Securing Success:

The Role of Cybersecurity in SME Growth

A WPI Strategy report for Vodafone UK

April 2025

Contents

About WPI Strategy

WPI Strategy is a specialist public affairs consultancy, focused on combining economic research with political advocacy. We provide a range of private and charitable clients with research and advice to deliver better outcomes through improved public policy design and delivery.

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

About Vodafone

Vodafone UK is a technology communications company that connects people, businesses and devices to help our customers benefit from digital innovation. Our services span mobile, fixed-line connections, home and office broadband, and the Internet of Things (IoT).

We have a strong track record as a tech pioneer, making the UK's first mobile phone call, sending the first text message, and making the UK's first live holographic call using 5G in 2018. We were the first to start carrying live 5G traffic from a site in Salford, Greater Manchester and now have 5G in locations across Germany, Ireland, Italy, Spain as well as the UK. Meanwhile, our 4G network coverage currently reaches over 99% of the UK population.

Today, Vodafone serves more than 18 million mobile and fixed-line customers in the UK. Vodafone is the largest provider of full fibre in the UK – our superfast broadband services are now available to nearly 12 million homes across the UK.

Sustainability is also at the heart of what we do: as of 1 July 2021, 100% of the grid electricity we use in the UK is certified to be from renewable sources.

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

Foreword

At a time where digital threats are becoming exponentially more sophisticated and pervasive, businesses of all sizes face an escalating battle against cyber-attacks, often unaware of the dangers that could already be compromising their operations.

SMEs (Small to Medium Enterprises) in particular face significant challenges. As the backbone of the UK economy their success is key to unlocking long-term economic growth - driving innovation, job creation, and community development. However, they are becoming increasingly vulnerable to the rising threat of cybercrime, which has both financial and operational implications.

Vodafone is investing £11 billion to deliver a nationwide 5GSA network, which will bring significant benefits to the whole country including SMEs. Our research indicates that expanded 5GSA coverage could generate up to £8.6 billion in annual productivity savings for SMEs by enabling technological advancements such as the Internet of Things, AI-driven security solutions, and cloud-based infrastructure. However, we must ensure that our SMEs are protected against cyberattacks and are resilient.

In my role leading Vodafone Business in the UK, I speak with business leaders on a regular basis to understand their growing concerns around cybersecurity and help them navigate risks in an ever-evolving digital landscape.

The National Cyber Security Centre states that basic cyber security practices are frequently ignored nationwide, which can be especially devastating for SMEs. Our research reveals that insufficient cybersecurity measures result in annual losses of £3.3 billion for SMEs.

On average, affected businesses incur a loss of £3,398, encompassing costs related to data recovery, legal fees, regulatory penalties, and operational downtime—all of which hinder growth and resilience.

For SMEs with 50 or more employees, this financial burden increases to £5,001, highlighting the heightened vulnerability of expanding enterprises.

Beyond direct financial losses, SMEs also face severe operational disruptions, reputational damage, and, in extreme cases, potential closure. The urgency for strengthened cybersecurity measures is clear - SMEs require immediate support to safeguard their future.

At Vodafone Business, we are committed to supporting and collaborating with SMEs by providing bespoke cybersecurity services and solutions to protect businesses and drive growth. We adopt a proactive approach to cybersecurity by offering complimentary training and resources through our business.connected initiative. This underscores how large organisations can partner with smaller businesses to enhance resilience and foster growth.

Addressing the cybersecurity gap requires decisive government action to minimise revenue losses and incentivise investment in digital security.

This report calls on policymakers to take immediate and decisive action to protect SMEs online, by offering financial support in the form of tax incentives, grants, and subsidies for cybersecurity training and certification.

Furthermore, collaboration among government bodies, industry leaders, and technology providers is crucial to equipping SMEs with the tools, knowledge, and support which is essential to their success in an increasingly digital economy.

Ensuring the security of these businesses is not merely about preventing financial losses - it is about fostering their long-term resilience and sustaining their vital contributions to the broader economy.

Vodafone Business remains committed to working alongside government and industry partners to drive meaningful change and create a more secure digital future for all SMEs.

Nick Gliddon, Business Director, Vodafone UK

Executive Summary

SMEs are the backbone of the UK economy, generating 25% of GDP, employing 60% of the workforce, and making up 99% of UK businesses.[1] Driving job creation and productivity, a thriving SME sector is crucial to the government's economic growth ambitions.

Since our last investigation into the cyber security experiences of SMEs at the beginning of 2023, rising global tensions and the development of shadow warfare have made businesses across the UK prime targets for cyber-attacks. The rapid development of AI has further increased the sophistication of threats, leaving SMEs more vulnerable than ever.

Yet, for many SMEs, cybersecurity is still not seen as business critical. The National Cybersecurity Security Centre's (NCSC) Richard Horne recently emphasised the need for cyber security preventative measures to be seen as an investment and a 'catalyst for innovation' rather than a cost.[2] As large businesses invest to strengthen their defences, SMEs cannot afford to lag behind.

