

EXTERNAL REPORT

Fit for a Secure Future

Why cyber security is about more than staying safe.

July 2023



vodafone
business

CONTENTS

	Foreword	03
01	Background	06
02	The findings	08
03	Conclusion	25
	Methodology	29

FOREWORD

Today's businesses operate in a fast-paced, hyperconnected world, where they need to intelligently connect data, people and things in order to run seamlessly. This environment is the perfect breeding ground for cyber attacks, making them a major concern for businesses of all shapes and sizes.

If businesses are to safely accelerate their operations, embrace new technologies and change the way they work, it's crucial they have robust cyber security measures in place.

Our research has uncovered that many businesses don't have adequate safeguards in place to protect against cyber attacks. In fact, over 65% of businesses still don't believe they'll be affected by a cyber security incident, despite recent Omdia research showing that 91% of security decision makers have dealt with a security incident in the last year – which is a staggering amount. Businesses need to start looking at cyber security measures as if they were brakes on a car – not because we need to slow down but, quite the opposite, they provide the necessary control and security that enable us to drive faster while minimising the risk to our journey.

So, what's the first step? It's all about the planning – businesses need to have a clear cyber security strategy in place. After all, you wouldn't set off on a journey in your car without knowing where you want to get to, what you're going to need along the way and how much it might cost. This strategy should be built into the foundation of the business and needs

to be adopted by all stakeholders and employees. People are not only the most important part of the strategy but can also be the weakest link in your defences, so developing a cyber-aware culture within the business and a plan designed with people at the core will be crucial to driving success.

Having strong cyber security measures in place also fosters trust – a critical component for success in today's hyperconnected world. Just as passengers in a car trust the driver's ability to apply the brakes when needed, customers, partners and stakeholders trust businesses that prioritise their cyber security. It creates a sense of assurance that their data, privacy and sensitive information are safeguarded, building long-lasting relationships and credibility. And should an incident occur, businesses will need to rely on these trusted relationships and close collaboration with suppliers and partners to overcome a breach, quickly and effectively.

Businesses should be investing in cyber security solutions that offer real-time threat detection, rapid incident response and continuous monitoring. These capabilities provide the necessary confidence to navigate the ever-evolving cyber security landscape, just like a skilled driver relying on the responsiveness and reliability of their brakes to confidently manoeuvre through challenging road conditions with precision.

However, it's important to remember that cyber security is not a one-time implementation; it's an

ongoing process of maintenance and improvement. Like regularly inspecting and maintaining the brakes of a car to ensure optimal performance, businesses must continuously assess and strengthen their cyber security defences. This includes educating employees, updating software, conducting vulnerability assessments both internally and throughout their supply chains, and staying informed about emerging threats.

Our research also shows the broader value of cyber security and that it can enable much more than just protection. Just like a car equipped with high-performance brakes can confidently navigate curves and reach higher speeds, businesses with strong cyber security defences can embrace innovation and drive forward with greater agility. Effective cyber security acts as a protective barrier, enabling organisations to swiftly adapt to changing work models, implement new technologies and achieve enhanced productivity. Businesses that fully embrace a holistic approach to cyber security can benefit from new and exciting opportunities, and can enjoy a genuine competitive advantage.

Fit for the Future (FFTF) businesses do just that – not only are they prepared and can respond quickly and effectively to cyber security incidents, but our report reveals that having a clear strategy and the right measures in place allows them to seize new opportunities and deliver growth.

This report will demonstrate how FFTF businesses grasp the importance of cyber security, enabling them to drive faster and achieve success. They take a proactive approach to protecting their business, planning ahead to ensure they're ready for anything. And just as reliable brakes instil confidence and enable high-speed driving, robust cyber security measures empower these organisations to innovate, adapt and excel in today's digital era. So, buckle up, secure your 'brakes', and enjoy the journey towards a safer and more prosperous future.



Andrzej Kawalec
Head of Cyber Security,
Vodafone Business

INTRODUCTION

In recent years, cyber security has climbed high up the business agenda. Today, even those organisations that once considered cyber attacks “something that happens to others” now realise that they, too, are vulnerable.

To help mitigate the risks, every organisation must take a proactive approach to cyber security – whether they’re in the private or public sector, or a not-for-profit. Only then, can they successfully navigate today’s challenging business environment and be on the front foot. They can be more responsive to market demands, collaborate seamlessly, and safely develop new products and services.

FFTF businesses already embrace this thinking; they have both a defensive and innovative mindset when it comes to cyber security. Alone, cyber security is not a differentiator. It is a baseline that organisations must achieve to be able to operate. Without effective cyber security, organisations cannot be resilient, and resilience is key to businesses progress and growth.

As customers, we expect the organisations that we engage with to be available constantly. We also expect them to provide ever improved ways of delivering engagement. At Omdia, we term this ‘digital resilience’ – it is the ability to continuously operate and quickly leverage digital opportunities. Cyber-resilience is a key component of digital resilience, ensuring that the organisation can continuously operate despite security challenges.

Thus, FFTF businesses are both digitally resilient and cyber-resilient. They take a proactive approach to cyber security in full recognition that doing so will encourage their customers to trust them. This is far from an on/off switch, however.

With a proactive mindset towards cyber security, organisations can help minimise and manage cyber threats. This means they can remain continuously available to their customers, which helps build trust and loyalty. Although very few customers actively review security breaches by companies that they engage with, if a breach is

brought to their attention – for example, via the press – then trust can be damaged, if not lost altogether.

The proactive mindset for cyber security helps build customer trust in a different way. It enables organisations to develop new and better models for engagement – this might be products or services – and deliver those new capabilities, so that they are available quickly and they work. Private sector businesses want customers to spend with them rather than anywhere else, so the organisation must be innovative in bringing new products and services to market at pace. Other types of organisations have different drivers but, nevertheless, must also be innovative in order to meet customer expectations.

A strong cyber security foundation is vital for resilient innovation. Without it, customer engagement and trust could be damaged when launching new products and services.

Investing in cyber security can result in the organisation being more competitive in the market and serving its customers better. Not investing in cyber security leaves the organisation more vulnerable to outages, unfavourable headlines, fines and more – all of which damages customer trust. FFTF businesses take the first option – investing in cyber security – to deliver growth.



Maxine Holt
Senior Director,
Cyber Security Research



THE IMPORTANCE OF BEING FIT FOR THE FUTURE

In 2020, we set out to discover which businesses are prepared for the future, what they're doing differently to other businesses, how they approach different challenges and how they fared during the pandemic. We conducted qualitative and quantitative research across 10 markets globally in 2019 and 2020 and during the research there were six characteristics that correlated most clearly with businesses – we called these businesses 'Fit for the Future' (FFTF).

Over the past few years, we've analysed these businesses against different challenges spanning different industries, countries and business sizes and we found that FFTF businesses showed a very different approach to these challenges compared to other businesses.

We also partnered with the London School of Economics (LSE) to develop a model that found that – for those businesses currently reporting average financial performance compared to their competitors – if they were to increase their 'fit for the future' score by 10 points, there would be an increase in the likelihood of outperforming their competitors financially by 36%*.

In addition, businesses that increase their 'fit for the future' score by 10 points can also expect to have an Environmental, Social and Corporate Governance (ESG) commitment that's six points greater*.

In this report, we examine how FFTF businesses manage their cyber security strategies and how that contributes to the success of their business.

*Relative increases based on a self-reported assessment.

What common characteristics do FFTF businesses have?

1

Positive attitude to change
They see change as an opportunity and are excited by the future.

2

Open to new technology
They understand the power of technology to solve their business challenges.

3

Plans for technology
They have roadmaps in place for how technology can transform their ways of working.

4

Detailed strategies
They have wider business strategies for the future that are documented, specific, funded and measured.

5

Up to date with emerging trends
They work to understand the forces shaping their business and they get help from key thought leaders.

6

Adaptable
They can react quickly to new trends or challenges and are quicker to market than other companies.

01

BACKGROUND



FFTF BUSINESSES ARE BETTER PREPARED

This has been a decade of incredible technological advancements. The pandemic, in particular, accelerated changes to both the way we work and how we do business. These are exciting times, but new technology brings with it new cyber security risks.

A lack of confidence

Businesses of all shapes and sizes worry about whether they are prepared to meet the challenges brought by the rapid implementation of new technology. Our research shows that many are struggling to cope with disruption to their procedures and are growingly concerned they won't be ready for what's to come.

FFTF businesses are proactive towards cyber security

FFTF businesses see investing in cyber security as more than simply protecting data and assets. They know that if they get it right, processes can be streamlined and infrastructure modernised, to help drive growth. The key is to take a proactive approach, getting on top of cyber security before it becomes an issue. Clear planning is the route to success, ensuring cyber security meets their specific needs without becoming prohibitively expensive. To be fit for the future, businesses need to be ready for anything.

