

DIGITAL REVOLUTION

CONNECTED, SECURE AND DYNAMIC: NAVIGATING OUR DIGITAL FUTURE



FUTURE OF
THE
ECONOMY
WHERE BUSINESS BELONGS



British
Chambers of
Commerce
DIGITAL
REVOLUTION

FUTURE OF THE ECONOMY

WHERE BUSINESS BELONGS

This paper is part of a series of five policy areas which develop realistic recommendations for the future of the UK economy, and fresh and compelling proposals for government.



CONTENTS

Foreword from The Lord Hague of Richmond	4
Introduction from Priya Guha MBE, Chair, Digital Revolution Challenge	5
British Chamber of Commerce Insights	6
Executive Summary and Recommendations	7
Connected, Secure and Dynamic: Navigating our Digital Future	10
Section 1: Digital Connectivity	10
1.1 Broadband	10
1.2 Wireless Connectivity	14
Section 2: Cyber Security	19
Section 3: Artificial Intelligence	24
Appendix	30
References	31
Contributors	35



FOREWORD

THE LORD HAGUE OF RICHMOND



The Lord Hague
of Richmond

It has been 18 months since OpenAI launched ChatGPT3.5, and with it a global race to develop and deploy artificial intelligence.

This technology is driving a rapid wave of technological change across the world, allowing companies to redesign their business models, empowering workers to be more productive, but while also enabling criminals to design more sophisticated cyber attacks. In this new age of limitless opportunities and risks, the businesses that move fastest to adopt this technology will thrive. Those that do not will join the likes of Kodak, Blockbuster, and MySpace in the graveyard of businesses too slow or hubristic to adapt to technological change.

Yet this global race is not only confined to businesses. The economic benefits of a country being at the forefront of deploying this emerging technology are matched only by the geopolitical risks of falling behind their competitors. Helping British businesses to adopt AI and better protect themselves from the threat of AI cyber security attacks therefore must be a critical mission for ministers.

To its credit, the government already recognises its role here. The Department for Science, Innovation and Technology (DSIT) have launched a Flexible AI Upskilling Fund to support SMEs to train their employees in the use of AI. Ministers have created an AI Opportunity Forum of business leaders to discuss how the technology can be rolled out across the private sector. And the Prime Minister has launched a world-leading AI Safety Institute, with a keen focus on mitigating the risks of this technology, including persuadability and cyber threats. But the scale of the task is so great that much more action will be needed in the next parliament.

This timely report sets out the areas in which the next government must take action. It calls for more direct support for firms seeking to adopt AI, such as through courses and webinars. The report advocates faster progress on digital connectivity, both broadband and wireless, and reforms to make it easier for companies to insure for cyber security.

These proposals will help keep Britain at the forefront of the deployment of AI, and should be carefully considered by all political parties crafting their manifestos for government. Only by sustained commitment in each of these areas will the UK and British businesses be able to keep the pace in this ever-accelerating global race.

CHAIR'S INTRODUCTION

PRIYA GUHA MBE



Priya Guha MBE
**Chair, Digital
 Revolution Challenge**

The UK is an incredible place to start, grow and scale a business. As a country, we have a rich history of innovation and a world-leading academic research base that underpins it. The digital revolution provides opportunities for companies to transform in ways that could not have been foreseen a decade ago. However, it also poses a stark risk to the UK's small business economy of being left behind in the race to the UK's digital future and the productivity benefits that this future will bring.

Firms need help to embrace the digital journey and they need to be confident the UK's tech infrastructure is reliable. This report outlines a clear set of priorities for policymakers to implement to support business at this exciting time.

In the Digital Revolution challenge, we made a clear decision to focus on four related areas: broadband, wireless connectivity, cyber security and artificial intelligence. They are the foundations for thriving businesses, now and in the future. Without reliable and secure broadband and wireless connectivity, companies won't be able to fully embrace AI.

Huge strides have been made in broadband provision in recent years, but the UK still lags behind many other countries. No matter the size of your business, or which sector you're in, broadband is now an essential utility we can't do without. We need to improve access, speed and infrastructure planning.

Firms also need better connectivity on the move, to do business wherever they need to. The Government's 5G ambitions must be urgently realised, with the UK leading the world in setting 6G standards. Once again, standing still is not an option.