Vodafone's 2024 Supercharging Small Businesses report showed that standalone 5G has the power to boost productivity across SMEs, producing up to £8.6 billion for UK SMEs through enabling new technologies and services.[3] However, with new technologies comes new cyber threats.

To better understand the current SME cybersecurity landscape, we conducted polling of SME business owners on their cybersecurity habits, exposure to attacks, and the risk to business operations. The findings are stark:

- **Cyber-attacks are costing UK SMEs an estimated £3.4 billion per year in lost revenue**, severely limiting their ability to invest for growth.
- **Over a quarter (28%) of SMEs say a single attack (£6,940) could put them out of business.**[4] When calculated alongside the number of businesses targeted over the last year, this suggests over 530,000 SMEs across the UK are operating at constant risk.
- **Scaling businesses face far greater risks – over 8 out of 10 SMEs with over 50 employees have experienced an attack in the past year**, more than four times the rate of smaller firms. This suggests that many SMEs are not scaling up their cybersecurity alongside their business growth.
- **The North West is the hardest hit area, experiencing the highest cost per attack.** Given the region's thriving start-up culture, cyber threats could stifle SME growth and deter investment.
- **Over half (52%) of SMEs have not received cybersecurity training.**
- **Awareness of the government's Cyber Essential's scheme appears to have fallen,** with less than 18% of SME owners familiar with it, down from 28% in 2023.

Various support schemes are offered as part of the government's Active Cyber Defence (ACD) programme, including Cyber Aware, a Free Cyber Action Plan, and advice on hybrid working.[5] However, our analysis suggests that not enough SMEs are aware of the security and benefits that is provided by the Cyber Essentials scheme. Additional resource should be provided to support uptake.

SMEs instinctively prioritise investment in assets like machinery or staff but, as the NCSC warns, cybersecurity should be treated as a growth enabler. We welcome steps to provide more tailored support, as seen with the government's Cyber Local schemes, and our research reinforces the need for a regional approach.[6] However more can and should be done to encourage SMEs to tackle their cybersecurity risks.

Our analysis makes clear, for SMEs to protect themselves and unlock their full potential, cybersecurity must become a core business decision – not an afterthought.

Recommendations

- Government should expand targeted schemes such as the Cyber Local scheme to increase the number of protected SMEs.
- A targeted SME cybersecurity strategy and campaign to support uptake should be rolled out to ensure that SMEs are made aware of the importance of cybersecurity when businesses are making business critical decisions.
- Government should incentivise cybersecurity investment through a new cybersecurity capital allowance scheme.
- Government should encourage the uptake of public / private partnerships to foster knowledge sharing and collaboration.

Chapter 1. State of Play

Ongoing international insecurity persists and so does the environment of heightened cyber security threats. These risks are amplified considerably by the rapid expansion of AI capabilities and their ability to be used by hostile actors. The development of Deepseek is an example of AI model that has been shown to lack the necessary guard rails of other Large Language Models (LLM).[7]

The changing geo-political environment has brought with it increasing threats and activity by hostile actors. To meet this challenge, the UK's approach to cybersecurity has undergone a series of revisions in recent years. The National Cyber Security Centre (NCSC), established in 2016, remains the primary UK authority focused on educating and providing guidance to support businesses in the UK on cyber security.

At a national level, the government plans to legislate through a planned the Cyber Security and Resilience Bill, mirroring much of the European Union's updated network and information systems (NIS2) regulations, as well as strengthening data safeguards and AI infrastructure.[8] Largely focusing on critical infrastructure and government operations, the Bill puts an increased emphasis on incident reporting and risk management for senior executives. Recent proposals on ransomware attacks reflect this increased focus on incident reporting and intelligence gathering.[9]

At an SME level, the Cyber Essentials scheme continues to offer support with the 'Cyber Advisor' credential offering organisations the chance to become an NCSC Assured Service Provider.[10] These schemes look to encourage basic cyber hygiene for SMEs and provide a level of trust for both public and private procurement processes. Cyber Essentials also offers automatic cyber liability insurance if the entirety of a small business is covered.[11] However, the most basic certification is an annual, self-assessed measure that can provide a false sense of security concerning cyber-threats.

Recent initiatives, such as Cyber Local with its regional grant scheme, have begun to recognise that cybersecurity requires adaptable support that keeps advice relevant and accessible.[12] A £1.3 million fund, targeting regional disparities will see 30 successful projects spanning a range of objectives. Although a move in the right direction, more can be done to expand the scheme and support SMEs expand their cyber resilience.

Vodafone's V-hub advisers make cybersecurity simple for small businesses

Since its creation in 2020, Vodafone V-hub's have supported 1.7 million UK SMEs to upskill their digital capabilities.[13]

Cybersecurity guidance isn't difficult to find online; a quick search will bring up reams of information.

