Protecting our SMEs

Cybersecurity in the new world of work

A WPI Strategy report for Vodafone UK

February 2021

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

More of the UK's economy is digital than ever before. Since the start of the Covid-19 pandemic, work meetings have increasingly taken place remotely through video conferencing software, and more and more businesses have relied on the internet to sell their goods and services and keep in touch with suppliers and clients. Covid-19 has transformed the work practices of practically all businesses, from the largest to the smallest, and even when the pandemic is over we can confidently expect more economic activity to take place online than it did beforehand – helping to drive the UK's economic recovery as well as accelerating a process of digitisation which was already taking place.

There are almost six million small and medium-sized businesses (SMEs) in the UK – 99.9 per cent of the business population. As they rightly embrace the opportunities of digitisation, it is important that they take seriously the risks that go with them. Being small makes you agile, but it can also make you vulnerable. And one of the biggest vulnerabilities SMEs have is to cyberattacks.

The shift to remote working linked to Covid-19 has seen an increase in the number of attempted cyberattacks, building on an upward trend that was already visible. Almost a third of the SMEs polled for this report said that they had seen an increase in such attacks since the start of the March 2020 lockdown. Recent figures from the National Cyber Security Centre (NCSC) have revealed that more than a quarter of all cyber incidents detected in the past year involved criminals and hostile states exploiting the coronavirus pandemic, with ransomware often embedded in what appeared to be important official communications from the Government about Covid-19.

We know that cyber criminals target SMEs, but those SMEs often lack the awareness, the skills and the security measures to withstand them. Yet they often also lack the resources that bigger companies, with deeper reserves, have to deal with the financial consequences of a successful cyberattack. The average cost of a cyberattack successful enough to have a material cost to its victim is £3,230: barely an irritation to a FTSE-100 company, but enough to wipe out many small businesses. In fact, polling carried out for this report shows that almost a quarter of small businesses in the UK would be incapable of surviving a loss on this scale: that's the equivalent of 1.3 million SMEs. And another 16 per cent, the equivalent of a million more SMEs, would have to lay off staff if they were faced with this cost.

That's a risk to individual SMEs and their employees, but it's also a risk to the wider supply chains of which they are part, and ultimately to the economy as a whole. As this report argues, it makes sense for the Government to build on strong progress it has made with cybersecurity for big businesses by putting SME cybersecurity on the same footing, taking more proactive steps to raise awareness among SMEs of the risks they face and support them to protect themselves more effectively. That should include placing SME protection prominently within the next National Cyber Security Strategy, greater incentives to encourage SMEs to strengthen their own security, and supporting the delivery of more effective, locally delivered cybersecurity skills training for SMEs.

It is in everyone's interests to have businesses of all sizes, throughout the economy, properly equipped to deal with the opportunities and challenges of a digital world. That means being clear-eyed about the cybersecurity threats that they face, and making sure that they have the support that they need.

Anne Sheehan, Business Director, Vodafone UK

Executive summary

Improved and expanded cybersecurity provision for business is both a longstanding Government policy objective and a necessity in the digital world in which we live. Covid-19 has shown how important digital resilience is to the economy and society while also accelerating digitalisation. The UK economy contracted by 9.9% in 2020, according to the Office for National Statistics.[1] Economic recovery may be slow, but the road to recovery can be made easier. This report aims to make clear that with the opportunities brought by increased digitisation there are also attendant risks, and recommends policies to mitigate this.

Our focus is SMEs, which will be the backbone of the UK's economic recovery, making up 99.9 per cent of the business population and employing 16.8 million people. But SMEs are also uniquely vulnerable to cyberattacks due to lower turnover, tighter margins, and poorer standards of cybersecurity protection compared to larger businesses. Polling conducted for this report found that over 1.3 million small and medium sized businesses across the UK are at risk of folding given the cost of an average cyberattack. To ensure cyber safe economic growth, the Government must build on its world-leading work and support UK SMEs in adopting the latest cybersecurity technology.

Building more robust cybersecurity practices in both the public and private sector has long been an aim of Government policy. The movement to online working and increased use of online services such as click and collect and online shopping throughout 2020 has introduced more businesses to the opportunities brought by digitisation but also exposed many to further risk.

- Cyberattacks are already costing the UK economy £34 billion a year[2] – equivalent to around 10 per cent of Government Covid-19 borrowing – but with more businesses working remotely as a result of the pandemic, we expect this figure to rise.
- Covid-19 is accelerating the changes which made cybersecurity policy commitments necessary.
- Further digitisation across the economy is inevitable and welcome. The Government has gone some way to recognising that this reliance on digitisation comes with risk, but there is further to go.
- Data suggests cyberattacks have increased since the Covid-19 pandemic began, with a 30 per cent rise in attacks on UK businesses during the first quarter of 2020 alone.[3]
- In June 2020, PwC noted an "increase in ransomware and phishing attacks linked to Covid-19,"[4] with many of these attacks disguised within emails purporting to be from the UK Government.

SMEs are uniquely vulnerable to cyberattacks. Currently, 30 per cent of small businesses don't have a cybersecurity strategy in place,[5] and low awareness of Government cybersecurity schemes is adding to this risk.

- There are more than 5.9 million small and medium sized businesses (SMEs) in the UK – 99.9 per cent of the business population, accounting for three fifths of private sector employment.[6]
- SMEs have always struggled with digital skills. As the Business, Energy, and Industrial Strategy Committee noted in 2018, "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".[7]
- That low capacity is a cause for concern. As the insurer Senseon noted in 2019, "today, SMEs face greater security challenges than ever before and are increasingly targeted by attackers".[8]
- Currently, 30 per cent of small businesses don't have a cybersecurity strategy in place,[9] and low awareness of Government cybersecurity schemes is adding to this risk.

- Additionally, the cost of such attacks adds further pressure to smaller sized businesses compared to their larger peers due to their lower levels of financial reserves.