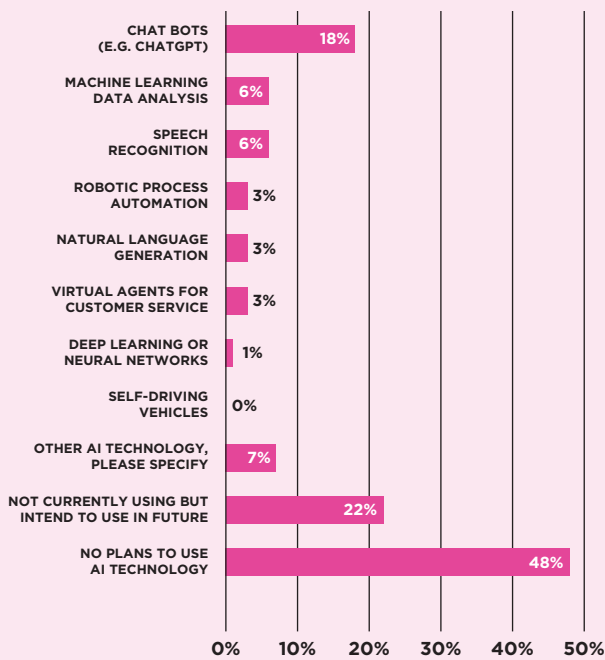
Businesses need confidence that the digital technology they are using is both safe and secure. The threat posed by cyber attacks to businesses is growing. It's crucial that both cyber resilience and insurance are strengthened.

We are still just at the beginning of an exciting story of artificial intelligence and the impact it will have. And there will be other future transformative technologies where the UK is poised to lead. AI is essential for competitiveness and productivity in the modern business landscape, so we must make sure that every UK company is involved in this journey. Improving clarity and certainty amongst business on AI will drive confidence to use it effectively.

The ever-changing world of technology is of huge strategic importance to business. Equipping companies of all shapes and sizes for the digital journey ahead is essential. Both for their own future, and the future of an innovative economy in the UK where all businesses thrive.

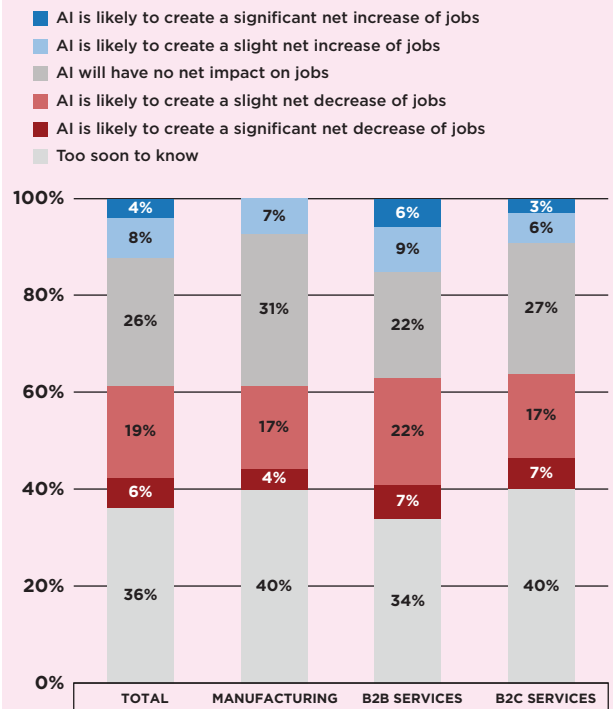
BRITISH CHAMBERS OF COMMERCE INSIGHTS

IS YOUR ORGANISATION CURRENTLY USING ANY OF THE FOLLOWING AI TECHNOLOGIES?



Total: N = 715; Manufacturing: N = 236; B2B services: N = 302; B2C services: N = 140

OVER THE NEXT THREE YEARS, DO YOU EXPECT TO SEE A NET INCREASE OR DECREASE IN THE NUMBER OF JOBS CREATED BY AI TECHNOLOGY IN YOUR SECTOR?



BASE: (Total: N = 694; Manufacturing: N = 229; B2B services: N = 295; B2C services: N = 134)

ARTIFICIAL INTELLIGENCE DATA FROM AUGUST 2023

27%

OVER A QUARTER (27%) OF BUSINESS-TO-BUSINESS SERVICES FIRMS ARE USING AN AI CHATBOT TECHNOLOGY SUCH AS CHAT GPT.

25%

AROUND A QUARTER (25%) OF FIRMS THINK AI WILL CAUSE A NET DECREASE IN JOBS IN THEIR SECTOR, WHILE AROUND 12% EXPECT A NET INCREASE.

DIGITAL CONNECTIVITY DATA FROM FEBRUARY 2023

56%

JUST OVER HALF (56%) OF RURAL BUSINESSES REPORT RELIABLE BROADBAND, COMPARED WITH 82% FOR THOSE BASED IN URBAN AREAS.

EXECUTIVE SUMMARY AND RECOMMENDATIONS

The digital revolution opens a wealth of opportunities for UK businesses of all shapes and sizes. This report outlines a clear roadmap for action from policymakers across a series of interconnected areas. Without better broadband and wireless connectivity – and improved cyber security – businesses will not be able to engage with Artificial Intelligence (AI). In short, businesses want to be connected, secure and dynamic.

The Covid-19 pandemic dramatically increased the importance of business and household internet connectivity, with the provision of broadband a fundamental part of the UK's digital infrastructure. Research by the British Chambers of Commerce has revealed a big divide between businesses based in urban and rural areas: 82% of firms in urban areas agreed they had reliable broadband, which fell significantly to 56% for firms in rural areas. In addition, weak digital infrastructure makes the UK less attractive for foreign investment and limits growth in underserved areas.

