The business of cyber security

Protecting SMEs in the changing world of work

A WPI Strategy report for Vodafone UK

February 2023

Contents

Disclaimer & Legal

This report has been produced by WPI Strategy and Vodafone. The views expressed in the report are based on independent research and represent solely the views of the authors. They are provided for informative purposes only. Whilst we undertake every effort to ensure that the information within this document is accurate and up to date, Neither WPI Strategy nor Vodafone accept any liability for direct, implied, statutory, and/or consequential loss arising from the use of this document or its contents.

About WPI Strategy

WPI Strategy is one of the UK's leading political communications consultancies, with a track record of delivering high impact public affairs campaigns. We offer senior strategic counsel and work extensively with our sister company, WPI Economics, to ensure that campaigns are underpinned by evidence-based content.

wpi-strategy.com nick@wpi-strategy.com @wpi_strategy

About Vodafone

Vodafone UK connects people, businesses and devices to help our customers benefit from digital innovation. Our services span mobile, fixed line, broadband and the Internet of Things (IoT). We employ around 11,000 people across the UK, and operate more than 420 retail stores nationwide.

Having made the UK's first mobile phone call and sent the first text, Vodafone has a history as a tech pioneer. In 2018 we made the UK's first live holographic call using 5G, and were the first to start carrying live 5G traffic from a site in Salford, Greater Manchester. Today we serve over 18 million mobile and fixed line customers in the UK, with 4G network coverage at 99 per cent. Vodafone has launched 5G in 100 places across the UK so far. Our customers voted us the UK's Best Network Provider at the 2020 Trusted Reviews Awards. To help deliver Gigabit UK, we are rolling out full fibre broadband across 12 towns and cities in partnership with CityFibre, reaching one million homes and business by 2021.

Our ReConnect programme is supporting women and men back into work after a career break, our IoT technology is working to create a low-carbon society, and our free Digital Parenting magazine is helping families across the UK to navigate the online world safely. For two years running, we have been named one of the UK's 25 Best Big Companies to Work For by the Sunday Times, and a Top 100 Employer by Stonewall.

Vodafone is taking significant steps to reduce our impact on our planet by reducing our greenhouse gas emissions by 50% by 2025 and becoming net zero by 2040, purchasing 100% of our electricity from renewable sources by 2025, and reusing, reselling or recycling 100% of our redundant network equipment.

We are part of Vodafone Group, one of the world's largest telecommunications companies, with mobile operations in 21 countries, partnerships with mobile networks in 42 more, and fixed broadband operations in 17 markets. As of 30 June 2020, Vodafone Group had approximately 300+ million mobile customers, 27 million fixed broadband customers and 22 million TV customers, including all of the customers in Vodafone's joint ventures and associates.

For more information about Vodafone UK, please visit: **www.vodafone.co.uk**

Foreword

As they embrace the opportunities of digitisation, it is important that all businesses take seriously the risks of cyber attacks. Small and medium-sized businesses are no exception, with cyber criminals frequently targeting SMEs. But too often those SMEs lack the awareness, the skills and the security measures to withstand them.

This much was evident when we first explored the issue of SMEs and cybersecurity in our 2021 report. Back then, the shift to remote working linked to Covid-19 had led to an increase in the number of attempted cyberattacks, building on an upward trend that was already visible.

Two years later the trend towards hybrid working has only accelerated. Businesses also face fresh cybersecurity risks as a result of Russia's invasion of Ukraine and continuing geopolitical tensions. And yet for many SMEs the urgent need to invest more in cyber security products risks being overshadowed by the cost-of-living crisis and high energy prices.

It is in this context that we once again explore the issue of SMEs and cybersecurity in this report. We do so with new polling providing further detail on the extent to which SMEs are currently experiencing attempted cyberattacks, the scale of the risk they pose, and what – if anything – they are doing about it.

With the latest data we can see that businesses are still heavily targeted by cyberattacks, with many seeing an increase. While there is clearly a need for better cybersecurity protection, too many SMEs are still holding back from putting that protection in place.