In order to better understand the potential impact of cyberattacks on SMEs during the Covid-19 pandemic, we polled SMEs across the UK in August 2020. Our data suggests that over 1.3 million small and medium sized businesses across the UK are at risk of folding given the cost of an average cyberattack.

- Almost a quarter (23 per cent) of SMEs polled said that an average cyberattack costing £3,230 would destroy the business. That amounts to 1.3 million SMEs.
- Another 16 per cent, almost a million SMEs, said that it would likely mean having to lay off staff.
- 23 per cent said that it would likely mean having to use up financial reserves.
- Only 22 per cent of those polled said that a loss of this level would not have a material impact on the business.
- 4 in 10 SMEs (41 per cent) had experienced some form of cyberattack in the previous 12 months, with 20 per cent experiencing six or more attacks.
- Finally, almost a third (31 per cent) said that they had seen an increase in cyberattacks since the UK went into lockdown in March 2020.

This report sets out a series of policy recommendations as part of a five-step framework to make businesses of all sizes more cyber secure, but with a particular focus on the gap in provision among SMEs, centring around the broad theme of improving digital skills and cybersecurity awareness:

- **The next National Cyber Security Strategy should include a section on SME protection, with reference to the increased risk associated with remote working:** this section should mention how cybersecurity best practice among SMEs can be best supported by central Government as well as a pledge to develop clearer guidance on how SMEs can best protect themselves.
- **The Government should consider appointing a dedicated unit for cybersecurity for business within the National Cyber Security Centre, and provide the required additional funding:** the National Cyber Security Centre is world leading, and an integral part of our national resilience architecture and a dedicated unit would ensure that businesses receive the appropriate level of support during the recovery from Covid-19.
- **The Government should explore direct subsidies for cybersecurity for businesses:** SMEs should be incentivised to strengthen their own cybersecurity through direct subsidies. This could be paired with a reduced 5 per cent VAT rate on cybersecurity products.
- **The Government should commit an additional 5 per cent to the National Cyber Security Strategy budget to support the delivery of local cybersecurity skills and training:** Evidence shows that police-fronted interactive "enhanced engagement programmes" delivered locally have the most impact in terms of improving long-term cybersecurity skills and resilience. We recommend an additional 5 per cent is committed to the National Cyber Security Strategy budget for this purpose, equivalent to around £95 million.
- **Part of the Government's doubled and rebalanced R&D budget should go towards cybersecurity product development in research centres in the North and Midlands:** The Government has pledged to more than double R&D spending to £22 billion a year by 2024. Part of this budget should be directed towards cybersecurity product development in new research spin-off centres attached to universities in the North and Midlands, modelled on the Advanced Manufacturing Research Centre in Sheffield. This would carry out world-leading research and innovation with digital businesses from across the UK.

Introduction

- **Strong cybersecurity is a longstanding commitment of the UK Government.**
- **The Covid-19 pandemic has accelerated the movement online of more and more economic activity in almost every sector.**
- **This increased reliance on digitisation brings attendant cybersecurity risks to SMEs who are also less prepared.**
- **Our polling reveals that more than 1.3 million SMEs would collapse if forced to deal with the cost of an average cyberattack, which stands at £3,230.**

Long before the Covid-19 outbreak, the Government had already set out its ambition for the UK to become the best place to start and grow a digital business.[10] But recent events have both hastened this process and demonstrated its necessity. The pandemic has accelerated the movement online of more and more economic activity in almost every sector, from traditional office work to retail.

This would not have been possible without the pre-existing strength of the UK's digital sector. It is a sector which is growing six times faster than the economy as a whole;[11] in 2018, the latest year for which figures are available, it contributed £149 billion to the UK economy.[12] But some of this extraordinary growth risks being lost without action from Government. A previous report from Vodafone and WPI Strategy found that £15 billion of UK economic output which would have been created by the UK digital sector is at risk of being lost over the next decade, along with 37,400 digital sector jobs and 10,800 digital sector businesses.[13]

In June 2020, Secretary of State for Digital, Culture, Media, and Sport, Oliver Dowden MP delivered a speech intended to signal a significant shift forward in the Government's digital strategy. From now on, he argued, the UK needed to "build a highly-skilled digital workforce across every region of the UK, so that people can shift into the digital or tech sectors or indeed digitise their own businesses."[14]

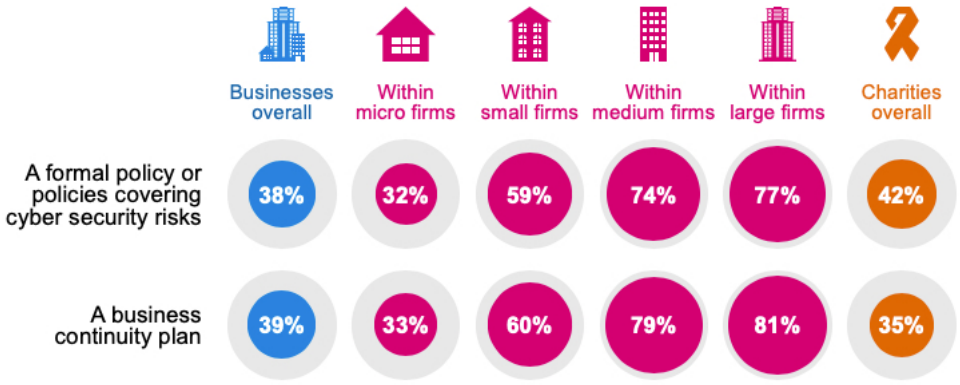
It was a challenge laid down to both central Government and the tech sector: to create not just more extensive digitisation but the attendant deep digital skills across the country to realise it. Such a challenge is an exciting and realisable prospect, given Britain's role in developing leading digital technologies.