“If we were exposed to a cyber attack, our clients would be compromised and reluctant to work with us. The financial impact of cyber security is something that we have calculated.”

FFTF Professional Services company in South Africa

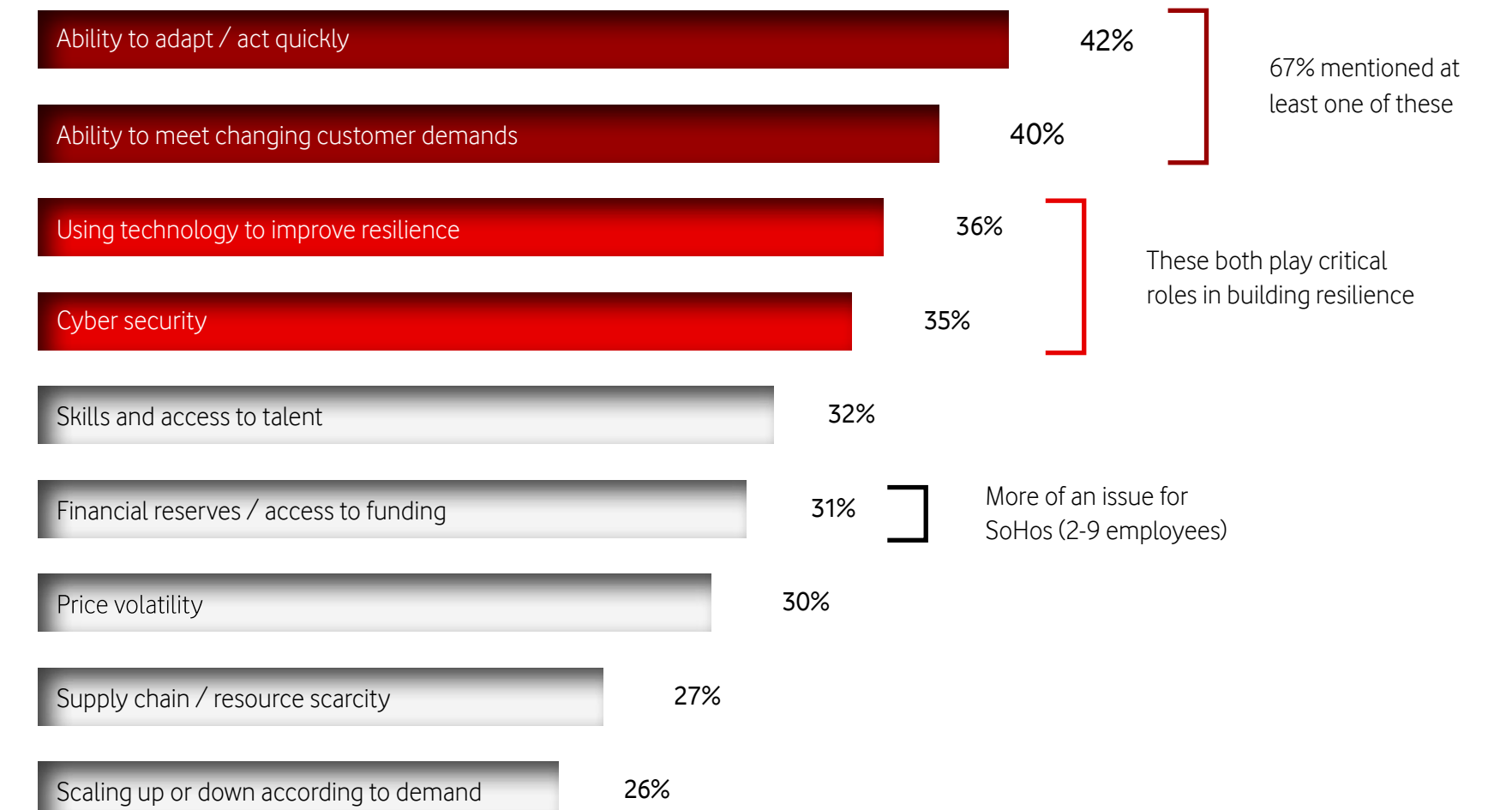
53%

of firms report coping well when a business disruption has occurred in the last 12 months

37%

of SoHos (2-9 employees) report coping well

Ways in which organisations need to become more 'resilient'



02

THE FINDINGS



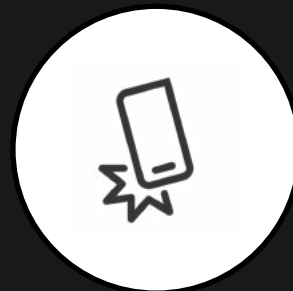
THE TOP 5 CYBER SECURITY CHALLENGES FOR BUSINESSES

Cyber security is a key area of focus for businesses as they embark upon another period of unpredictability. But cyber security itself is a vast topic that covers many things.

Through our research, we've dived deeper into the subject to uncover the five biggest cyber security challenges.

**1**

Ensuring all company and personal data is safe

**2**

Securing all business devices, wherever they're used

**3**

Securing cloud activity

**4**

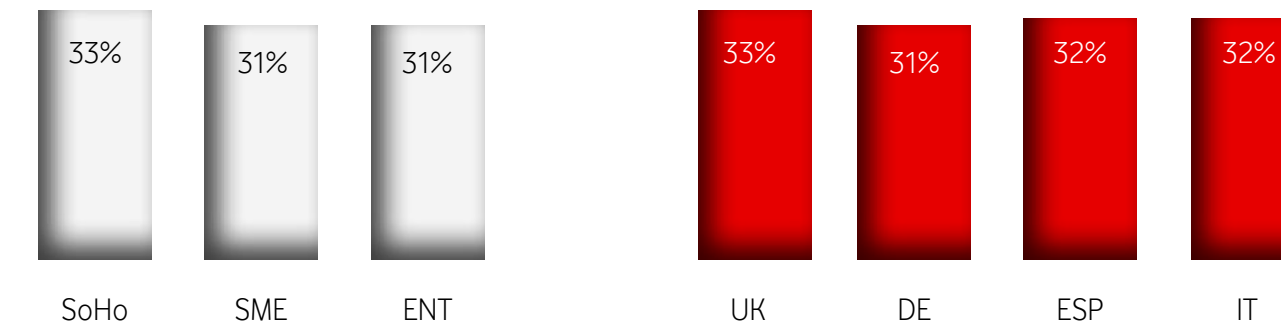
Responding quickly and effectively to security incidents

**5**

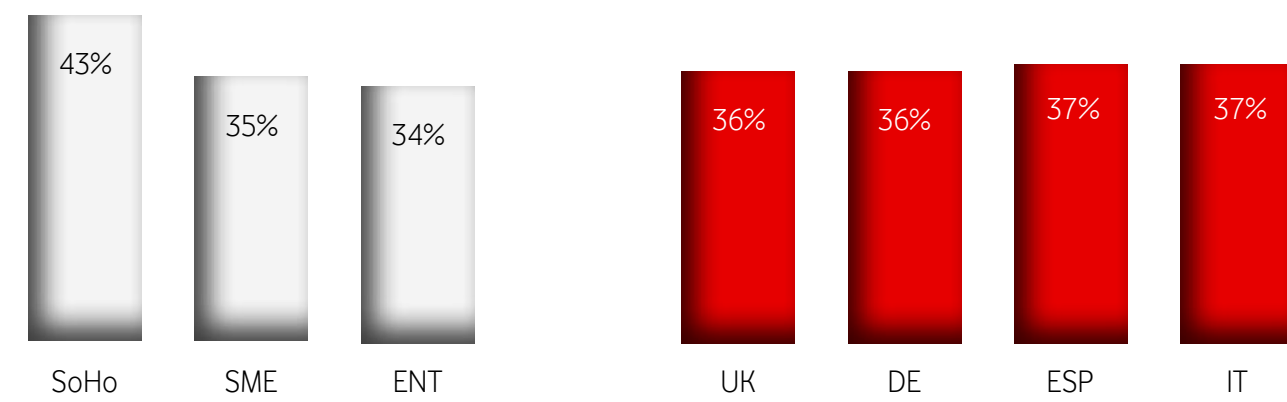
Making sure systems and data are only accessed by authorised users

According to Omdia research, around two thirds of security breaches involve data exposure and with data breaches on the rise, mitigating the impact of a breach is a big challenge for businesses. Some data breaches can cause irreversible damage, losing customers, harming brand reputation and compromising competitive advantage. And with more data, now spread across more devices, it's more vulnerable than ever.