But that can often be the crux of the problem. For smaller businesses, an overload of information and often lacking the necessary time, money or resources to sift through hordes of materials, it's easy to get stuck in a state of analysis paralysis, unable to make a meaningful decision due to the sheer number of options available.

That's where V-Hub comes in. Aided by a team of expert advisers, each with their own individual specialty, V-Hub focuses on stripping away the vast reams of technical information that businesses are often faced with when it comes to keeping themselves secure online.[14]

A longstanding supporter of SMEs and the small office/home office (SoHo) sector, Vodafone created V-Hub to ensure this community is equipped with the digital skills and knowledge it needs to repel potential attacks.

Free to access, V-Hub features an expansive library of business resources covering everything from setting up a new website and managing a business online to marketing and cybersecurity. In addition, users can also speak with a V-Hub adviser for tailored business guidance either on the phone or online – free of charge.

Chapter 2. Key Findings

Our polling and economic analysis tells a wider story of the cybersecurity landscape facing UK SMEs, highlighting key trends in awareness, perception and exposure to attacks. We also assessed the collective and regional threats to these businesses. Several important themes have emerged:

Cybersecurity Awareness:

- **More than half (52%) of SMEs reported that no one in their organisation has received cybersecurity training.**
- **Fewer than one in five SME business owners are aware of the Cyber Essentials scheme, down from 18% when we last conducted this research in 2023.**

Government efforts, including those of the NCSC, do not appear to be impacting a considerable number of SMEs. More targeted awareness campaigns are needed to ensure SMEs embed cybersecurity into their business plans and to support proactive cyber risk management.

Risk to business scalability:

- **Cyber threats increase significantly as SMEs begin to scale – over eight out of ten SMEs with a headcount over 50 have experienced an attack, over four times the number for those with a headcount between 0 and 50.**

Our findings show that cyber threats grow exponentially once a small business expands beyond 50 employees. At crucial times where SMEs are investing and growing, this raises concern that businesses are not receiving the support and products they need to securely continue their growth. Government and NCSC have looked to raise the attention of this issue and offer certifications that aim to encourage SME take-up of good practice. However, as illustrated by our findings, more needs to be done to ensure that growing businesses grow securely.

Scale of the threat:

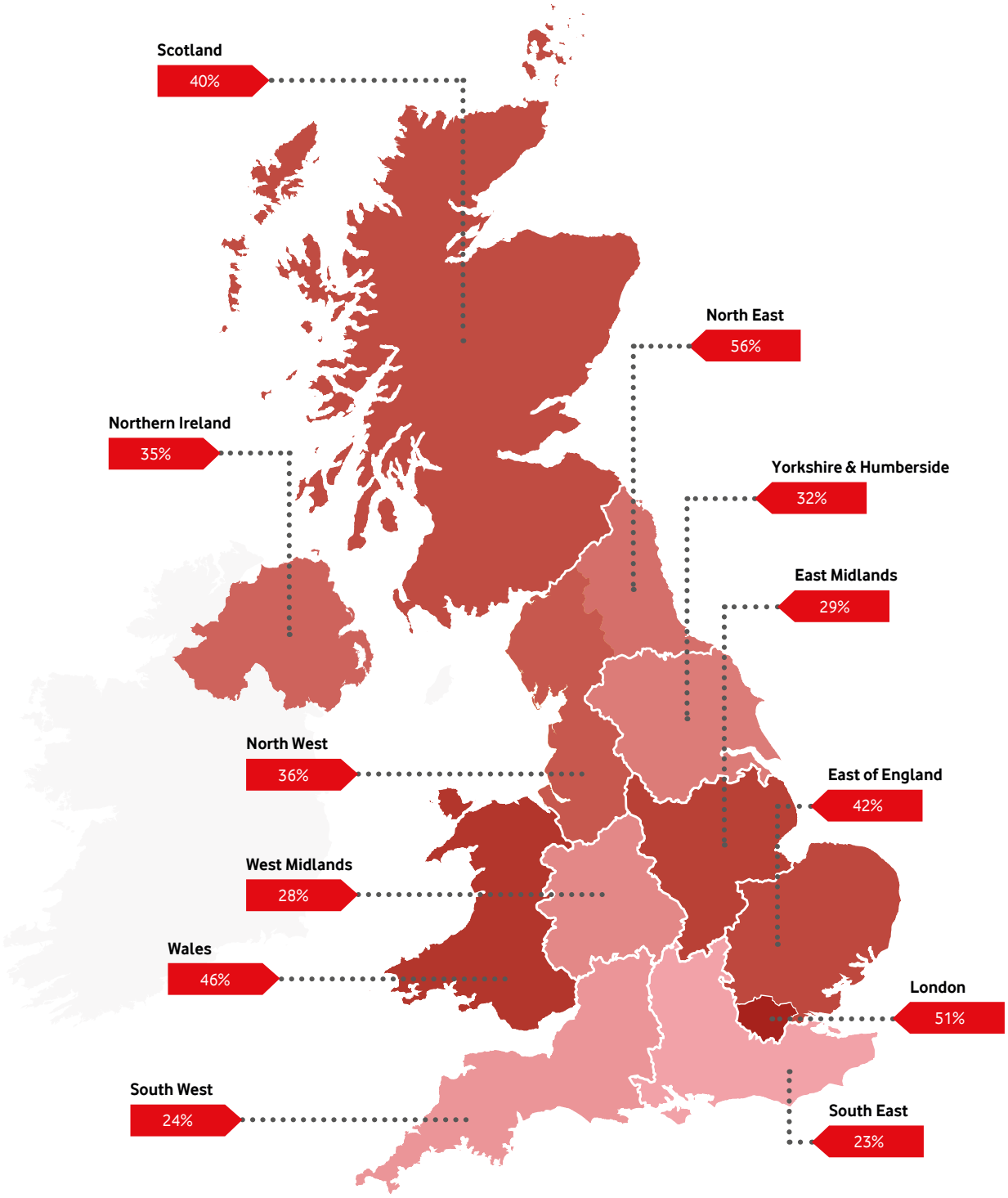
- **Cyber-attacks are costing UK SMEs up to £3.4 billion in lost revenue per year.**
- **Over a quarter (28%) of SMEs surveyed stated that the average cost of a cyber-attack (£6,940) would be enough to put them out of business. Based on the cyber-attack rate of those surveyed, this equates to 530,000 SMEs at risk.**