There are already some obvious opportunities. Making digital central to the Government's economic recovery plan, and ensuring the UK is a leader in faster 5G rollout, will be essential in the UK's economic recovery from Covid-19. Investing in 5G alone, for example, could add as much as £158 billion to the UK economy over the next decade.[15] But digitisation is a broad programme and securing digital assets is just as important as developing initial capability and capacity.

Opportunities and Risks

But deeper reliance on digitisation comes with inevitable risk. Rolling out digital processes and systems means ensuring those systems are adequately protected against malicious cyberattacks. Building more robust cybersecurity practices in both the public and private sector has long been an aim of Government policy.

Cyberattacks cost the UK economy £34 billion a year[16], but with more businesses working remotely as a result of the pandemic, we can expect this figure to rise. Early data shows a 30 per cent rise in cyberattacks on UK businesses during the first quarter of 2020.[17] Attackers are also increasingly using the pandemic as a pretext to initiate contact with vulnerable businesses and test cybersecurity architecture. In other words, opportunities for the extensive compromise of private business, colleague, or customer data have expanded. Enhancing the digital potential of UK businesses, and indeed ensuring that they can continue to operate at all, must therefore also mean building cybersecurity skills and awareness into everyday working.



Bases: 1,348 UK businesses; 642 micro firms; 277 small firms; 216 medium firms; 213 large firms; 337 charities

Source: Cyber Security Breaches Survey 2020, DCMS

Focusing in on SMEs

We have decided to focus attention on SMEs, the most individually vulnerable segment of the business population. Some of these businesses will have robust cybersecurity measures in place, but many – as the polling in this report demonstrates – won't, especially when compared to larger companies with teams of security experts. There is also a lack of awareness among SMEs when it comes to advice on how to protect themselves from cyber threats. According to the Government's Cyber Breach Survey 2020, only 23 per cent of small businesses are aware of the UK Cyber Essentials scheme, the Government-backed standard which provides a basic level of protection against cyberattacks.[18] That's over 4.5 million businesses potentially unaware of the protection and benefits of the basic certification as well as being at possible risk of exposure. And with typically smaller turnover and lower cash reserves to deal with crises, SMEs are more likely to suffer business failure as a result of a serious cyberattack. Any national cybersecurity strategy which aims to be world-leading will have to respond to the amplified threats posed by Covid-19. Later in this report we present the results of SME polling which suggests that up to 1.3 million businesses are at risk of collapse given the cost of an average cyberattack.

What's even more worrying is the uneven impact across the UK's regions. Previous polling has revealed a major regional disparity, with businesses located in Wales and the North East being up to half as likely to have cybersecurity protections in place than businesses in London.[19] Given the Government's commitment to boost growth across every region of the UK, and the economic impact a cyberattack could have on smaller businesses' ability to operate, it is vital that policymakers do everything in their power to raise awareness of the problem and work with businesses to mitigate the risk.

This report sets out a series of policy recommendations as part of a five-step framework to make businesses of all sizes more cyber secure, but with a particular focus on the gap in provision among SMEs, centring around the broad theme of improving digital skills and cybersecurity awareness. If the Government's new digital strategy is to be successful, it must reform its own cybersecurity awareness programmes, build better skills and training, invest in cybersecurity development, and introduce new cybersecurity standards that correspond with business size. The world-leading National Cyber Security Centre is more than capable of responding to the increased threat environment post-pandemic. Changing these policies could prevent smaller and medium-sized businesses being left behind in a fast-moving cybersecurity threat environment, as well as delivering on longstanding Government priorities.

With the current National Cyber Security Strategy due to expire in 2021, the Government has a golden opportunity when formulating the next one to take an even bolder approach and build on the UK's existing strengths: ensuring that the deep digital skills in cyber defence currently held at a national level and in larger businesses are spread more widely, so that smaller businesses and organisations have the tools they need to keep themselves cyber secure.

Chapter 1. State of play on cybersecurity

- **Evidence suggests that there was a 30 per cent year-on-year increase in cyberattacks on UK businesses in Q1 of 2020, with a high number of attacks occurring as the UK entered lockdown.**
- **The digital economy has been central to the continuation of economic activity during the Covid-19 pandemic, and will need to be the engine of post-pandemic growth.**
- **The UK has seen an apparent rise in the sophistication and complexity of threats, meaning businesses must remain even more vigilant in the face of rising attacks.**

The Department for Digital, Culture, Media, and Sport's 2020 Cyber Security Breaches Survey suggests that cyber-crime is now extensive. Around a third of businesses and two in ten charities reported breaches or attacks over the last 12 months.[20]

An increase in remote working during the pandemic and an increasing reliance on digitisation in general has driven up the volume of cyber threats. The increase in cyberattacks seen during the early stages of the pandemic was building on a year-on-year upward trend, with smaller businesses seeing an increase in attacks of 14 per cent from 2018 to 2019, and medium-sized businesses seeing a 27 per cent jump.[21] A recent poll of medium and large businesses in the UK found that 92 per cent had seen an increase in cyberattacks over the past few months, with many concerned about the increased security risks associated with the movement to remote working.[22]

This trend is not restricted to the UK; it is global. A recent survey from VMware Carbon Black found that 53 per cent of incident response professionals globally had seen an increase in cyberattacks following the spread of Covid-19.[23] One of the most commons cyberattack trends is so-called 'island hopping', in which attackers target a smaller company or supplier to a larger company, in order to access the latter's digital assets.[24] Such attacks mean attacks on SMEs can have an outsized impact on the wider economy and throughout supply chains.

Low awareness of the cyber threat adds further complexities. Around two-thirds (66 per cent) of business leaders at companies with up to 500 employers do not believe that they will fall victim to a cyberattack,[25] whilst around the same proportion of companies (67 per cent) experienced an attack in 2018.