Since our last report in 2021, the Government has made progress in supporting the delivery of local cybersecurity skills. Most notably, the nine regional Cyber Resilience Centres (CRCs) set up across England and Wales can play an important role helping smaller organisations to make their cyber operations safer, more secure and more resilient.

However more still needs to be done. In this report we have set out some of the steps that Government could take to further make sure that small businesses have the help they need to cope with the cybersecurity threats, leading to a place where businesses of all sizes are properly equipped to deal with the opportunities and challenges of a digital world. However, we also call on SMEs themselves to take action, to protect themselves and the wider supply chains of which they are a part.

With SMEs accounting for around 99% of all businesses in the UK, it is essential that we get this right. Cyberattacks can have a devastating impact on the businesses concerned, as well as the economy as a whole. By stepping up, the UK Government can make sure that UK SMEs are better equipped to deal with the cybersecurity challenges they face.

Andrew Stevens,
Commercial Director & Head of SME, Vodafone

Executive summary

When we previously examined the cybersecurity risks facing SMEs in 2021, the UK – and the world – faced different challenges. Since then, while government bodies have raised the alarm about the risks associated with operating online, the trend towards hybrid working has only accelerated. Russia's invasion of Ukraine and continuing geopolitical tensions have also highlighted fresh cybersecurity risks, with the National Cyber Security Centre stressing that "now is not the time for complacency" and asking all UK organisations to bolster their cyber defences.

But the urgent need to invest more in cyber security products comes as the cost of living crisis has hit many households and businesses hard. With the cost of gas and electricity skyrocketing since 2021, research by the Federation of Small Businesses indicated that one in four small firms have cancelled or scaled down investment or expansion plans.[1]

It is against this backdrop that the National Cyber Strategy 2022 intends to lead the UK into a future where we are "even more resilient to cyber attack". It states that government will help organisations better understand how the data they hold could be used to facilitate crimes like fraud, identity theft or extortion. In addition, the Government's new Telecoms Security Framework has strengthened cyber and network security among big operators, but SMEs are not being supported to boost their own defences so as not to provide weak links in the chain.

With the cybersecurity risks faced by SMEs coming in various guises, help is clearly needed. For some businesses, there is a real risk of loss of staff and even of business collapse. Yet there continues to be a lack of basic digital skills as well as a vast disconnect between how vulnerable most business leaders think they are, and how vulnerable they are in reality.

Our own polling shows the extent to which SMEs are currently experiencing attempted cyberattacks, the scale of the risk they pose, and what – if anything – they are doing about it. We found:

- Almost one in five (19 per cent) of SMEs polled said that an average cyberattack costing £4,200 would destroy the business. That amounts to more than a million SMEs.
- The majority of SMEs polled (54 per cent) had experienced an attempted cyberattack in the past 12 months.
- 18 per cent said their business was not protected with cybersecurity software and a further 5 per cent did not know.
- Only 28 per cent were aware of the Government's Cyber Essentials scheme – with more SMEs saying they had heard of a cybersecurity product that does not actually exist.

Clearly, there is a need for better cybersecurity protection. Yet it remains the case that many SMEs are insufficiently persuaded, or lack the knowledge they need, and importantly the finance they need, to put that protection in place.

To address these problems, our previous report recommended that Government should do more to support the delivery of local cybersecurity skills. We welcome the progress that has been made here with the establishment of nine regional Cyber Resilience Centres (CRCs) across England and Wales.

However, as our latest polling shows, more still needs to be done to raise awareness of current initiatives. Government should therefore explore options for incentivising those SMEs who are yet to take advantage of help currently available to bolster their cyber defences.

As this report makes clear, since we first published our recommendations, the case for taking action to make businesses of all sizes more cyber secure has only become stronger.

Introduction

We previously examined the cybersecurity risks facing SMEs in 2021. Our report, Protecting our SMEs: cybersecurity in the new world of work was published in February, after the peak of the second wave of Covid-19 in the UK but before the onset of the third wave in July 2021. Of course, much has changed in the UK since the publication of our last report.