In practical terms, this lost revenue means fewer new jobs, reduced expansion plans and less investment in growth. These findings also highlight the financial vulnerability of emerging SMEs, underscoring the need for tailored support that acknowledges the limitations of SMEs to invest heavily in cybersecurity and how to approach their investment confidently. Crucially, maintaining cyber security is not merely an optional extra for one in four SMEs, but a necessity for business survival.

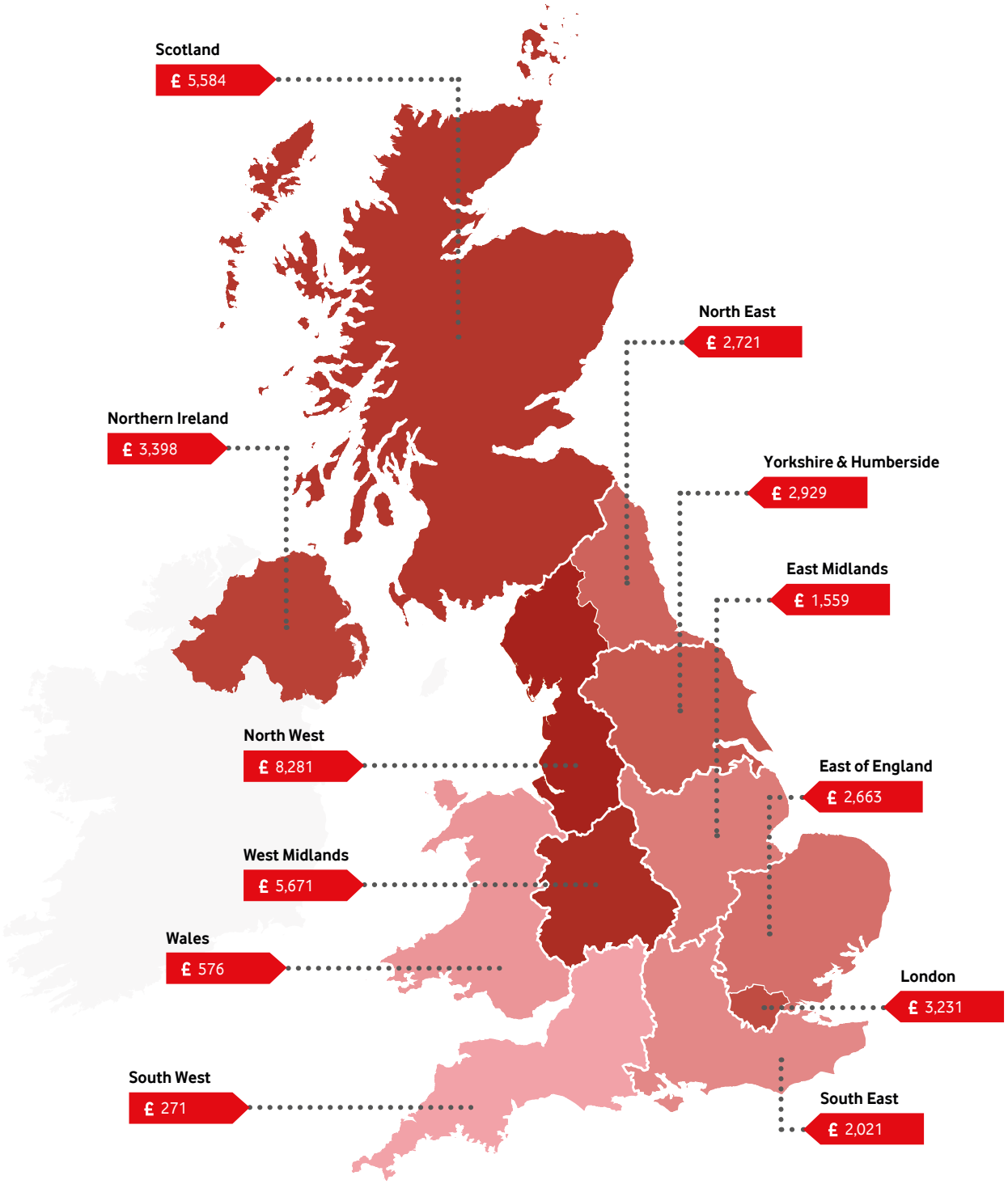
Regional Challenges

The government's Plan for Change has promised to boost growth and raise living standards in all parts of the UK.[15] The experience of businesses locally is important. We looked at how the cybersecurity challenges facing SMEs break down region by region. This is not a uniform picture across the country, the frequency, success rates, and impact of cyber-attacks at a regional level highlight the disparities in the UK's SME cybersecurity landscape.