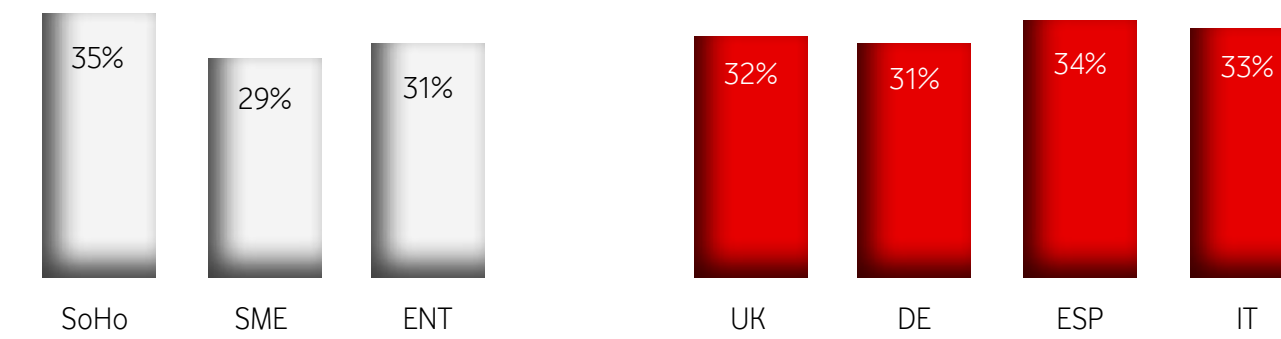
Security in the cloud



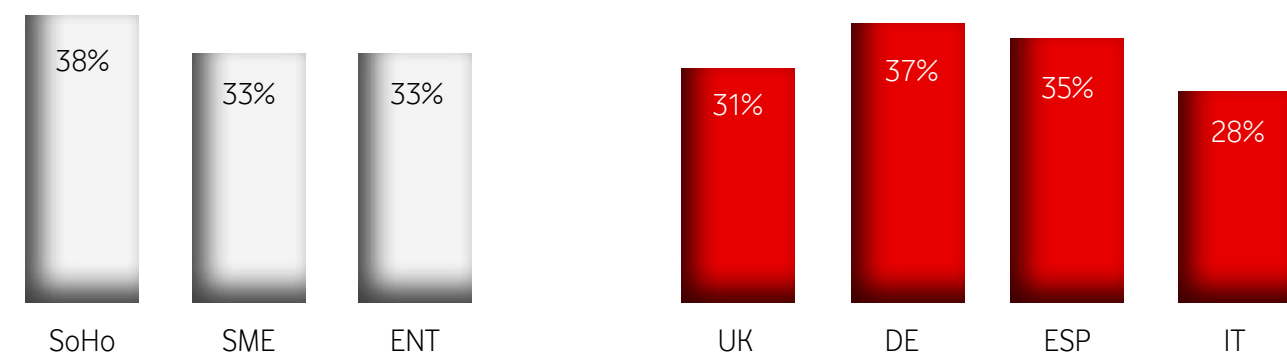
Protecting sensitive company and personal data



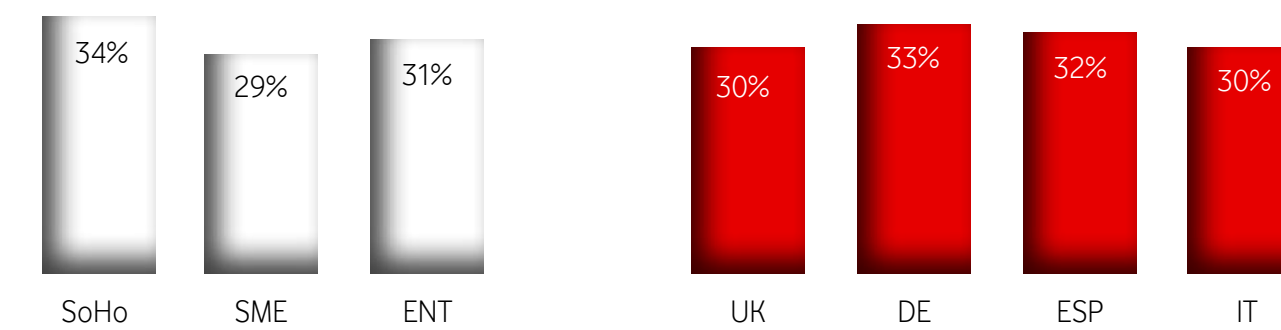
Responding to security incidents, quickly and effectively



Securing the many different devices used across the business



Ensuring that only authorised people have access to systems



Business size Key markets

NOT ALL BUSINESSES ARE REALISTIC ABOUT CYBER SECURITY

According to Omdia research:

91%

of security decision makers have dealt with a security incident in the last year

and

47%

of these were classed as severe incidents

In spite of these figures, only

33%

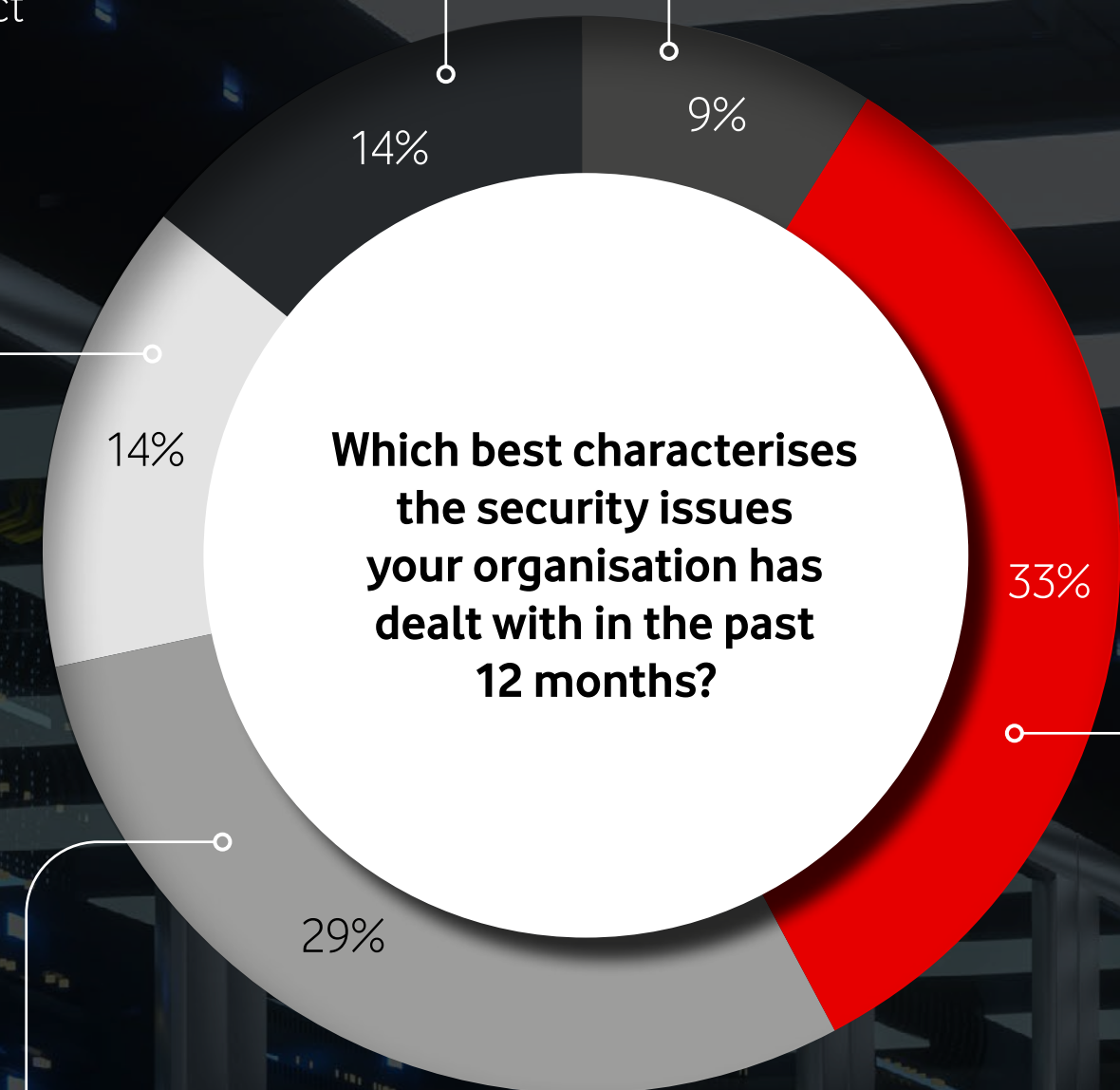
of businesses believe they will fall victim to a cyber attack

This clear disconnect highlights the increasing importance of educating and aligning all business stakeholders behind a cyber security strategy to ensure resilience for the future.

FFTF businesses take a more realistic view of cyber security risks and recognise that the severity of cyber security challenges is increasing.