First, the Covid-19 pandemic led to increased working from home and the implications and the full extent of this behavioural shift are now much clearer than before. In late 2021, the National Cyber Strategy 2022 noted the "increased exposure to risks" resulting from that the growing dependence on digital technologies for remote working and online transactions. The National Audit Office has also sounded the alarm, stating that moving most aspects of our social and economic life online kept "many businesses, social networks and relationships going. But it also came with a significant downside, as we all became more vulnerable to the risks associated with operating online."[2]

Since then, figures published by the Office for National Statistics indicate that the trend towards working both from home and the workplace has only accelerated. In the first quarter of 2022, 9.9 million people in the UK reported working from home, more than double the 4.7 million in the last quarter of 2019. The ONS' regular tracker of working arrangements also shows that almost 40 per cent of workers in the UK have been using a hybrid model of working in the final quarter of 2022.[3]

Second, Russia's invasion of Ukraine has highlighted fresh cybersecurity risks. In January 2022, ahead of the invasion, the National Cyber Security Centre (NCSC) asked all UK organisations to bolster their cyber defences.[4] Explaining this action, the NCSC subsequently stated that "now is not the time for complacency" and "your best long-term response to changes in cyber threat (without your staff having to work 24/7) is to permanently improve your organisation's cyber security and resilience by building more secure networks and bolstering your resilience capabilities".[5]

Since that guidance was published, the EU, UK, US and other allies announced that Russia had been behind a series of cyber attacks. It is natural for smaller businesses to assume they may not be targets of nation state sponsored cyber attacks. This, however, would be mistaken. Many small businesses work with, or are in supply chains alongside, major firms and data is not necessarily shared in the safest ways. Smaller businesses must always be aware of heightened cyber security risks.

The third significant change in the UK since the publication of our last report is the cost-of-living crisis that the UK has experienced since late 2021. The British Chambers of Commerce said in 2022 that record high inflation presented the biggest threat to business growth while the Federation of Small Businesses highlighted rising energy costs. As Government support with energy costs has been significantly scaled back from April 2023, small businesses are likely to be once again faced with difficult decisions to keep up with rising costs. An FSB survey in November 2022 revealed that one in four small firms anticipate having to close, downsize or radically change their business model in light of reduced support with energy bills.[6] 32 per cent of small businesses surveyed had already cancelled or scaled down planned investments in their business as a result of increased energy prices, meaning SMEs will be even less inclined to invest in much-needed cybersecurity products in this economic climate, and may need further support or incentive to do so.

Chapter 1. Where we are now on cyber security

Eye-catching Government announcements in the digital space in 2022 have focused on broadband and the next generation of wireless technology, rather than cyber security. This may explain why, in his final speech as prime minister, Boris Johnson was keen to highlight the "the roll-out of gigabit broadband up over the last three years".

Prior to that speech it was announced in July 2022 that universities and telecoms firms had been invited to apply for up to £25 million to research and develop the next generation of 5G and 6G network equipment. “The seamless connectivity and blistering speeds of 5G and then 6G will power a tech revolution which will enrich people’s lives and fire up productivity across the economy”, said then Digital Infrastructure Minister Matt Warman.

In the years ahead, while investing in broadband and the next generation of wireless technology is hugely important, ministers would also do well to place a heavy emphasis on the need to protect the people and businesses who make use of these and other technologies.

The Government’s latest thinking on cyber security was set out in the National Cyber Strategy 2022, published at the end of 2021. This document takes over where the National Cyber Security Strategy 2016 leaves off, intended to lead the UK into a future where we are “even more resilient to cyber attacks”. The strategy is outlined under five pillars, with the second pillar specifically focused on reducing cyber risk in the UK.

Government has stated its intent to build on its experience of responding to significant cyber incidents, ensuring that by 2025 lessons identified are used to improve our policies and processes. While UK businesses and organisations “have a clearer understanding of what to do in the event of an incident”, the strategy states that government will improve access to training and exercising, supported by assured industry services, including a new Cyber Incident Response scheme and Cyber Incident Exercising service.