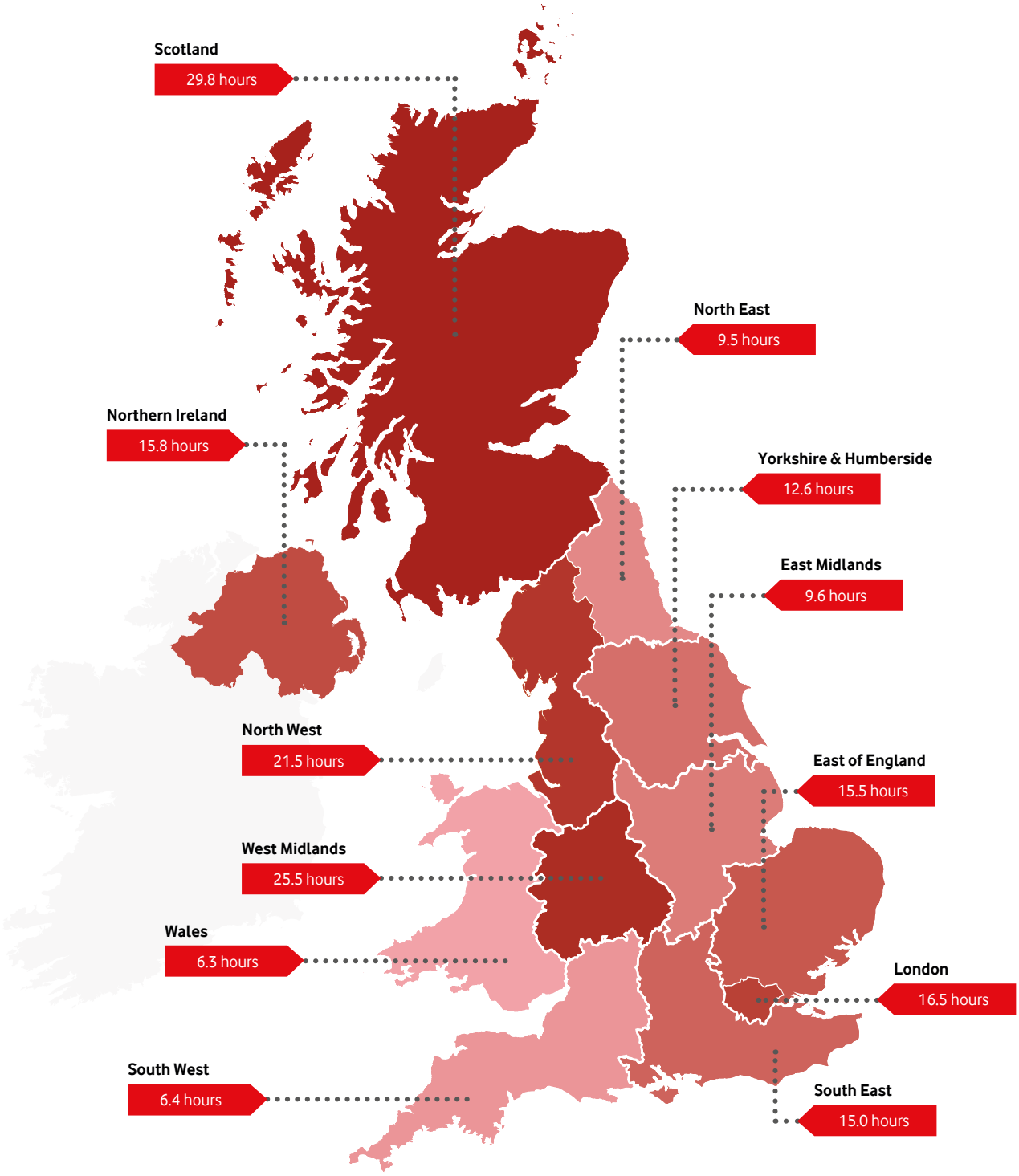
Percentage of SMEs attacked



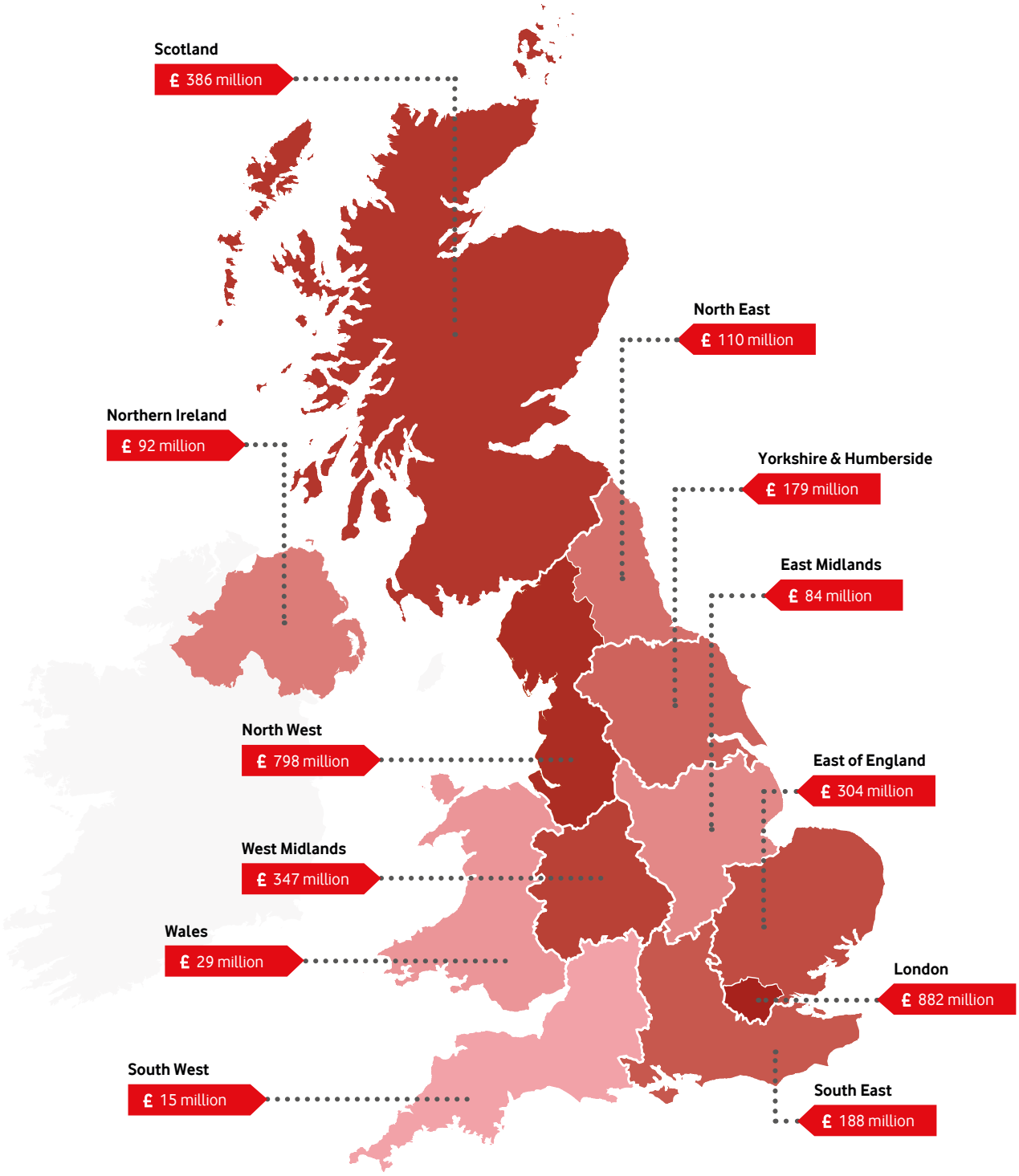
Average lost revenue per SME cyber-attack



Average number of business hours lost as a result of a successful cyber-attack



Total SME lost revenue per year



Our research found that aside from London SMEs in the North East (55%), Wales (46%), Scotland (40%) and the East of England (42%) are more likely to suffer cyber security attacks that other parts of the country. Conversely, SMEs in the South East, South West, West Midlands and Yorkshire and Humber regions all reported fewer cyber security attacks against the average.

Alongside the frequency of cyber-attacks, we looked at how long it takes for SMEs to recover from a cyber-attack. On average SMEs reported losing just under two working days to a cyber-attack. Whilst some regions reported being able to bounce back in just over a day, SMEs in Scotland (29.75 hours), the West Midlands (25.50 hours) and the North West (21.50 hours) all stood out as particularly affected and losing well over the average number of hours to an attack. Understanding why SMEs in these areas are more affected and lose more hours to cyber-attacks than other parts of the country, should be a focus.