In March 2020, the UK Government estimated that an average cyberattack in the past twelve months with a material outcome cost businesses £3,230

This lack of awareness has significant financial consequences. In March 2020, the UK Government estimated that an average cyberattack in the past twelve months with a material outcome cost businesses £3,230, a higher figure than in 2018 (£3,160) and 2017 (£2,450).[26] Not only do these serious attacks drain personnel and financial resources, but they can have a damaging impact on companies up and down supply chains. For example, the cyberattack reported by Ticketmaster in 2018[27] saw not only Ticketmaster UK and International being affected but their customers and other ticket sale sites such as TicketWeb and Getemin.[28]

One of the biggest challenges is simply a lack of awareness among business owners about what measures can be taken to mitigate the risk of a cyberattack. Only 13 per cent of all businesses, for example, are aware of the Cyber Essentials scheme.[29] Some businesses do understand the cyber threat but don't think of their cybersecurity as a process but only as a one-off product. The problem with that is they are left more vulnerable as cyber attackers find ways to get around the initial layer of security.

What is the Cyber Essentials scheme?

Cyber Essentials is a Government-backed scheme designed to protect all sizes of organisation against cyberattacks. The scheme provides certification that your network and digital assets are safe against some of the most basic forms of attack. There are two primary types of certification:

Cyber Essentials – this is a self-assessment which provides protection against the most common forms of cyberattack.

Cyber Essentials Plus - this includes everything in the basic Cyber Essentials package, plus the reassurance of an external technical verification.

The benefits of earning certification are clear: it allows businesses to make clear their level of IT security, secure their own network, and – in some instances – bid to work with Government contracts.

The scheme does not include mandatory staff awareness training, despite human error being frequently cited as one of the biggest gaps in any cybersecurity system. There are, however steps the Government can take to address this need, which we explore in our policy recommendations.

Digitisation as an opportunity and a challenge

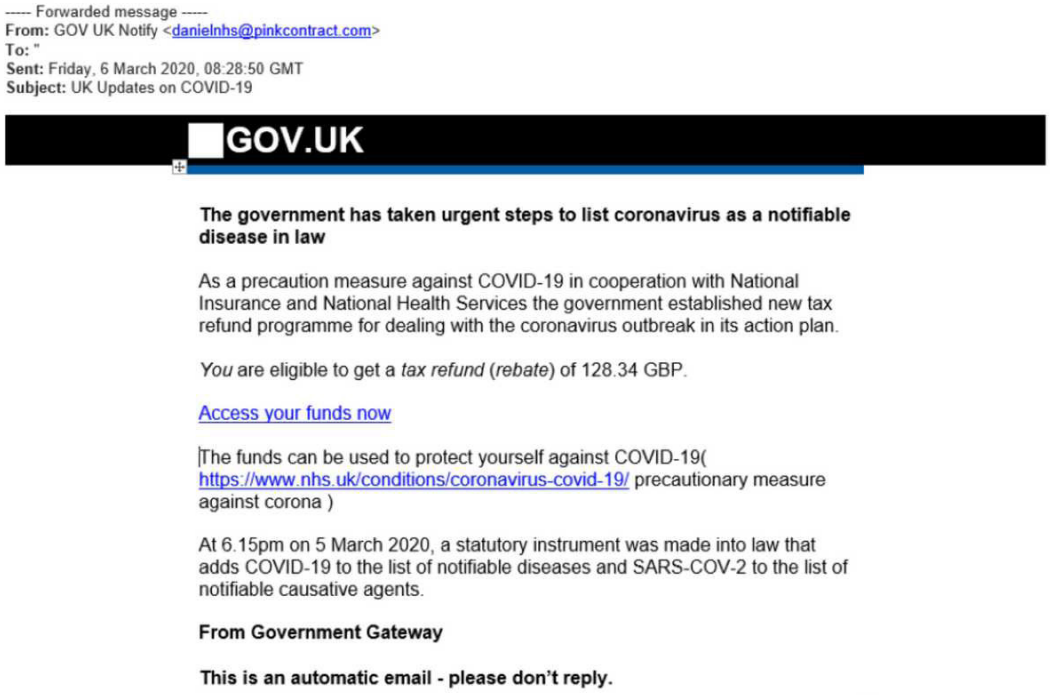
While technological change was happening at a rapid pace pre-Covid, the process has undoubtedly been accelerated. With business and society now far more reliant on online trading, strengthening cyber resilience should be a top priority. As Vodafone's recent report 'Levelling up: How 5G can boost productivity across the UK' has shown,[30] digitisation will be at the heart of the recovery, stimulating growth and creating opportunities. The nation's digital companies produce 7.7 per cent of the UK's total output and underpin far more by providing productivity-enhancing digital products and services to firms in every other industry.[31]

Cybersecurity has been a long-term priority for the Government. In 2010, the National Security Strategy rated cyberattacks as "Tier 1" threats. The Government is developing its new priorities for cyber in its upcoming cyber strategy for the next five years. The strategy is an encouraging sign for businesses, and it will help to secure the country's business base for the long-term. However, it should recognise the increased threat of attacks post-Covid, particularly for SMEs.

Increased threat sophistication

As PwC noted in June 2020, "alongside the increase in ransomware and phishing attacks linked to Covid-19, businesses need to consider how the rapid shift to remote working might have increased the risk of a cyber incident".[32] This double risk should be at the forefront of SME business planning, paired with an awareness of the increased sophistication of cyber threats.

Throughout the Covid-19 pandemic, for example, cyber criminals have often used the cover of Government communication to send emails containing links which, when clicked, send private data from a victim's computer to the attacker. Despite the type of threat – phishing – remaining basic, the sophisticated design of the attacks was unusual. It is as yet uncertain whether or for how long these innovative attacks will remain a threat. Included below is an example of a phishing email published on the UK Government website GOV.UK as a warning against these threats:



----- Forwarded message -----
From: GOV UK Notify <danielnhs@pinkcontract.com>
To: "
Sent: Friday, 6 March 2020, 08:28:50 GMT
Subject: UK Updates on COVID-19

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

The funds can be used to protect yourself against COVID-19(https://www.nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

From Government Gateway

This is an automatic email - please don't reply.