Government initiatives aimed at tackling cyber crime at an SME level include the Cyber Aware advertising campaign and the Cyber Essentials Scheme, which offers two levels of certification to help organisations guard against a cyber attack. In addition, the NCSC is preparing to launch a new assured Cyber Advisor scheme. This will extend assured cyber security consultancy services to a wider market of SMEs, with the aim of helping to ensure a minimum standard of security. In December 2021, Regional Cyber Resilience Centres were also rolled out in each of the nine policing regions, and London. These are a collaboration between police, public, private sector and academic partners to provide subsidised or free products and cyber security consultancy services.

Yet the previous flagship government initiative to assist SMEs with digitalisation offered nothing help with cyber security. The Government unveiled the ‘Help to Grow: Digital’ scheme at the Spring Budget 2021. Those eligible could access discounts worth up to £5,000 on approved software. In July 2022 the scheme was expanded so that businesses with at least one employee would be eligible to benefit, up from the previous requirement for businesses to have more than five employees.

Until the scheme's curtailment in February 2023, various business support tools and products were available for subsidy under the scheme, but cybersecurity products were not. This was a missed opportunity which failed to recognise that cybersecurity is essential for safeguarding productivity and growth. Including cybersecurity products in the scheme would have been of tangible benefit to many thousands of businesses at real risk of cyber attacks. It would also have helped to stimulate demand in the UK’s world-leading cybersecurity sector, which itself is made up of many SMEs.

Chapter 2. Cybersecurity risks for SMEs

Small and medium-sized enterprises (SMEs) are central to the UK economy. At the start of 2022 there were 5.5 million small businesses (with 0 to 49 employees)[7] and a further 35,900 medium sized businesses (50 to 294 employees). SMEs account for 99.9 per cent of the business population and for three fifths of the employment and around half of turnover in the UK private sector. Total employment in SMEs was 16.4 million (61 per cent of the total) whilst turnover was estimated at £2.1 trillion (51 per cent).

However, beneath the headline figures, the total number of businesses in the UK decreased by 8 per cent between January 2020 and January 2022. This consisted largely of businesses with no employees – i.e., self-employed workers – the largest category of UK businesses.[8]

In July 2022, the Department for Digital, Culture, Media & Sport's Cyber Security Breaches Survey found that four in ten businesses (39 per cent) reported having cyber security breaches or attacks in the last 12 months, remaining consistent with previous years of the survey.[9]

Principal vulnerabilities and potential impact

The primary vulnerabilities of SMEs are not the same as for larger companies. As already noted, SMEs are at a much higher risk of collapse than larger firms when cyberattacks take place. Where this can have a major impact is in supply chains; breaches can compromise confidentially shared databases, often containing customer or employee information. Below, we list the main types of external cyberattack and the associated risks to SMEs:

Web-based attacks

Web-based attacks are the most common form of attack on SMEs. These attacks leverage browsers and their extensions, websites, and components of web-based applications to harvest credentials or confidential data. SMEs should ensure that websites are built securely and with cybersecurity in mind to prevent this kind of attack.

Ransomware

Ransomware is a particularly devastating kind of cyberattack, involving theft of files and a subsequent ransom demand. These kinds of attacks can be particularly difficult for SMEs due to the high-cost burden. Although there has been a recent decline in the prevalence of ransomware attacks, the threat is still high.

Credential

Credential stuffing: credential stuffing is where an attacker uses a stolen or guessed password to access confidential systems. SMEs are a particular target for these kinds of attacks as they are less likely to have stringent password policies. Many SMEs, for example, do not have basic protections such as two-factor authentication in place.

Trojans

A trojan is an attack which, once allowed into the IT system (usually under the guise of an innocent programme), is very difficult to remove. Once inside, a trojan could be stealing data or sending IP information outside the network. This is another kind of attack for which the risk can be lowered by training and awareness among employees.

A key theme running through these attacks is that cybersecurity attacks are composed of two parts: firstly, the actual cybersecurity architecture, but also the limited staff training and awareness which allows them to detect threats that exploit human error. Both the first and second parts are integral to establishing a secure network.

The risks for SMEs from these attacks are extensive. Financial loss can result from theft of information or banking details, from reputational damage or from when a business is prevented from trading. SMEs hit by cyber attacks may also face the costs of fines from authorities if personal data is compromised; the costs from cleaning affected systems; and costs to the wider sector if other companies are damaged in the supply chain; There is also the risk of loss of staff and business collapse due to any of these factors.