Separately when looked at the perspective of revenue lost per cyber-attack, SMEs in the North West stood out against every other part of the UK. On average cyber-attacks cost SMEs nearly £5,000 more than the national average of £3,400. This meant that the region was second only to London in the total cost of cyber-attacks on SMEs, losing £797m in lost revenue. That level of cost could well be hindering the region's burgeoning tech and startup culture.

These findings demonstrate the need for an SME cybersecurity strategy that looks at local factors. It is clear the impact these cyber-attacks have on SME is not uniform across the UK. Understanding the unique scenarios of each SME is challenging, but collaboration with larger businesses can help offer SMEs more tailored support services, like Vodafone's V-hubs, to increase their understanding of NCSC guidance and how they can proactively tackle cyber risks.

Cybersecurity for Business

At Vodafone, we offer a range of cybersecurity services that look to protect, test, and secure businesses of all sizes.[16]

We have in-house cyber security teams and work with industry-leading cyber security partners to offer specialised capabilities - integrated into a single relationship. Utilising these capabilities we offer:

CybSafe portal- This platform is designed to help SMEs improve their organisational risk management, leveraging AI, data, and behavioural science to measure and improve cybersecurity awareness, behaviour and culture within organisations.[17] Launching alongside this report, **Vodafone Business are offering a free, one-month trial of this service**, encouraging SMEs to incorporate cybersecurity into their business-critical decision-making.

Firewall Management- helps reduce vulnerabilities, increases access visibility and optimises efficiencies.

Network Security Assessment and Testing- provides an assessment and test your network security.

Recognising that not every business will require these comprehensive services, tailored support is offered through distinct phone lines depending on the size of your business. This demonstrates how, alongside the free, one-month trial of our Cybsafe portal, Vodafone UK is supporting SME cybersecurity across the UK.

Chapter 3. The Impact of AI

We also explored the impact of AI on cyber-attacks. Nearly two thirds (65%) of SMEs expressed concerns about the technology increasing the frequency and sophistication of cyber security attacks. Our findings demonstrate that as businesses explore the benefits of AI, they need to be prepared for the changing cyber risks that follow.

The rapid development of AI presents both challenges and opportunities for UK SMEs. For cybercriminals, AI provides the potential to create ever more sophisticated attacks that are often automated and difficult to detect. With the ability to cycle through innumerable possibilities and produce realistic 'deepfakes', the threat of AI-phishing campaigns has already seen high-profile businesses fall victim to criminal gangs.[18]

Partnerships with larger organisations like Vodafone can enable SMEs to not only meet the challenges but capitalise on AI.

How has AI-phishing left a majority of UK businesses unprepared?

Vodafone Business has launched an exclusive, free online AI-driven phishing cybersecurity course led by renowned ethical hacker Katie Paxton-Fear.

Available on Vodafone Business and Enterprise Nation's business.connected platform, this expert-led course equips SMEs with the tools to identify and defend against AI-driven phishing scams, including spear phishing, whaling, clone phishing, voice cloning, and deepfakes.

With a PhD in natural language processing and insider threats, Katie – a cybersecurity lecturer at Manchester Metropolitan University - specialises in AI, machine learning, and InfoSec, regularly speaking at major events like BlackHat and OWASP. She also creates cybersecurity education videos for over 30,000 YouTube followers and has reported critical security vulnerabilities to organisations like Verizon Media and the US Department of Defence.

As the rise in AI helps cyber threats become even more sophisticated, this course delivers practical insights and hands-on strategies to help SMEs stay ahead of evolving digital risks. By making cybersecurity education accessible and free, Vodafone Business continues its mission to empower SMEs and strengthen their digital resilience.

Chapter 4. Conclusion and Policy Recommendations

To achieve the UK's mission to drive economic growth, SMEs must harness digital technologies and realise the potential of advanced connectivity. However, to achieve that growth, businesses must protect themselves against the impact of cyber-attacks. This report highlights that more can be done to minimise lost revenue, and support SMEs to invest and scale. More must be done to persuade smaller businesses to embed cybersecurity into their businesses, both through investment and by taking advantage of government resources. Cyber resilience must be seen as a business-critical priority.

Our research puts forward four key recommendations:

1. Increase the funding and expand targeted schemes such as Cyber Local:

Our research illustrates the varied threat landscape that faces SMEs of all sizes. The government's Cyber Local scheme recognises that support can work better when tailored both to the size and location of SME. However, the scheme's successful grants include a wide range of projects with only a few targeting SMEs. In addition, the scheme in its current form only applies to targeted regions in England and Northern Ireland. While it is a welcome step, there is scope to expand the scheme to wider projects that look to support SMEs in all regions of the UK.

2. Targeted SME cybersecurity strategy and campaign to support uptake:

Our research found that the SME awareness of the government's Cyber Essentials programme, last updated in 2022, appears to have decreased since 2023. It is not reaching a large proportion of the UK's SMEs and addressing this knowledge gap among SMEs is crucial. Strategy, direction and awareness are key, ensuring that SME business owners do not just engage with cyber security once an attack has occurred but recognise how they can be proactive in a way proportionate to their size.