Cyber threats have also been sent via text message with what appears to be a genuine Government website link:.

Such threats are part of the increase seen since the start of the pandemic. In our own polling, nearly a third (31 per cent) of SMEs said they had seen an increase in attacks since the start of the UK's lockdown.

Covid-19, however, is just one pretext used by cyber criminals to make contact with potential victims. As the methods used by attackers increase in complexity and sophistication, there is a real risk that the 'digital divide' between businesses in cybersecurity competence results in more widespread business collapse.

Chapter 2. Zeroing in on SMEs

- **SMEs are central to the UK economy, making up 99 per cent of all UK businesses and employing 16.8 million people.**
- **Individual SMEs are more at risk of collapse than larger businesses if they suffer a cyberattack.**
- **Businesses in Wales and the North East are up to twice as likely to have no cybersecurity measures in place than businesses in London.**
- **Cybersecurity skills are crucial digital skills, and not investing in the abilities of SMEs to protect themselves could seriously impact the economic recovery.**

SMEs are central to the UK economy, making up 99 per cent of all UK businesses and employing 16.8 million people.[33] (60 per cent of all private sector employment). Since 2000, the number of SMEs has increased by 2.2 million, an increase of 64 per cent. [34]

Whilst there are far more of them, individual SMEs are more at risk of collapse than larger businesses due to the economic impact of Covid-19. Whilst large organisations can often spread risk across multiple sites or sections and employ a dedicated Chief Information Security Officer, smaller businesses usually concentrate this risk into one site and a smaller employee base. In late July 2020, Simon Clarke MP, then Minister for Regional Growth and Local Government, announced £20 million in new grant funding to help SMEs across England recover from the Covid-19 pandemic.[35] It was a recognition of the SME economic contribution, and demonstrated the Government's readiness to extend financial support to SMEs at risk of collapse.

That contribution will be essential when the UK enters recovery. There are almost twice as many SMEs outside London as in the capital, 3.8 million outside compared to 2 million within;[36] and looking after the UK's small business base requires regional thinking and a local agenda. The Government's aim to increase growth and productivity across the UK's regions is therefore very welcome.

Boosting regional growth shouldn't stop at physical infrastructure. The geographic spread of cybersecurity protection is not even: companies outside London are less prepared to combat cyberattacks than those in the capital. In previous research, only 18 per cent of businesses in London and 20 per cent of businesses in the East of England indicated they had no cybersecurity protection in place, compared to 40 per cent in Wales and 32 per cent in the North East.[37] This low uptake compares unfavourably with business uptake of other forms of risk mitigation. Most businesses would not want to trade without fire or theft insurance in place, yet in the UK, companies are fifteen times more likely to suffer a cyberattack than an incident of fire or theft.[38]

There are further complications on the horizon. Unemployment is expected to increase over the coming months, and cybersecurity can play a small but still significant role in mitigating the worst effects of Covid-19 on employment levels. Although recessions force some companies out of business, they can also encourage "necessity entrepreneurship", when unemployed workers start microbusinesses in an attempt to guarantee income.[39] These businesses, with low turnover, are often the most individually vulnerable to cybersecurity threats. In our own polling, businesses with a lower turnover were more likely to say that the cost of an average cyberattack would see their business collapse. Both industry and Government must remain especially aware of threats to these SMEs as unemployment rises.

SMEs and Cyber Threats

Perhaps this low take-up is not surprising. Many SMEs have always struggled with digital skills. As the Business, Energy, and Industrial Strategy Committee noted in 2018, "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".[40] That low capacity is a cause for concern. As the insurer Senseon noted in 2019, "today, SMEs face greater security challenges than ever before and are increasingly targeted by attackers".[41] As we highlighted in the last chapter, there is a vast disconnect between how vulnerable most business leaders think they are, and how vulnerable they actually are.

SMEs face additional consequences and challenges when attacked online due to a lack of resources. Getting the right cybersecurity protection in place can be very daunting for businesses with fewer staff and less expertise. The single entrepreneur-led business of six people may have expanded quickly without concern for cybersecurity protection, for example. Cyberattacks on SMEs are often most successful when the company is large enough to hold customer data but not large enough to have a dedicated cybersecurity lead. Currently, 30 per cent of small businesses don't have any form of cybersecurity strategy in place[42] and low awareness of Government cybersecurity schemes is adding to this risk. Additionally, the cost of such attacks adds further pressure to smaller sized businesses compared to their larger peers due to their lower levels of financial reserves.

How Vodafone is helping SMEs secure themselves

Vodafone Business research found that 50 per cent of SMEs across Europe expect lower profits in 2020 compared to 36 per cent of larger rivals. And as we have made clear so far in this report, individual SMEs are far more at risk from cyberattacks.

Vodafone's V-hub therefore 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 cyberattacks. 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.

Trend Micro's Worry-Free Service is a new detection service, offered by Vodafone, to protect businesses and their employees from online security threats such as ransomware, out-of-date applications, and phishing attacks on desktops and laptops. The service offers various features, from anti-ransomware protection through to access to their global smart protection network.

Lookout Mobile Security is an on-device security solution providing businesses with the ability to prevent, detect and remediate against threats on mobile and tablet devices. As more and more sensitive business communications and information is contained on mobiles they are increasingly becoming a target for cyberattackers. Lookout Mobile Security offers anti-virus, network protection, and security in one package to ensure businesses can remain safe whatever device employees and colleagues are working from.

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.

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.

Ransomware

This attack utilizes a Trojan Horse or even a worm (both defined below) to enter a user's device, and will then threaten to leak the victim's data or permanently block access unless a ransom is paid.

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.