How Vodafone is helping SMEs secure themselves

Vodafone has been securing networks and protecting businesses for over 30 years, and therefore has the experience to help small businesses make the right cyber security decisions for their operations. We've invested over £1bn in our UK network, worked with over 70% of the Fortune 500 and for the last three years have been recognised as a leader in the Gartner Magic Quadrant for Network Services.

Our cybersecurity solutions span the full range of services for SMEs:

Device security: Keeping sensitive data secure requires thought and precision. Our range of Mobile Threat Defence, Endpoint Protection and Unified Endpoint Management solutions will help keep SME teams secure and business protected.

Network security: Benefit from our years of supplying secure networking to large enterprises, critical national infrastructure organisations and government bodies.

Cloud and app security: Keeping work private and data safe with intelligent technology that can help SMEs determine when sensitive information is at risk.

Operations security: From phishing awareness services to Managed Security Operations Centres our operations services are built to help SMEs detect and respond to cyber attacks.

Vodafone's V-hub: Provides SMEs with guided information for businesses going through digital transformation through its digital business insights, one-to-one support and topical information, including protection from cyber attacks. V-hub draws on the expertise of local partners and industry leaders to help SMEs get the right support. With content catered to different levels of understanding, the aim is to provide a comprehensive level of support for any organisation.

Yet there continues to be a lack of basic digital skills. In 2018, the Business, Energy, and Industrial Strategy Committee noted that "many SMEs lack basic digital skills, while others do not have the capacity to take advantage of new digital technologies, reducing their ability to become productive and innovative and allow their workers to reskill and upskill".[10] More recently, a 2021 report by the Department for Digital, Culture, Media & Sport further developed the point, stating that approximately 680,000 businesses (50 per cent) have a basic skills gap, "that is, the people in charge of cyber security in those businesses lack the confidence to carry out the kinds of basic tasks laid out in the government-endorsed Cyber Essentials scheme."[11] This means that many SMEs are in the vulnerable position of using technology without understanding the security risks, and failing to put in place appropriate – but often basic – controls.

There also continues to be a vast disconnect between how vulnerable most business leaders think they are, and how vulnerable they actually are. Back in 2016 the National Crime Agency found that SMEs "often do not have the resource to implement cyber security measures or are not aware of the risks".[12] Five years on from the NCA's report, research from TechRadar indicated that little had changed, suggesting that SMEs simply don't see the need for cybersecurity. 34 per cent stated they didn't invest more because their business was too small and 19 per cent said their data was not a target and their business was not under threat. The report noted that "this laissez-faire approach to security has to change if SMEs are to protect their business and avoid financial hardship".[13]

Our own polling, outlined in the next chapter, provides further detail on the extent to which SMEs are currently experiencing attempted cyberattacks, the scale of the risk they pose a risk and what – if anything – they are doing about it.

Why is small business vulnerability so important?

