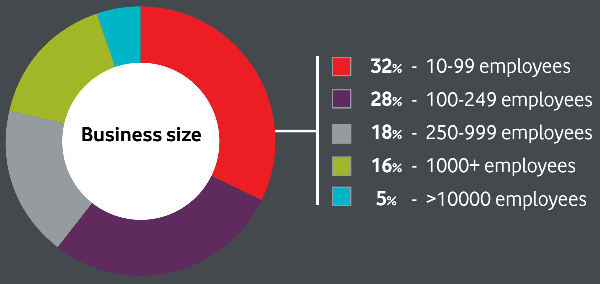
All respondents by country

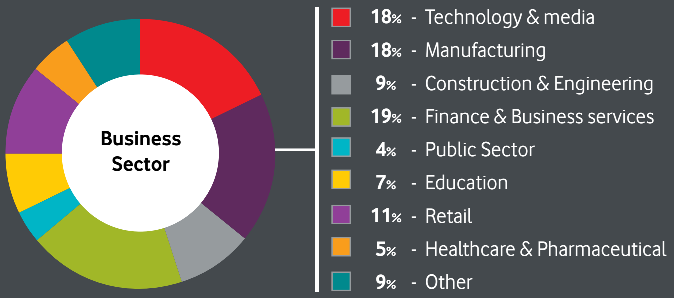




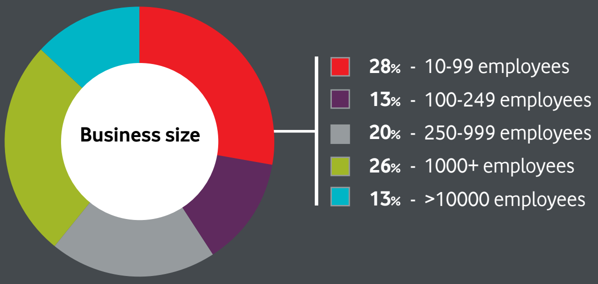
Split of business decision maker respondents

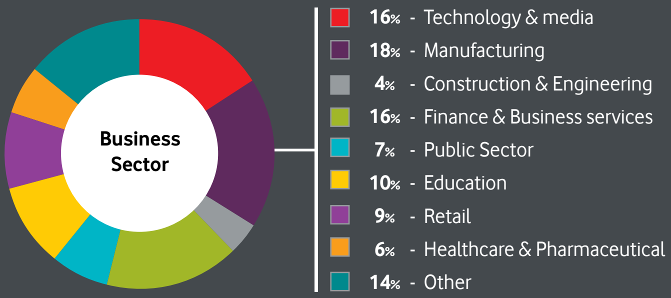






Split of employee respondents' employers





Methodology

We conducted interviews online, and these have been supplemented by in-depth telephone interviews.

We interviewed qualified IT and security decision makers/influencers at manager level or above, working in all sizes of business and across multiple sectors. In larger businesses, these are dedicated IT or IT security leaders. In smaller businesses, they are more commonly those who run the business.

We defined the 1,732 employee respondents as those working in companies with 10+ staff, in the same vertical sectors as the business survey and they also had to use technology or digital devices as part of their job role on at least a daily basis. The consumer group were general citizens who didn't meet the employment criteria.

- All figures have been rounded to the nearest 1%.
- This report describes the findings from the research, supplemented by Vodafone's perspective and commentary from a panel of cyber security industry experts.
- A range of comments from these businesses are included in the report. As the subject matter is often sensitive, we have provided appropriate levels of anonymity for the respondents.
- This is the second annual cyber security report by Vodafone, having launched in 2017.

7.3 Contributors

In addition to our Vodafone experts, we have worked closely with a team of industry experts from a range of countries and functions to provide their valued additional perspective on the research findings in this report.

We thank them for their contributions and insight.

External contributors

Mike Sapien

Mike Sapien is a Chief Analyst at Ovum. Mike tracks the areas that are of importance to global large enterprise customers and complex managed services. He also provides analysis of the networking, security, and enterprise mobility requirements of these large customers globally.

Ovum is a market-leading research and consulting business focused on helping digital service providers and their vendor partners thrive in the connected digital economy.

www.ovum.com

Piers Wilson

Piers Wilson has over 20 years of experience in cyber and information security at Huntsman Security, IISP, PwC and Insight Consulting. He is Head of Product Management at Huntsman Security and Director of the IISP and has worked across most sectors and at all levels in consulting, service and product businesses.

www.huntsmansecurity.com

Colin Robbins

Colin Robbins is Nexor's Principal Security Consultant, a company specialising in secure information exchange. He is a fellow of the Institute of Information Security Professionals, a NCSC Certified Professional and Chair of the East Midlands Cyber Security Forum.

www.nexor.com

Dr Emma Slade

Dr Emma Slade is a Lecturer in the Department of Management at the University of Bristol. Her research and teaching interests revolve around digital technologies and consumer behaviour. She has published her research in numerous internationally recognised journals and is also an alumnus of CHERISH-DE's Digital Economy Crucible funded by the EPSRC.

View Profile

Dr Emma Williams

Dr Emma Williams (CPsychol, CSci, AFBPsS) is a Vice-Chancellor's Fellow in Digital Innovation and Wellbeing within the School of Psychological Science at the University of Bristol. She researches human aspects of cyber security and cybercrime, primarily in organisational settings, and has published her research in several highly-regarded international journals.

View Profile

Randolph Kent

Randolph Kent currently holds the role of Director - The Futures Project at The Royal United Services Institute (RUSI). RUSI is the world's oldest independent think tank on international defence and security.

www.rusi.org

Richard Archdeacon

Richard is the Duo Advisory CISO for the EMEA region. He was previously with DXC - HPE - where he was a Chief Technologist in the Security Practice working with clients across all industries and regions. Prior to that, he worked for Symantec. He has also contributed to security industry organisations such as IAAC, ENISA and the IISP.

www.duo.com

James Hatch

James Hatch is Director of Cyber Security Portfolio at BAE Systems Applied Intelligence. He leads a diverse cyber security business covering cyber intelligence, security advisory and technical services, managed security services and government security programme.

www.baesystems.com

Vodafone contributors

Maureen Kaplan
Vodafone Enterprise Cyber Security Lead

Andrzej Kawalec
Group Head of Enterprise Cyber Security Strategy & Innovation

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