A key theme running through these attacks is that cybersecurity is composed of two parts: firstly, the actual cybersecurity architecture, but secondly the 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 from theft of information or banking details
- Financial loss when a business is prevented from trading
- Financial loss from reputational damage
- Costs from cleaning affected systems
- Costs of fines from authorities if personal data is compromised
- Costs to the wider sector as other companies are damaged in the supply chain
- Loss of staff due to any of the above factors
- Collapse of a business due to any of the above factors

We would encourage the Government to see a lack of cybersecurity skills and certification as an issue which affects the entire economy and regional growth. We would encourage the Government to see it as an economic recovery and regional growth problem. Cybersecurity skills are crucial digital skills, and not investing in the abilities of SMEs to protect themselves could seriously impact the economic recovery. In 2018, the Business, Energy, and Industrial Strategy Committee suggested that "digital skills should be at the heart of business support and we recommend that the Government explores how financial incentives can be used to help SMEs invest in them."[43] This report agrees that financial incentives are a necessary next step in protecting SMEs from harm.

Chapter 3. What do SMEs think about cybersecurity?

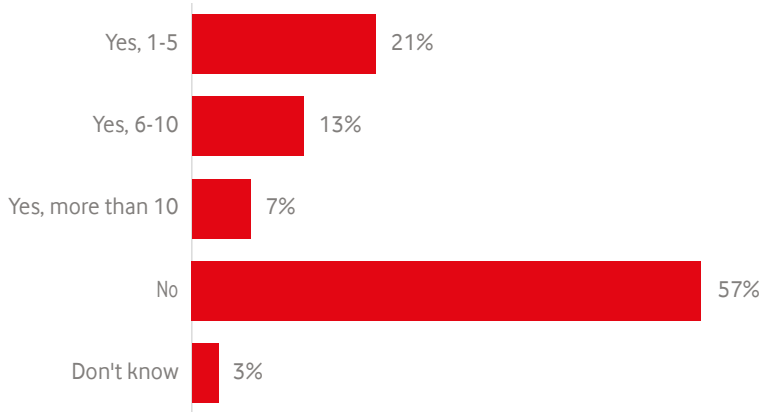
A poll carried out for Survation of over 500 SME leaders for this report in August 2020 found that:

- **A quarter of SMEs would collapse if forced to deal with the cost of an average cyberattack.**
- **Only 22 per cent of those polled said that a loss of this level would not have a material impact on the business.**
- **31 per cent had seen an increase in cyberattacks since the UK went into lockdown in March 2020.**
- **Yet just 59 per cent said that they considered their business's investment in cybersecurity, in general, to be worth the money.**
- **While there is a need for better cybersecurity protection, many SMEs are insufficiently persuaded, or lack the knowledge they need, to put that protection in place.**

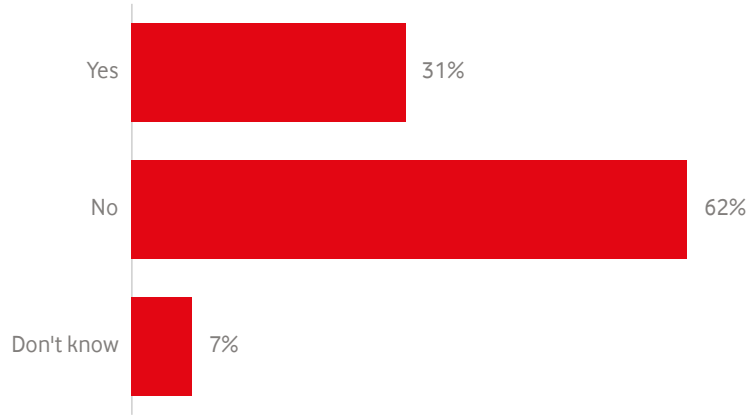
Previous research has suggested that the managers of small and medium-sized businesses are insufficiently aware of the risk of cyberattacks. A 2019 survey found that as many as two-thirds of business leaders at companies with up to 500 employees did not believe that they would fall victim to a cyberattack, and that just 12 per cent understood that attacks are likely regardless of the size of their company.[44] But our research suggests that this complacency is dangerously misplaced.

A poll of 503 leaders of businesses employing up to 249 people, carried out by Survation on behalf of Vodafone in August 2020 for this report, found that 41 per cent of them had experienced some form of cyberattack in the previous 12 months, and that 20 per cent had experienced six or more such attacks. A quarter of those polled said that they had suffered at least one cyberattack which had cost their business £1,000 or more. And almost a third (31 per cent) said that they had seen an increase in cyberattacks since the UK went into lockdown in March 2020.

Has your business suffered a cyber-attack in the past twelve months (this includes all forms of attack including data breaches, phishing emails, and impersonation emails)?

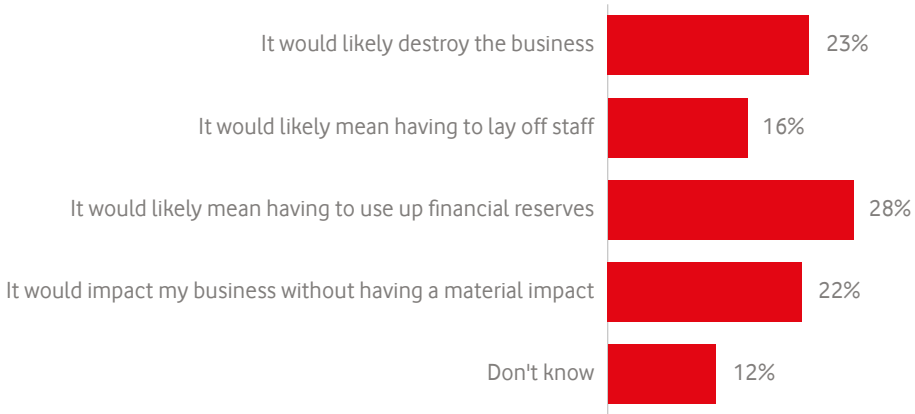


Has your business seen an increase in the number of cyberattacks (including phishing emails) since the UK went into lockdown in March 2020?