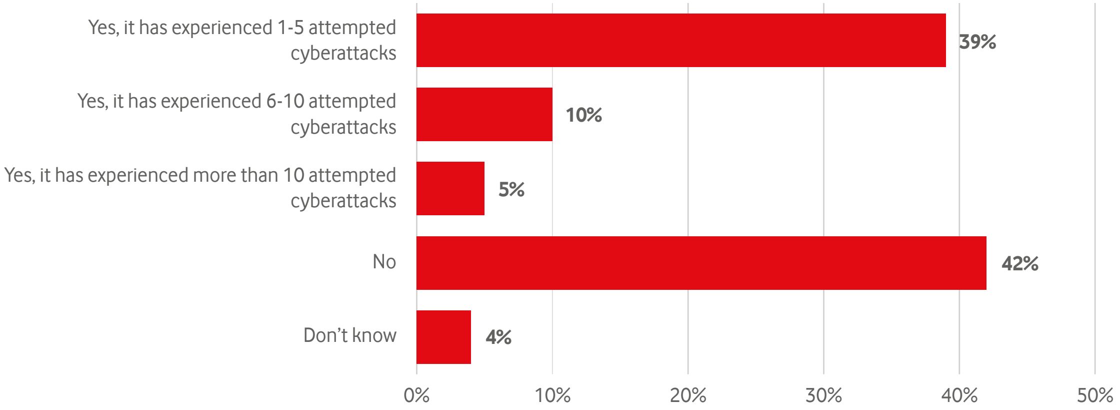
- Small business X is a health start-up with 56 employees and a number of major businesses clients for which it holds health data. Since the pandemic, they have adopted a hybrid approach to working, but decided not to invest in more than basic cyber security or employee training.
- Colleague A recently joined as an account manager. They receive an email from what looks like a senior director's account, with an urgent subject line asking them for support on another account. They follow a link to a document, not realising the email was sent by a hacker disguised as their director. The hacker manages to capture colleague A's login details.
- By using these details, the hacker gains access to the company's database, which includes private health data from several major pharmaceutical companies. They steal and delete this data from the server, with one of the clients losing all access to sensitive and critical information on customers across the country.
- The breach affects patients across the country, with health plans being disrupted and medication unable to be dispensed. Customers worry about their data being safe and opt out of the programs, forcing a major company to close its projects. With sensitive data at risk for being sold on, or used for future attacks, the breach also means the major business client has to pay out thousands of pounds in settlements.
- Although no major company ever experienced a security breach directly, the impact of the SME attack causes a major loss in revenue and public trust, permanently damaging their future and reputation.

Chapter 3. How SMEs are handling cyber security

Previous research has suggested that the managers of small and medium-sized businesses are insufficiently aware of the risk of cyberattacks. Our latest research makes clear that despite the risks associated with increased levels of online work, levels of awareness remain dangerously low.

A poll of 515 leaders of businesses employing up to 250 people or less, carried out by Survation on behalf of Vodafone in June 2022 for this report, found that 54 per cent of them had experienced some form of cyberattack in the previous 12 months. This compares to 39 per cent when the same polling was conducted in August 2020 for our previous cyber security report. Our latest polling also showed that 33 per cent of businesses had seen the number of attempted cyber attacks increase since the beginning of 2021 while just 18 per cent had seen the number go down.

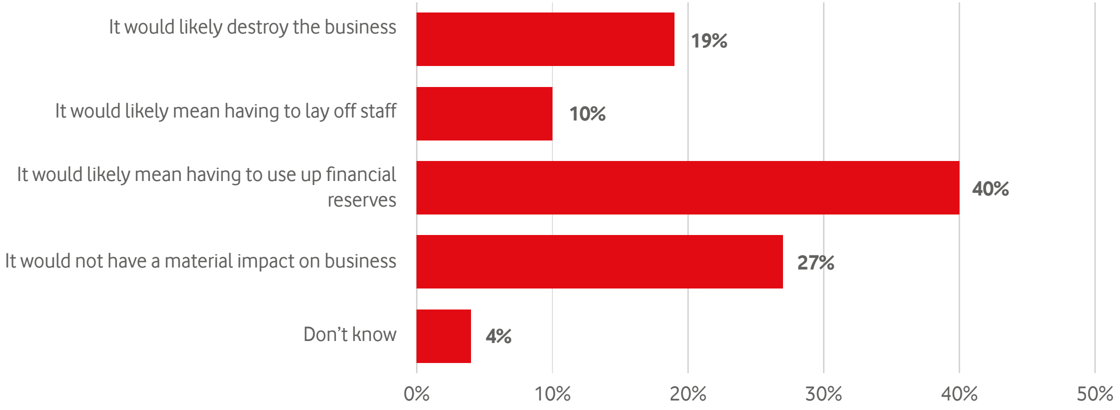
Q1. Has your business experienced an attempted cyber-attack in the past twelve months (this includes all forms of attack including data breaches, phishing emails, and impersonation emails)?



Cyberattacks present an existential risk to a significant proportion of the SMEs we polled. According to the Government's Cyber Security Breaches Survey, looking at organisations reporting a material outcome, such as loss of money or data, gives an average estimated cost of £4,200 for all cyber attacks from 2021-22.