Several security mishaps with limited impact

No security issues



Numerous severe security incidents with material impact to the organisation

Numerous security mishaps with limited impact

Several severe security incidents that required meaningful escalation

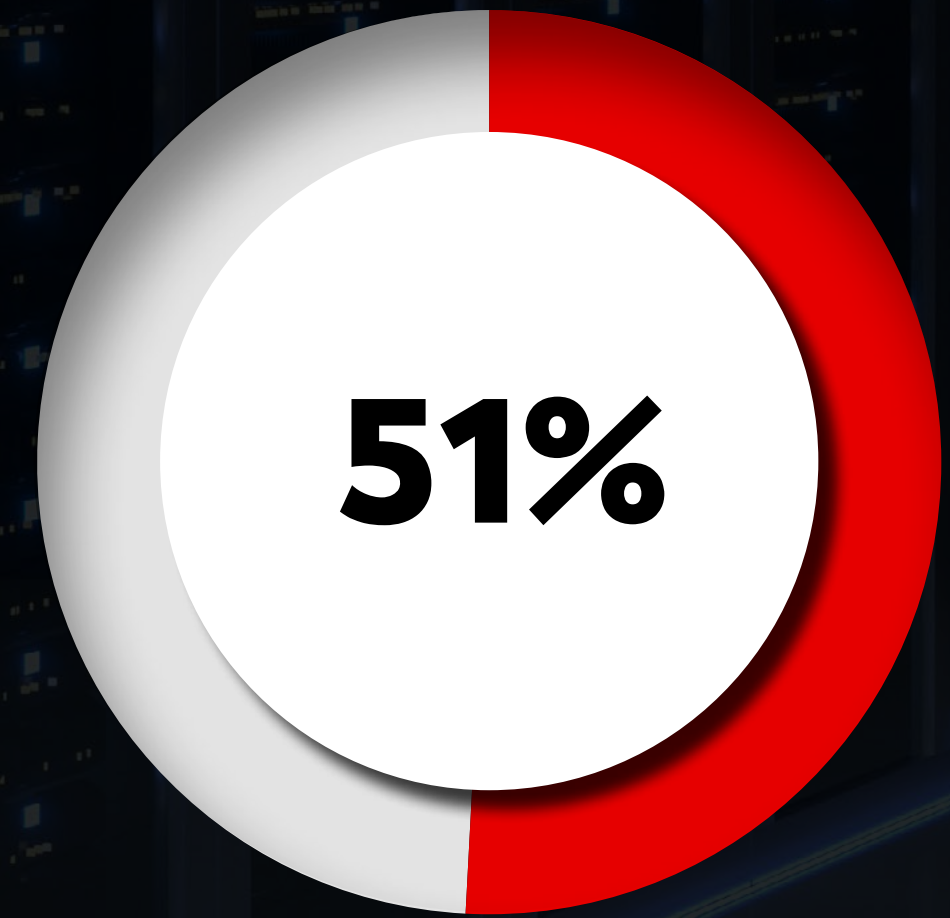
Perceived severity of cyber security challenges: % Growing (somewhat and significantly)



Declining significantly

Top 3 drivers of increase

- 1** Ability for cyber-criminals to make money from attacks
- 2** Easy access to tools to commit attacks
- 3** Perceived lack of punishment



of large enterprises perceive the severity of cyber security challenges to be growing, a significantly higher proportion than both SMEs (45%) and SoHos (38%)

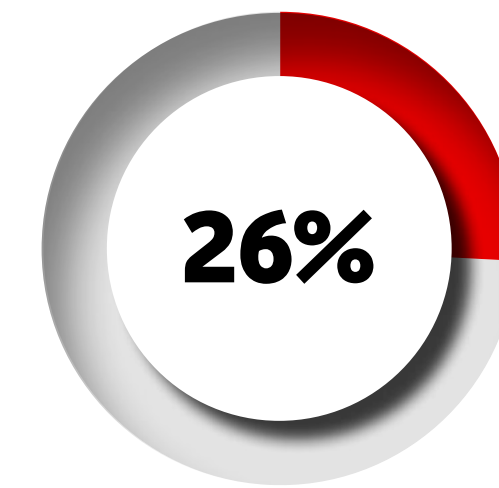
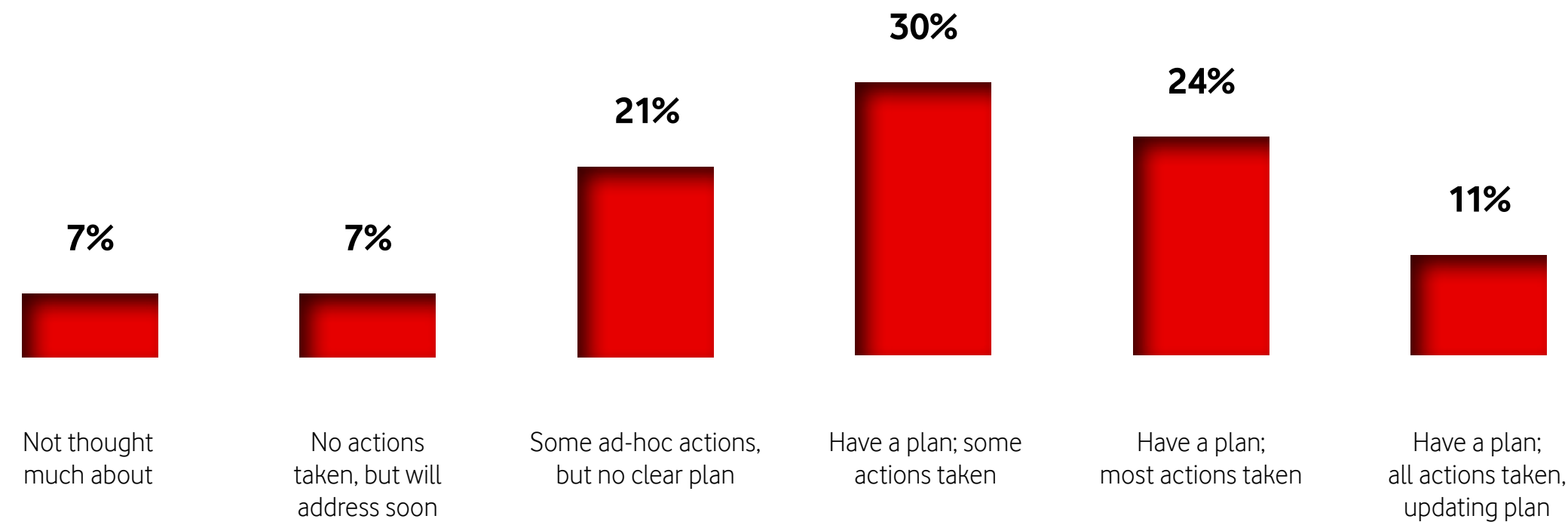


FFTF BUSINESSES ARE READY FOR THE UNEXPECTED

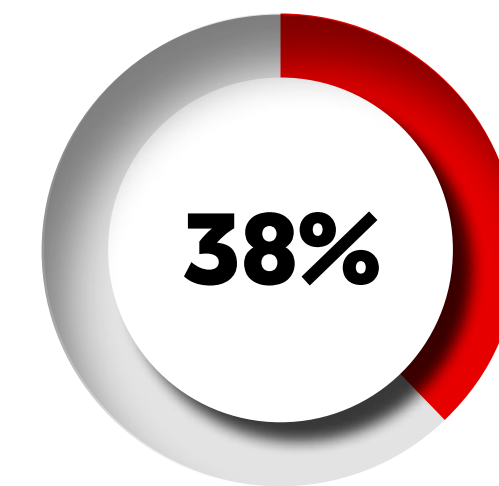
58% of FFTF businesses have clear cyber security plans and have taken most, if not all, of their planned actions – a significant increase on the figure of 35% of businesses overall.

As our research has shown, this willingness to prepare is part of the reason why FFTF businesses are more successful – they see comprehensive cyber security planning as a way of unlocking the potential of their business, rather than simply a way of protecting themselves.

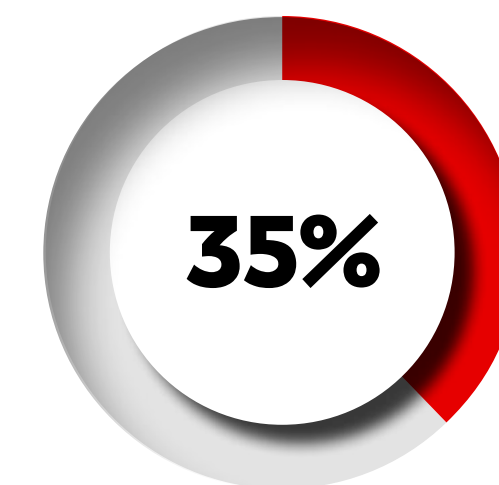
Cyber security: Self-reported maturity level



Have a regularly tested and updated security incident / data breach action plan



Currently engage third-party breach response and forensics services*



Have a clear plan for cyber security and have taken most of their planned actions

*A retainer-based, rapid incident response service to guide organisations through cyber crises

TURNING A CHALLENGE INTO AN OPPORTUNITY

Businesses have never been more connected than they are today. However, the vast, hyperconnected ecosystem that brings them all together presents both challenges and opportunities.