Cyberattacks present an existential risk to a significant proportion of the SMEs we polled. According to Government figures, the average cost of a cybersecurity breach with a material outcome in 2019-20 was £3,230.[45] This is the kind of loss which many of the businesses we polled simply could not bear: almost a quarter (23 per cent) said that it would destroy the business – including 28 per cent of SMEs with an annual turnover of under £100,000. Another 16 per cent said that it would likely mean having to lay off staff, and 23 per cent said that it would likely mean having to use up financial reserves. Only 22 per cent of those polled said that a loss of this level would not have a material impact on the business – with those with the highest turnover unsurprisingly being most able to absorb the cost. These results equate to over 1.3 million small and medium-sized businesses across the UK which would be incapable of surviving the average cost of a successful cyberattack, and almost a million more which would survive but would have to lay off staff as a result

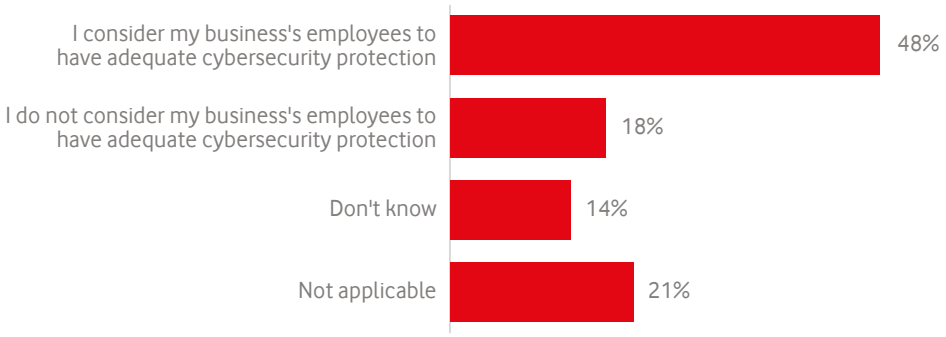
The average cost of a cyber-attack on a UK business is £3,230. Based on that assumption, what would the impact of such an attack be on your business?



According to our polling, over 1.3 million small and medium-sized businesses across the UK would be incapable of surviving the average cost of a successful cyberattack, and almost a million more would survive but would have to lay off staff as a result.

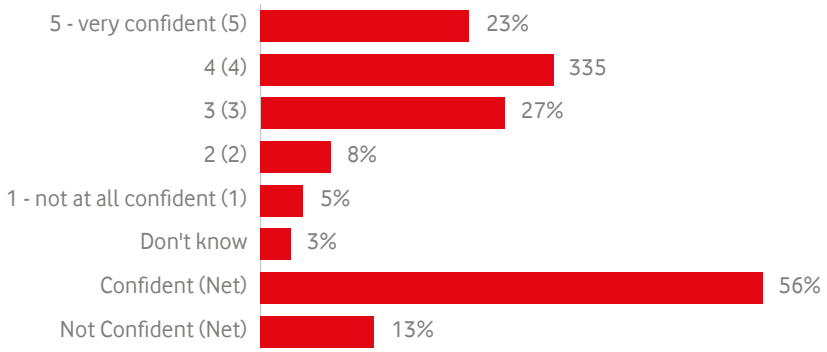
Homeworking during lockdown presents a particular risk to cybersecurity, with many workers using their own equipment and relying on whatever cybersecurity provision they have purchased for home use – if any. Almost a third of the business leaders we questioned were not confident about the cybersecurity of their employees who had been working from home as a result of Covid-19, with 18 per cent saying they did not consider their homeworking employees to have adequate cybersecurity protection, and a further 14 per cent saying they did not know. Yet more than a fifth (21 per cent) said that they had done nothing to encourage homeworking staff to take steps to improve their cybersecurity.

Regarding those employees who have been working from home due to the Covid-19 pandemic, which of the following statements comes closest to your view?



Evidence set out earlier in this report, including previous polling evidence, suggests that many SMEs have not taken cybersecurity as seriously as they should have done. Our polling bears this out. Less than a quarter (23 per cent) of respondents said they were "very confident" in their organisation's cybersecurity protection, and just 18 per cent said that they think they have "very strong cybersecurity protection". Meanwhile, 5 per cent said that they were "not at all confident" in their cybersecurity protection, and a worrying 7 per cent said they had no cybersecurity protection at all. Yet too many small business leaders believe the cost of investing in such protection seems difficult to justify. Just 59 per cent said that they considered their business's investment in cybersecurity, in general, to be worth the money, compared with 14 per cent who did not.

How confident are you in your organisation's cybersecurity protection? (On a scale of 1-5, where 1 is not at all confident and 5 is very confident)?



Overall, our polling reveals a worrying picture: small businesses are heavily targeted by cyberattacks, with an increase in such attacks since the start of the Covid-19 lockdown. 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. Few leaders of small businesses have high confidence in the cybersecurity protection they have – if they have it at all. And yet too few believe their investment in such security is worth it. Clearly, while there is a need for better cybersecurity protection, many SMEs are insufficiently persuaded, or lack the knowledge they need, to put that protection in place.