This is the kind of loss which many of the businesses we polled simply could not bear. Some 19 per cent said that it would destroy the business. That amounts to more than a million SMEs. Another 10 per cent said that it would likely mean having to lay off staff.

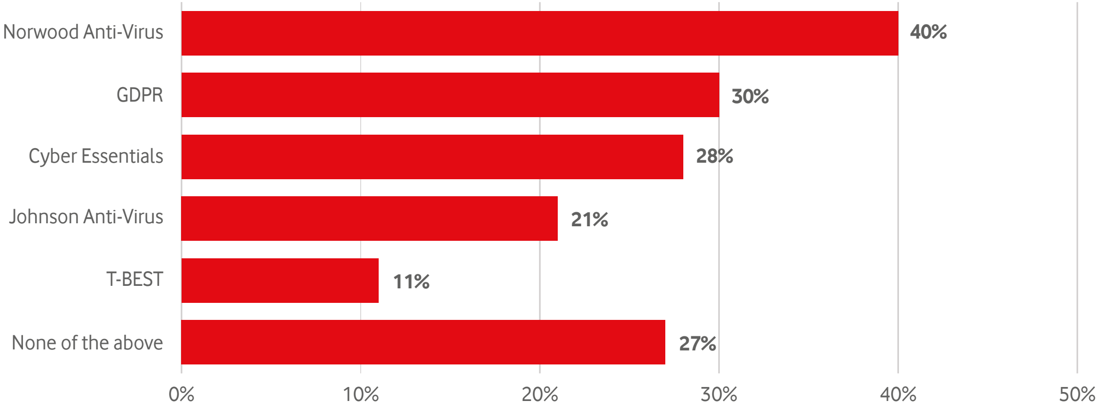
Q3. The average cost of a successful cyber-attack on a UK business is £4,200. What would the impact of a loss of £4,200 be on your business?



Our polling found 18 per cent of respondents saying their business was not protected with cybersecurity software and a further 5 per cent did not know. Only 28 per cent were aware of the Government's Cyber Essentials scheme – with more SMEs saying they had heard of a cybersecurity product that does not actually exist, Norwood Anti-Virus.

Furthermore only 30 per cent were aware of GDPR, created to alter how businesses and other organisations can handle the information of those that interact with them. There is the potential for large fines and reputational damage for those found in breach of the rules.

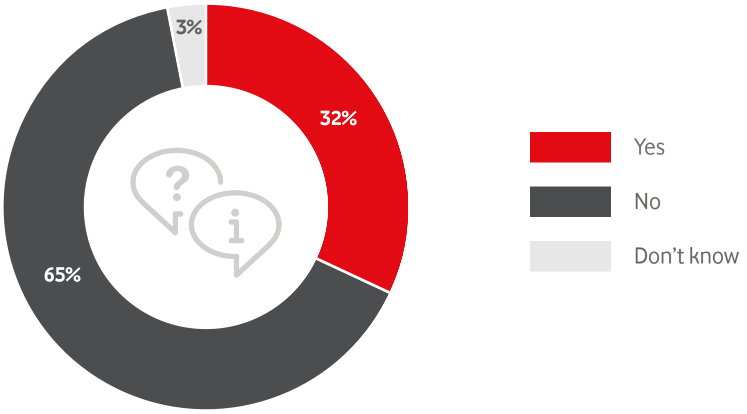
Q5. There are various schemes, certifications, or products related to cybersecurity. Which of the following products, if any, have you heard of? Please select all that apply.



Our polling indicated that just over half (52 per cent) would be open to their business becoming a supplier to major companies or the UK Government, while 12 per cent said that it already is. Of those who would be open to their business becoming a supplier to the Government or major companies, less than half (49 per cent) had heard of the Government's Cyber Essentials certification.

Less than half (46 per cent) were aware of the advice and support available to small and medium-sized enterprises through the National Cyber Security Centre. Most (65 per cent) had not received any advice or help tailored to the specific cybersecurity needs of their business from central or local government.

Q9. have you ever received advice or help tailored to the specific cybersecurity needs of your business from central or local government?