On one hand, it opens businesses up to more cyber threats. On the other, it enables flexibility, collaboration and innovation.

With the right cyber security strategy, businesses can embrace these opportunities while also protecting against the threats. As a result, they can become more agile, boost productivity and also build deeper trust with their customers. Ultimately, they can gain a competitive advantage.

This is what sets FFTF businesses apart. While most businesses are aware that cyber security can help prevent data breaches and mitigate the risks posed by security incidents and breaches, FFTF businesses can see further than that. When it comes to cyber security, FFTF business also think about preparation, they take a holistic viewpoint, they make the right investments for their business and they see cyber security as a way of boosting growth.

We'll now discuss five ways in which businesses that get their cyber security right can thrive – and how FFTF businesses are in pole position to take advantage of the opportunities it can bring.



CYBER SECURITY HELPS FFTF BUSINESSES BE MORE AGILE

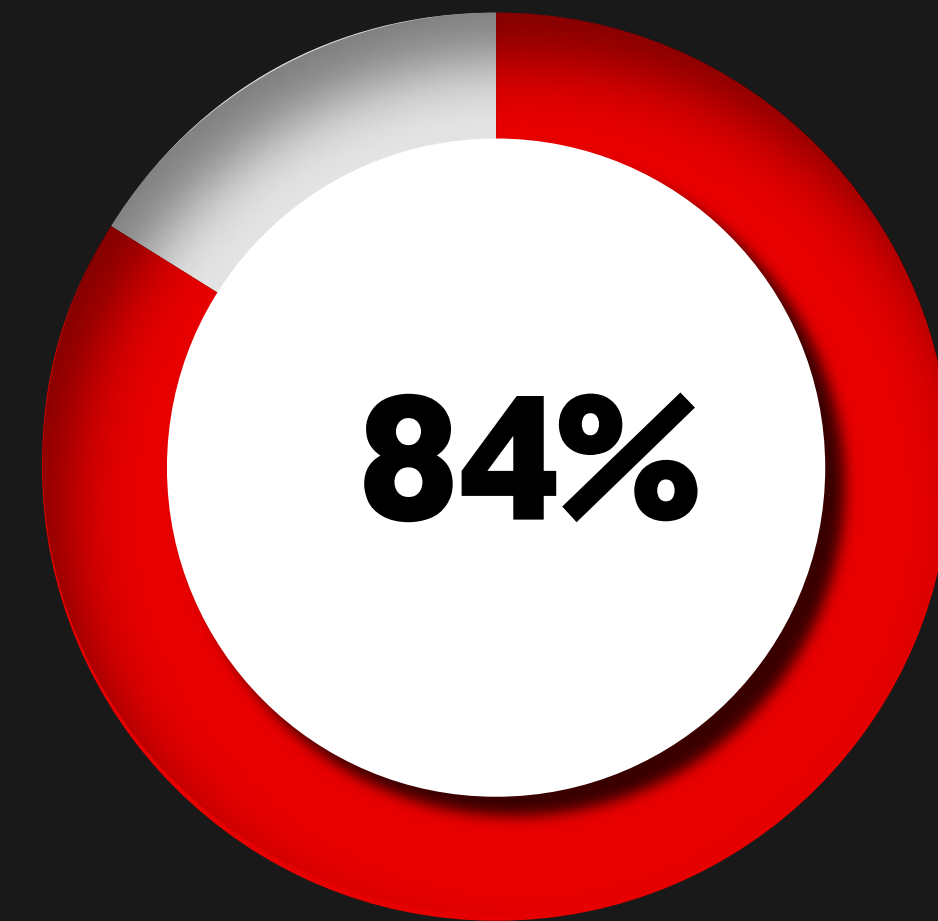
Operational agility allows businesses to evolve and adapt to shifting customer expectations. And FFTF businesses tend to be able to respond quicker to new challenges. Why? Because they take a more holistic view of their market and plan ahead, so they don't have to start from scratch when things change. 75% of FFTF firms strongly agree that their 'business embraces change, rather than trying to resist it' (vs. 46% for non-FFTF).

Standing still is not an option

According to Omdia research (Omdia IT Enterprise Insights survey, 2022-23), 53% of enterprises believe security, identity and privacy are crucial to a business becoming successful – and 61% of businesses consider themselves to be advanced or well advanced on this journey. A constant drive to innovate is also important, with 40% of the same organisations identifying this as a key task.

Security boosts agility

Businesses are constantly striving to deliver the speed and agility required to remain competitive and successful. This includes staying in tune with market dynamics, competitive pressures, new technology and evolving threats. By integrating the right cyber security measures throughout their processes, businesses can be more agile, responding quickly to ever-changing market and customer needs. FFTF businesses are more agile than their competitors, with 44% of FFTF firms seeing their company as strongly overperforming for 'ability to respond quickly to new trends or challenges' (vs. 11% non-FFTF).



84%
of FFTF businesses feel they are making rapid progress in terms of 'being quicker to market' (vs. 37% for non-FFTF)

▲
1
2
3
▼



“We have regular simulation testing exercises. We engage board members, senior management, and production staff in this simulation testing. We have external accreditation, and we conduct ‘lessons learned’ concerning any major incidents. We derive as much [cyber] intelligence as we can: I think this idea of being intelligence-led is important. If you can monitor for any abnormal behaviours, and then adapt to those changes, it’s going to give you a competitive advantage.”

CISO, Manufacturer, UK, 1k-5k employees (FFTF)

HAPPIER, MORE PRODUCTIVE EMPLOYEES

Employee expectations have transformed in recent years. Today, people expect to be able to work fluidly across devices and locations. Robust cyber security enables employees to work more flexibly – and get more done. By offering a frictionless user experience, businesses can boost both employee satisfaction and productivity.

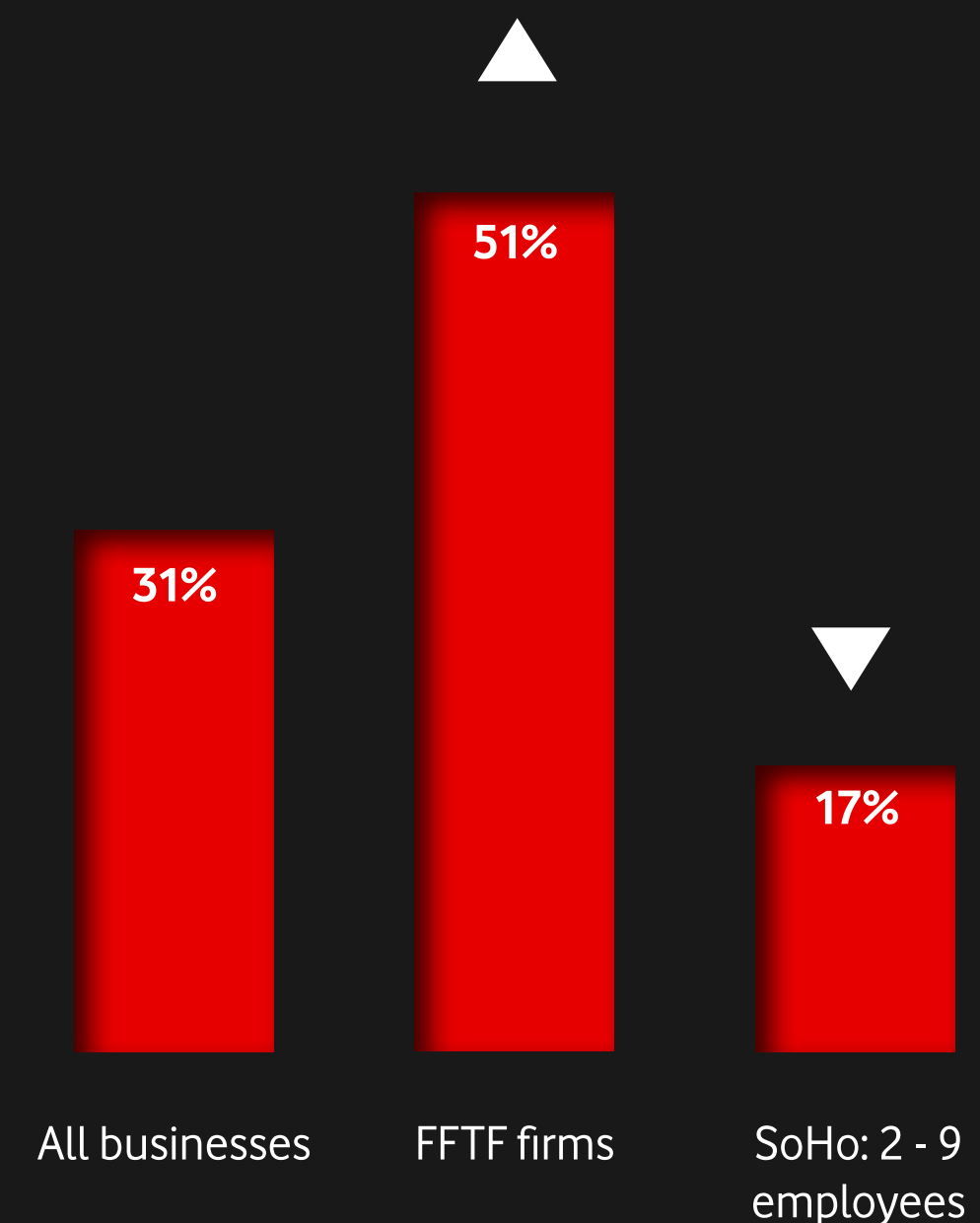
Addressing concerns around hybrid working

Although hybrid and home working have become the norm, it can still be difficult to ensure only authorised users are able to access critical systems. In fact, many non-FFTF businesses – particularly smaller firms – struggle to identify who is really using their systems. By contrast, the majority of FFTF businesses have checks and measures in place to verify the identities of the people using their systems, regardless of the type of device they're using or where they're logging in from.