Chapter 4. Policy Recommendations

The risks to our national recovery are clear: SMEs need targeted support, delivered locally, with further funding boosts. The substantial strengths the UK has in cybersecurity overall, with world-class expertise in agencies such as the NCSC, should be transmitted to even the very smallest businesses. Many of the policy recommendations below are aimed at national Government but they will have relevance for the devolved administrations and local government. Outlined below is a five-step policy programme which can support our economic recovery, as well as boost regional growth:

Recommendations:

- **The next National Cyber Security Strategy should include a section on SME protection, with reference to the increased risk associated with remote working:** this section should mention how cybersecurity best practice among SMEs can be best supported by central Government as well as a pledge to develop clearer guidance on how SMEs can best protect themselves.
- **The Government should consider appointing a dedicated unit for cybersecurity for business within the National Cyber Security Centre, and provide the required additional funding:** the National Cyber Security Centre is world leading, and an integral part of our national resilience architecture and a dedicated unit would ensure that businesses receive the appropriate level of support during the recovery from Covid-19.
- **The Government should explore direct subsidies for cybersecurity for businesses:** SMEs should be incentivised to strengthen their own cybersecurity through direct subsidies. This could be paired with a reduced 5 per cent VAT rate on cybersecurity products.
- **The Government should commit an additional 5 per cent to the National Cyber Security Strategy budget to support the delivery of local cybersecurity skills and training:** Evidence shows that police-fronted interactive "enhanced engagement programmes" delivered locally have the most impact in terms of improving long-term cybersecurity skills and resilience. We recommend an additional 5 per cent is committed to the National Cyber Security Strategy budget for this purpose, equivalent to around £95 million.
- **Part of the Government's doubled and rebalanced R&D budget should go towards cybersecurity product development in research centres in the North and Midlands:** The Government has pledged to more than double R&D spending to £22 billion a year by 2024. Part of this budget should be directed towards cybersecurity product development in new research spin-off centres attached to universities in the North and Midlands, modelled on the Advanced Manufacturing Research Centre in Sheffield. This would carry out world-leading research and innovation with digital businesses from across the UK.

Endnotes

1 See: https://www.cnbc.com/2020/11/25/coronavirus-uk-announces-largest-peacetime-budget-ever.html
2 See: https://www.techradar.com/uk/news/cyberattacks-costing-uk-smes-billions-every-year
3 Beaming analysis 2020, https://www.infosecurity-magazine.com/news/cyberattacks-uk-orgs-up-30-q1/
4 See: https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html (Accessed 08/09/2020)

5 Business in the Community Cyber Report, 2019 (pdf available)
6 Business population estimates for the UK and regions: 2019 statistical release, https://www.gov.uk/government/publications/business-population-estimates-2019/business-population-estimates-for-the-uk-and-regions-2019-statistical-release-html
7 See: https://publications.parliament.uk/pa/cm201719/cmselect/cmbeis/807/807.pdf (Accessed 08/09/2020)
8 Senseon SME Report, 2019
9 Business in the Community Cyber Report, 2019 (pdf available)
10 UK Digital Strategy 2017, https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy#the-wider-economy---helping-every-british-business-become-a-digital-business
11 See: https://www.gov.uk/government/news/digital-sector-worth-more-than-400-million-a-day-to-uk-economy
12 Ibid
13 Vodafone and WPI Strategy, 2020, From Local to Global: repairing the UK economy with thriving digital sectors in our towns and cities, https://newscentre.vodafone.co.uk/app/uploads/2020/11/Vodafone-From-local-to-global-Nov-2020.pdf
14 Oliver Dowden speech at UK Tech Cluster Group, June 2020, https://www.gov.uk/government/speeches/digital-secretarys-closing-speech-to-the-uk-tech-cluster-group
15 WPI Economics, Vodafone (2020), Levelling up: How 5G can boost productivity across the UK
16 See: https://www.techradar.com/uk/news/cyberattacks-costing-uk-smes-billions-every-year
17 Beaming analysis 2020, https://www.infosecurity-magazine.com/news/cyberattacks-uk-orgs-up-30-q1/
18 Cyber Security Breaches Survey 2020, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020
19 Business in the Community Report, 2019 (PDF available)
20 Cyber Security Breaches Survey, DCMS, 2020 (c)
21 Senseon SME Report, 2019
22 See: https://www.itproportal.com/news/most-uk-organizations-experienced-increase-in-cyberattacks-due-to-covid-19/ (Accessed 30/09/2020)
23 See: https://www.vmware.com/company/news/updates/carbon-black-incident-response-report-cyberattacks-2020.html (Accessed 30/09/2020)
24 Ibid
25 SME Vulnerability, YouGov and Keeper, 2019
26 Cyber Security Breaches Survey, DCMS, 2020
27 BBC News - https://www.bbc.co.uk/news/technology-44628874
28 See: https://www.telegraph.co.uk/technology/2018/06/27/music-fans-payment-details-stolen-cyberattack-ticketmaster/
29 Cyber Security Breaches Survey, DCMS, 2020
30 WPI Economics, Vodafone (2020), Levelling up: How 5G can boost productivity across the UK
31 See: https://www.cityam.com/no-deal-brexit-threat-to-digital-economy/
32 See: https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html (Accessed 08/09/2020)

33 BEIS Statistical Release, 2018, Business Population Estimates for the UK And Regions 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746599/OFFICIAL_SENSITIVE_-_BPE_2018_-_statistical_release_FINAL_FINAL.pdf

34 Ibid

35 See: https://www.techuk.org/insights/news/item/18260-government-launches-20-million-in-new-grants-to-help-smes-recover

36 See: https://www.statista.com/statistics/668723/number-small-and-medium-businesses-united-kingdom-uk/

37 Business in the Community Cyber Report, 2019

38 See: https://www.walesonline.co.uk/news/uk-news/chilling-report-reveals-one-six-18463536

39 See: https://www.bbc.co.uk/news/business-53075485 (Accessed 08/09/2020)

40 See: https://publications.parliament.uk/pa/cm201719/cmselect/cmbeis/807/807.pdf (Accessed 08/09/2020)

41 Senseon SME Report, 2019

42 Business in the Community Cyber Report, 2019 (pdf available)

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

44 https://www.computerweekly.com/news/252467348/Most-SMEs-severely-underestimate-cyber-security-vulnerabilities

45 https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

WPI Strategy Limited

50 Broadway,
London,
SW1H 0RG

@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 2021