Finally, our polling showed that almost half (47 per cent) said that the Russian invasion of Ukraine had made them more concerned about cybersecurity attacks in the UK.

Overall, our polling reveals a worrying picture – just as it did when we previously examined the cybersecurity risks facing SMEs in 2021. That picture is that small businesses are still heavily targeted by cyberattacks, with many seeing rising numbers of attempted attacks.

They are highly vulnerable in the event of a successful cyberattack, in many cases to the extent that the financial losses they would incur as a result would threaten their business's very existence. Their homeworking employees are often particularly vulnerable to attack, with too many companies either believing that their staff have inadequate cybersecurity measures in place at home or simply not knowing whether they do or not.

While there is a need for better cybersecurity protection, it remains the case that many SMEs are insufficiently persuaded, or lack the knowledge they need, to put that protection in place.

Chapter 4. Conclusion and recommendations

Our previous report on cybersecurity risks facing SMEs in 2021 encouraged the Government to see a lack of cybersecurity skills and certification as an issue which affects the entire economy and regional growth. We also recommended that Government should do more to support the delivery of local cybersecurity skills and we welcome the progress that has been made here with the establishment of nine regional Cyber Resilience Centres (CRCs) across England and Wales. These bodies can play an important role helping smaller organisations to make their cyber operations safer, more secure and more resilient.

Yet more still needs to be done to ensure that all SMEs are fully equipped to deal with the opportunities and challenges of a digital world. Cybersecurity skills are crucial digital skills, and not investing in the abilities of SMEs to protect themselves could seriously impact economic growth in the UK.

As this report makes clear, since we first published our recommendations in 2021, the case for taking action to make businesses of all sizes more cyber secure has only got stronger.

We are therefore urging Government to respond the growing threat levels by moving further and faster towards protecting all SMEs.

Raising awareness of current initiatives will be central to this. We know that SMEs tend to underestimate the threats from cyber attacks. This may be partly caused by low awareness of government cybersecurity initiatives and suggested certification.

The Government should therefore consider running a ‘Cyber Safe’ PR campaign, to improve uptake of support offered by Cyber Resilience Centres and improve awareness of the Cyber Essentials certification among small businesses. Government should also explore options for incentivising those SMEs who are yet to take advantage of help currently available to bolster their cyber defences, including other schemes promoted by private businesses.

The Government could also reallocate funding within the National Cyber Security Strategy budget to further support the delivery of local cybersecurity skills and training, including targeted initiatives for small businesses. In doing so, Government should closely examine evidence showing that police-fronted interactive “enhanced engagement programmes” delivered locally have the most impact in terms of improving long-term cybersecurity skills and resilience.

Endnotes

1 https://www.fsb.org.uk/resources-page/out-in-the-cold.html

2 https://www.nao.org.uk/naoblog/cyber-security-has-the-pandemic-changed-anything/

3 https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/datasets/publicopinionsandsocialtrendsgreatbritainworkingarrangements

4 https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

5 https://www.ncsc.gov.uk/blog-post/preparing-the-long-haul-the-cyber-threat-from-russia

6 https://www.fsb.org.uk/resources-page/one-in-four-small-firms-plan-to-close-downsize-or-restructure-if-energy-bills-relief-ends-in-april-next-year-new-survey-reveals.html

7 https://www.gov.uk/government/statistics/business-population-estimates-2022/business-population-estimates-for-the-uk-and-regions-2022-statistical-release-html#composition-of-the-2022-business-population

8 https://researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf

9 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

10 https://publications.parliament.uk/pa/cm201719/cmselect/cmbeis/807/807.pdf

11 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf

12 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/38-the-cyber-threat-to-uk-business/file

13 https://www.techradar.com/features/risky-business-the-state-of-cybersecurity-among-uk-smes

WPI Strategy Limited

1st Floor,
5-6 St Matthew Street,
London,
SW1P 2JT

@WPI_Strategy

wpi-strategy.com

WPI Strategy Limited, registered address 28 Church Road, Stanmore, Middlesex, England, HA7 4XR, is registered as a limited company in England and Wales under company number 10086986.

February 2023