Prioritising regular, effective upskilling and training for employees

When developing cyber security strategies, it's important to think about the right tools and processes. However, one area that's often overlooked but is without a doubt the most important, is people. Omdia's Cybersecurity Decision Makers Survey 2023 shows that 42% of organisations list employee security training failures as a top three challenge for the security function.

By implementing a robust and regular training programme, you can ensure that your employees are always up to speed on the latest threats, company policies and business procedures, which in turn, could help to limit the potential cyber security risks you may face. Businesses need to focus on improving the attitudes and skills of all employees around cyber security to strengthen the 'human firewall'.



% of organisations that are 'very well prepared' for checking and verifying the identity of those using their systems, wherever they are.

ATTRACT THE BRIGHTEST TALENT

The pandemic prompted people to reassess their priorities – and their work-life balance. Employees now place increasing value on work being fulfilling. They want the opportunity to grow and learn, and they want to work in flexible, diverse workplaces. At the same time, digital transformation is having a significant impact on the skills that businesses need.

Earn employees' trust

The right cyber security measures can help businesses adapt, allowing them to concentrate not on where work happens, but how it happens. To enable people to work in a connected, trusted and secure way from anywhere, businesses need to adopt intelligent and adaptive security controls that focus on the individuals, not the location or infrastructure. And this, in turn, can help businesses retain their talent.

Our research found that where employees have 'very high trust' in their employer's cyber security, those companies are significantly more likely to overperform against competitors for 'attracting and retaining the best employees' (66% vs. 40% where there's a low level of trust among staff). Furthermore, 69% of firms that have completed most of the actions in their cyber security plan feel that they overperform against competitors when it comes to 'attracting and retaining the best employees' (vs. 47% for everyone else).



HARNESS THE POWER OF EMERGING TECHNOLOGY

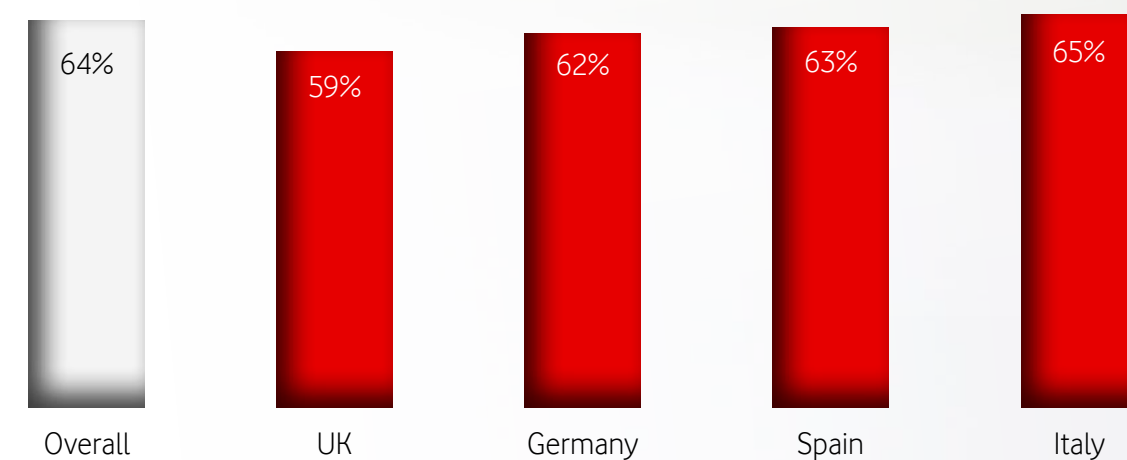
Being quicker than rivals to adopt new technologies such as IoT, AI or edge computing can give businesses a competitive advantage. But new technology can also highlight security weaknesses. Indeed, emerging technology is considered the biggest security risk for large enterprises.

An open-minded approach to business

Effective cyber security can help businesses embrace new technology with confidence. It enables them to create, innovate and personalise products safely. FFTF businesses recognise the benefits of introducing new technologies but they're also aware of the risks – this allows them to move forward quickly, but securely.

The new technologies that businesses agree require the most investment to resolve security concerns are:

VR/AR products and services

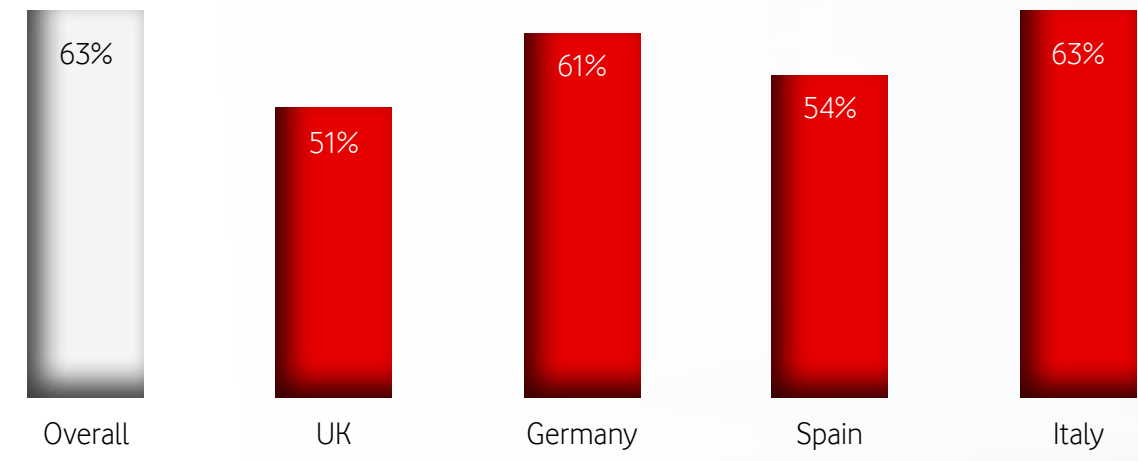


“Data security is an important topic – there has to be an understanding that data saves lives. More data in the health sector leads to better diagnoses, therapies and outcomes.”