Awareness schemes could look to capture SME business owners' attention when they are thinking about their wider business plans. One potential solution could be to offer support and advertise schemes like Cyber Essentials when businesses submit tax and employee data.

Similarly, providing clear, actionable cybersecurity guidance when registering a new business could incentivise new business owners to see cyber security as part of building a business.

3. Making cybersecurity investment an obvious choice:

The tax system has been used in a number of ways over the years to incentivise particularly types of investment by businesses. For instance, Research and Development tax credits and, since 2023, full expensing for plant and machinery have encouraged businesses to invest in their operations and upgrade their hardware.

Government should look at a simple and effective way to encourage cybersecurity investment by SMEs. Introducing a specific tax allowance that enables SMEs to invest in both cyber security hardware and software, in a simple and accessible way could rapidly improve cyber security take up by SMEs. If access was linked to gaining a Cyber Essentials accreditation then SMEs could be encouraged to both become more knowledgeable and invest in greater protection.

4. Encourage more public / private partnerships:

Collaboration with larger businesses is another route to stronger SME cybersecurity. Smaller firms that lack dedicated risk management teams could benefit from learning directly from larger firms that use those resources.

At Vodafone, we have already supported over 1.7 million UK SMEs with accessible education and product support.[19] We welcome additional steps to facilitate collaboration and exchange of knowledge between larger and smaller organisations. Taking these recommendations together, greater awareness campaigns around cybersecurity will hopefully see more SMEs seeking the guidance and support of larger organisations.

Our research demonstrates the considerable added growth potential of SMEs, if businesses can mitigate against the most common forms of cyberattacks. Doing so would open up to £3.4 billion of lost revenue, allowing it to be redirected into investment and jobs. By focusing on collaboration, support and education, the UK can help SMEs scale, thrive and ultimately realise the government's growth mission.

Methodology

1,008 SME business owners (owners of businesses with 250 employees or under) were polled online by independent market research agency Walr. Fieldwork took place between 7th-10th February 2025. Walr is a member organisation of the Market Research Society and abides by all codes of practice.

Utilising these polling results, we have produced economic analysis that looks to examine wider narratives concerning SME cybersecurity across the UK. Looking to map the collective threat to both SMEs and the wider economy, we used the polling data to calculate the regularity, proportion and impact of cyber-attacks that are being directed towards SMEs. This enabled us to create a future 'risk level' for vulnerable businesses.

Going further, we then calculated the average loss of revenue to SMEs and used geometric mean averaging to break down these costs for businesses within specific regions and commercial sectors. The risk level for each sector and region is then applied to the corresponding average cost of a cyber-attack and extrapolated against ONS data on the count and sectoral composition of SMEs by each region to generate a total annualised revenue lost figure.

Endnotes

1 SMEs defined as UK registered businesses with a headcount of under 250 and an annual turnover below £36 million., Gov.uk, Business population estimates for the UK and regions 2024, October 2024
2 NCSC, NCSC CEO's speech to mark the launch of the NCSC Annual Review 2024, 4 December 2024.
3 Vodafone UK, Supercharging Small Businesses, 1 March 2024.
4 Gov.uk, Cyber security breaches survey 2024, 9 April 2024. £6,940 is the mean cost of all businesses who experience an attack and identify a breach with an outcome.
5 National Cyber Security Centre, Small & medium sized organisations, Accessed March 2025.
6 Gov.uk, Cyber Local, 6 March 2025
7 Cisco, Evaluating Security Risk in DeepSeek and Other Frontier Reasoning Models, 31 January 2025
8 Gov.uk, Cyber Security and Resilience Bill, September 2024
9 Gov.uk, World-leading proposals to protect businesses from cybercrime, 14 January 2025
10 National Cyber Security Centre, Cyber Advisor, Accessed March 2025
11 iasme, The benefits of Cyber Essentials certification, Accessed March 2025.
12 Gov.uk, New regional skills projects to bolster UK cyber defences and deliver on Plan for Change, 8 January 2025.
13 Vodafone UK, 1.7 million UK SMEs have upskilled their digital capabilities thanks to Vodafone's V-Hub online service, 30 January 2025.
14 Vodafone UK, How V-Hub advisers make cybersecurity simple for small businesses, 31 October 2024.
15 Gov.uk, Plan for Change, December 2024
16 Vodaone UK, Secure your network with Vodafone Business, Accessed March 2025.
17 Vodafone, Vodafone Business launches cybersecurity platform to help SM&Es reduce human cyber risk, 9 October 2024
18 The Financial Times, Arup lost $25mn in Hong Kong deepfake video conference scam, 17 May 2024
19 Vodafone, 1.7 million UK SMEs have upskilled their digital capabilities thanks to Vodafone's V-Hub online service, 30 January 2025.

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.

April 2025