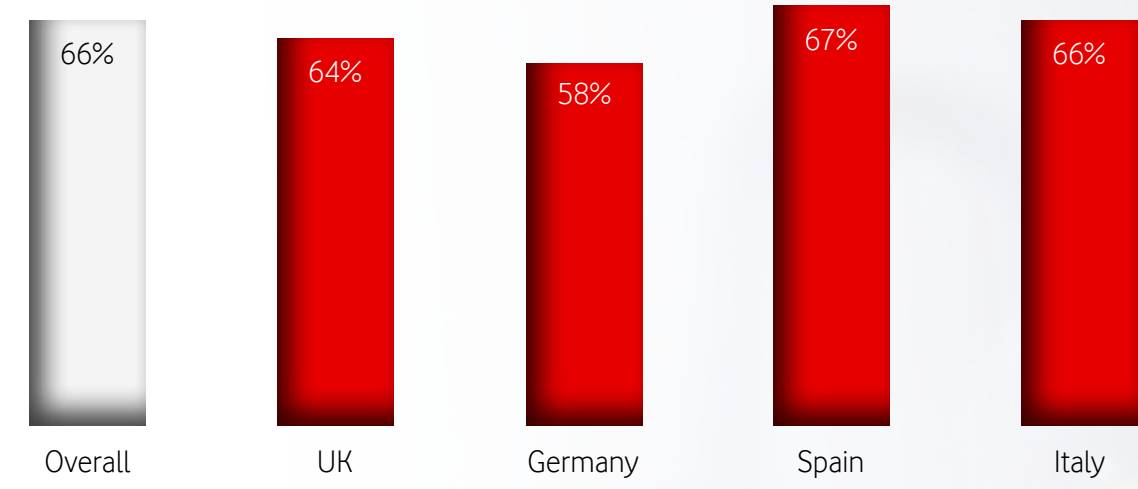
FFTF Healthcare organisation in Germany



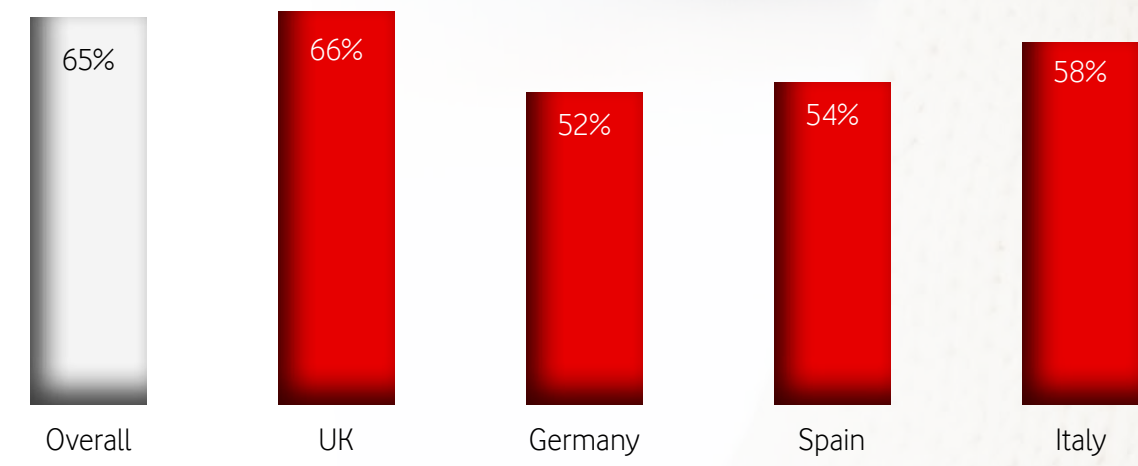
IoT solutions



Multi-access edge computing (MEC)



ML/AI technologies



Overall Key markets

- ▲
- 1
- 2**
- 3
- ▼



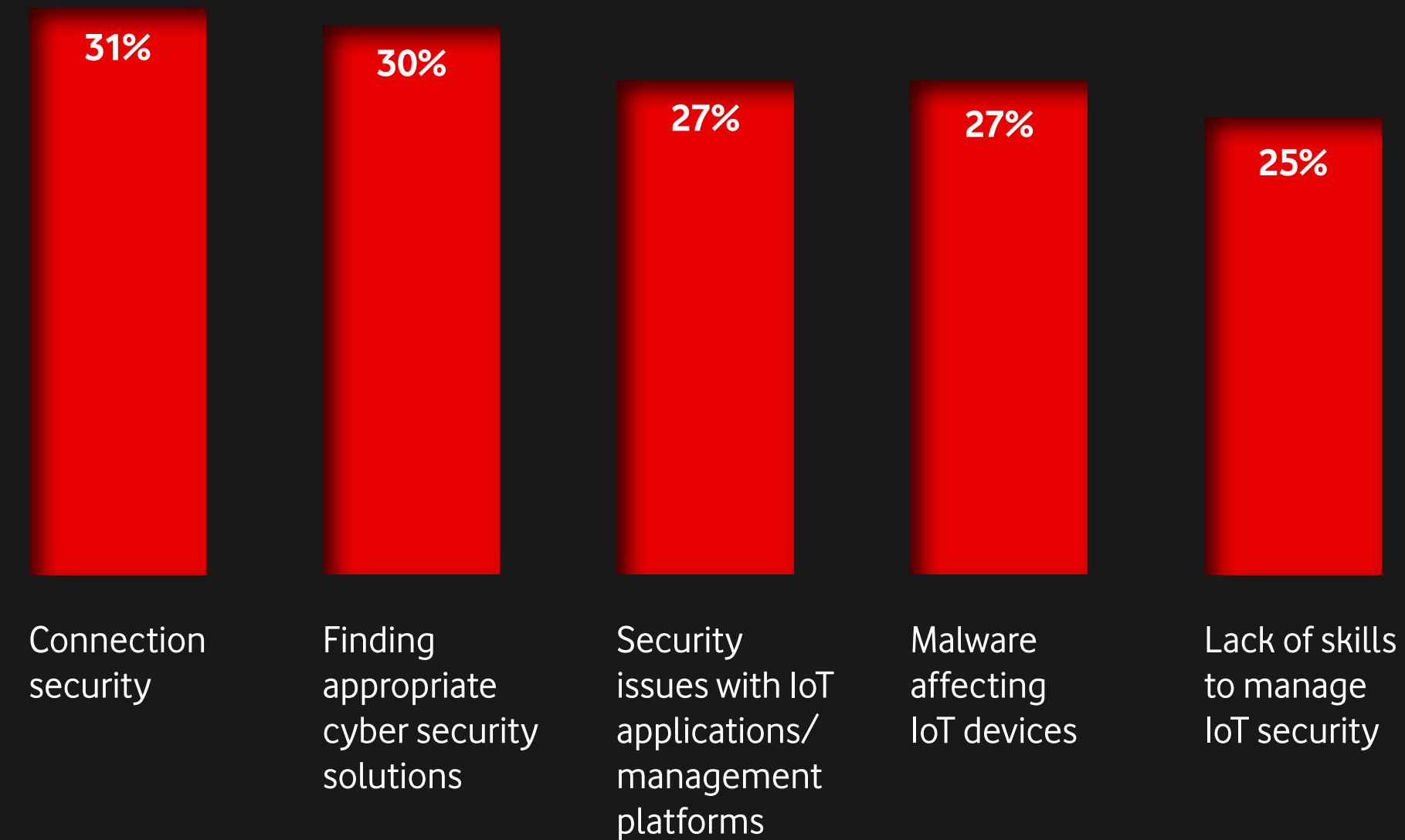
UNLOCK THE POTENTIAL OF IOT

In spite of the incredible potential of IoT, many businesses are still put off by the possibility of cyber threats. In fact, 32% of businesses said this is the biggest barrier for them adopting/considering IoT – making it the top reason, even above the expense of implementing IoT devices.

Common misconceptions

According to Omdia research (Omdia Cybersecurity Decision Maker Survey, 2022) the most common concern businesses have regarding IoT cyber security incidents is IP/financial theft. But these are, actually, far less common than ransomware, malware and data breaches. It's important that businesses have access to accurate information before adopting new technology, and it's here that FFTF businesses' comprehensive planning sees them get a fuller picture, allowing them to address any issues that arise and move forward with confidence.

Top 5 specific IoT cyber security challenges encountered



FFTF businesses recognise where they need help

Employees increasingly accessing cloud systems from a variety of devices and locations is an area of concern for businesses. Most businesses know they need to do more to make them less vulnerable in these environments. Our research shows that FFTF businesses are the ones taking action, and are more likely to use regular testing and assessment services to keep them secure.

Cyber security fuels innovation

65% of firms that have implemented most of their planned cyber security measures feel they're making rapid progress in terms of 'being more innovative than the competition' (vs. 45% that haven't implemented their plans, or don't have a plan at all).

Cyber security really is about more than just protection; it can help businesses drive innovation.



of firms versus 53% of FFTF businesses with cloud technologies use vulnerability assessment services*



of firms versus 43% of FFTF businesses with cloud technologies use penetration testing services**

*Services that assist with the identification and correction of flaws in the configuration/patching of technology that could be exploited intentionally or unintentionally

**Ethical 'hacking' / attack simulation exercise conducted to assess cyber security capabilities



BUILD CREDIBILITY THROUGH ROBUST CYBER SECURITY

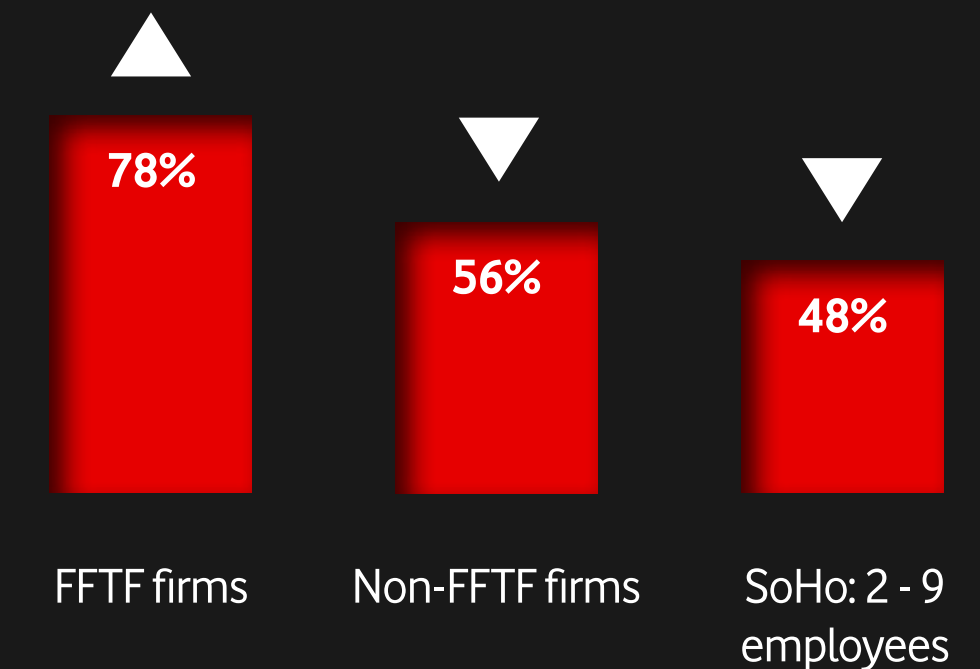
If customers trust a business, they're likely to stay loyal. Data breaches and other cyber issues can be hugely damaging from both financial and publicity perspectives. Hard earned trust can be lost in an instant. So, businesses that are secure can enjoy a real competitive advantage over their rivals, maintaining customer loyalty while being able to concentrate on their core business.

FFTF businesses have strong links throughout their supply chain

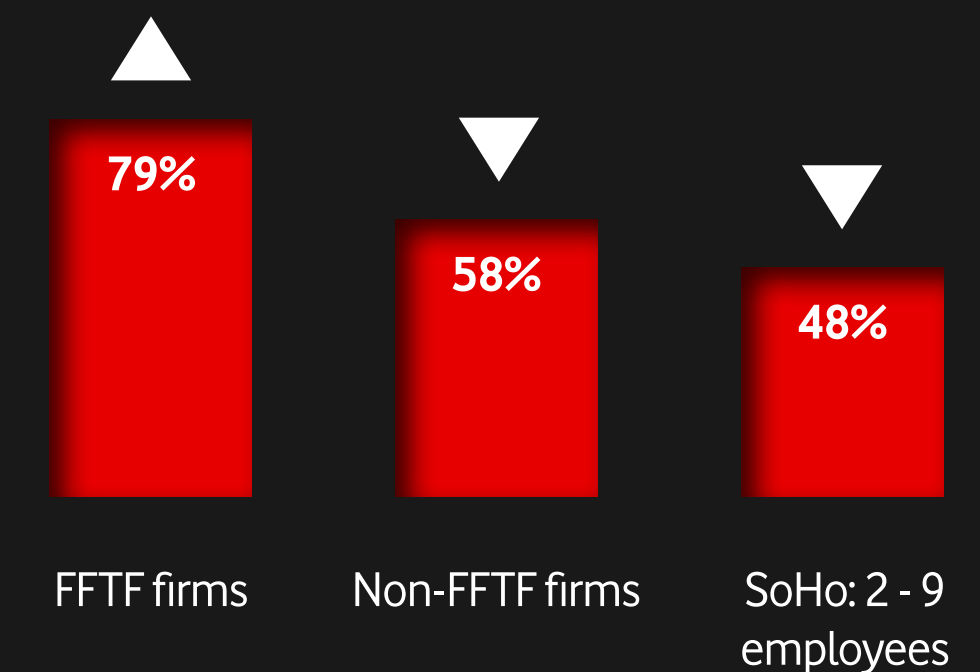
For a business to be secure, it takes more than just looking inwards – they need to have confidence in their entire supply chain. FFTF businesses understand this better than most, with 43% stating they have 'very high' levels of trust in the cyber security measures taken by their supply chain and business partners, compared to just 25% of non-FFTF businesses. And should an incident occur, FFTF businesses will rely on their trusted relationships and close collaboration with suppliers and partners to overcome the issues.

FFTF businesses are more likely to keep on top of auditing their suppliers, with 56% doing so regularly compared to just 36% of non-FFTF businesses.

“We see information security as an enabler of, rather than a barrier to new opportunities”



“A good reputation for information security is a differentiator that can help us to win new customers”



1

2

3



WORKING TOGETHER TO STAY SECURE

In light of a growing number of major data breaches, businesses need to know their third-party partners are secure. Teamwork is crucial here.

FFTF businesses get the full picture

FFTF businesses understand the importance of being prepared for cyber security threats throughout the supply chain. So, they regularly audit their partners for security compliance and ensure they have plans in place in case one of their suppliers experiences a security breach.

Demonstrate compliance to get ahead

An organisation's typical supply chain contains a network of businesses which is likely to include SMEs. Those SMEs that get cyber security right have an opportunity to stand out from the crowd. By using a security scorecard, SMEs can demonstrate and improve their cyber security credentials and win new business.

63%

of firms agree greater collaboration between organisations (particularly suppliers) is needed to resolve cyber security challenges



03

CONCLUSION



WHAT SETS FFTF BUSINESSES APART WHEN IT COMES TO CYBER SECURITY?

It's no coincidence that FFTF businesses are in prime position to build resilience for the future while also driving growth. They have taken the following steps to ensure their cyber security journey is a successful one:



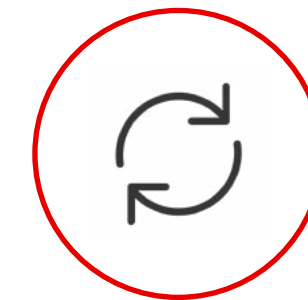
Plan

It's all about reviewing your current business operations and setting a clear plan for the organisation and employees. The vast majority of FFTF businesses tell us they've developed a clear cyber security strategy which all stakeholders have bought into whilst also ensuring a cyber-aware culture through relevant employee training programmes. This gives the whole organisation the confidence to address any challenges that might arise.



Prepare

There's no getting away from it: protection requires putting in the time, having resources in place to support and securing investment. FFTF businesses understand this and set themselves up in the right way to be able to implement their cyber security strategy and training plans effectively. They are also willing to seek outside support to help identify their business' cyber security needs to ensure costs are minimised without compromising security.



Practise

FFTF businesses realise the importance of a holistic approach to cyber security and embed it into the foundation of their organisation. It's integrated into everything they do – from their business strategy and operations to products and customer service – with a focus on people and partners.

A CLEAR CYBER SECURITY STRATEGY DOES MORE THAN JUST PROTECT BUSINESSES

We hope our research has given you an insight into what a comprehensive approach to cyber security can achieve. It shouldn't be seen as simply a cost of doing business or as a purely defensive measure.

Cyber security can give organisations freedom – to adopt hybrid working, operate more flexibly and boost productivity. It can help businesses unlock the benefits of new technologies, giving them a platform to innovate, stand out and drive growth, all while enabling them to respond quicker to changes in the market. So now, more than ever before, businesses should focus on the opportunities that robust cyber security can bring.

In a world of growing cyber threats, doing nothing is not an option – and not just from a security perspective. Businesses that fail to invest in cyber security are likely to see slower growth than competitors that see the bigger picture.

In such a competitive business landscape, building a brand that customers can trust has never been more important. As we've seen, FTF businesses are more likely to have comprehensive plans in place. It's this preparation which allows them to be ready for anything.

With the right strategic partner behind them, businesses can intelligently and safely connect their data, people and things in today's hyperconnected world. They can work seamlessly and build resilience, ensuring they're ready to take advantage of tomorrow's possibilities.

ARE YOU READY TO BECOME 'FIT FOR THE FUTURE'?

Start your journey towards a safer and more prosperous future today.

Find out more at:

www.vodafone.com/business/fitforthefuture



HOW WE IDENTIFIED OUR SUBJECTS FOR 2022

Our Market Research team started with wide-ranging desk research looking into topics across politics, economics, sociology, technology, law and the environment.

We distilled all our findings down into clear categories and based on these, plus key challenges/themes identified in previous waves of research in 2020 and 2021, we built a set of research objectives.

These included:

How businesses are evolving their security strategies to meet new cyber challenges brought by hybrid and remote working.

Qualitative and quantitative primary research conducted with our partner B2B International.

Quantitative:

3,101 businesses surveyed via online survey across 15 markets:

- | | | |
|---|---|--|
|  UK |  Germany |  Portugal |
|  Netherlands |  Spain |  Romania |
|  United States |  Italy |  UAE |
|  South Africa |  Australia | Fieldwork period:
August 2022. |
|  Ireland |  China | |
|  India |  Singapore | |

Qualitative:

25 in-depth interviews with businesses across UK, Germany, South Africa, Italy and Spain and 5 with journalists and investors.

Fieldwork period: July 2022.



Together we can
vodafone
business

© 2023 Vodafone Limited. This document is issued by Vodafone in confidence and is not to be reproduced in whole or in part without the express, prior written permission of Vodafone. Vodafone and the Vodafone logos are trademarks of the Vodafone Group. Other product and company names mentioned herein may be the trademark of their respective owners. The information contained in this publication is correct at the time of going to print. Any reliance on the information shall be at the recipient's risk. No member of the Vodafone Group shall have any liability in respect of the use made of the information.

The information may be subject to change. Services may be modified, supplemented or withdrawn by Vodafone without prior notice. All services are subject to terms and conditions, copies of which may be provided on request.