Estimates suggest that 5G could be worth as much as £159 billion to the UK economy by 2035, bringing improvement to productivity and spurring the development of connected cities. Businesses across the UK recognise the potential benefits of 5G and want its rollout to be accelerated. Connectivity remains patchy and the 5G rollout is falling behind our competitors. Investors lack the certainty or incentives to invest in the cutting-edge industries of the future. Planning uncertainty and constraints continue to adversely affect network rollout, increasing the cost of infrastructure. Fixed Wireless Access may be part of the solution to business broadband connectivity issues, helping to get better broadband to more places.

It is essential to recognise that the modern economy needs a safe and resilient digital environment. It is concerning that in 2022, the UK was the most digitally attacked country in Europe, accounting for 43% of cases. Large companies risk greater financial losses through a cyber attack, however smaller companies are often more exposed due to comparatively fewer protections. Nevertheless, the threat of cyber attacks also creates an opportunity for the UK to become a world leader in cyber security and the safest place to do business. Businesses must have confidence in the UK's digital infrastructure and must be supported to understand their responsibilities in ensuring the cyber security of their customers.

Finally, the rapid development of AI internationally presents extensive opportunities for businesses across the UK to benefit from its implementation. However, our survey data illustrate a patchy uptake of AI by UK businesses across different sizes and sectors so far. The research also highlights the perceptions, barriers and opportunities that this technology provides. The way the government responds to the development of AI must be tailored to the needs of all businesses – both small and large businesses – to ensure that they can realise the full benefits it presents, as well as mitigate against any possible safety risks.

RECOMMENDATIONS

Digital Connectivity: Broadband

Weak digital infrastructure makes the UK less attractive for foreign investment and limits growth. We call on the government to ensure that the rollout of gigabit broadband is able to benefit all areas of the UK. To ensure that this rollout is sustainable for the future, the government should take steps to support the development of digital skills, protect the management of underground infrastructure, monitor the fibre broadband market, and roll out the “flexi-permits” system to a wider area.

1. The government should take steps to reduce the persistent continuing geographical disparities found in the rollout of gigabit broadband, and ensure that Project Gigabit has a clear strategy for hard-to-reach communities, including tackling affordability issues.
2. The government should explore social tariffs for lower-income areas, to enable more people to access broadband services. Social tariffs could also be made available for small businesses and charities providing access to broadband services and teaching digital skills.
3. The ambition of government around the management of underground assets must be greater. There should be a full Digital Twin for underground assets. There must also be an urgent investigation into the risk of undocumented incursion into our underground infrastructure.

Digital Connectivity: Wireless Connectivity

Connectivity across the UK is patchy and 5G infrastructure is struggling to keep pace, preventing users from being able to fully reap the benefits of this technology. The UK needs to have a leading role in research and development, ensure that it has the network and planning infrastructure to benefit from this, and harness the role of local authorities to help drive the transition.

1. The government should strive for the UK to be at the forefront of research and development, building a network that can be looked at in the early 2030s as genuinely world-leading and setting the standards for what 6G technology will look like.
2. Network infrastructure should be strengthened through a pro-investment policy framework, supported by a planning regime that unlocks the UK’s 5G ambitions.
3. Business rate reductions should be introduced for 5G infrastructure development, taking a similar approach to full fibre between 2017 and 2022.

Cyber Security

Businesses must have confidence in the UK's digital infrastructure, and the government must demonstrate that it is able to address cyber security risks that are posed to the UK. It needs to promote the opportunities for businesses to benefit from strong cyber security training, and ensure a cyber reinsurance scheme to make it the insurer of last resort.

1. The government should work with the insurance industry to create a reinsurance pool that underwrites cyber risk and promotes effective cyber security practices for all UK businesses.
2. The government should increase business awareness of and access to cyber security training. This will provide them with digital confidence to tackle security concerns and prevent imbalances in how resilient firms of all sizes are to the threat of cyber crime.
3. Government guidelines should represent a clear standard for businesses to aspire to rather than a burden on small and resource-strained companies.

Artificial Intelligence

We support the approach that the UK government is taking in relation to AI regulation and propose additional steps that will create a framework of trust for businesses. This will ensure that they are aware of AI and know how to use it for their business, that they are able to communicate any key feedback to the government to ensure that the regulation of AI remains focused on innovation, and that they are able to engage with other stakeholders to fully benefit from the implementation of AI.

1. The government should create a Small and Medium-sized Business AI Programme to inform business owners about practical ways AI can enhance their operations, and also appoint a Business AI Champion.
2. The government should support the development of long-term AI, data science and digital skills by providing specific funding for AI apprenticeships (including both young people and to support lifelong learning), and to make these available to at-risk industries such as the creative sector.
3. The government should champion UK business AI adopters abroad through the GREAT Campaign and set up a specific programme to support UK businesses to export AI products to international markets.



CONNECTED, SECURE AND DYNAMIC: NAVIGATING OUR DIGITAL FUTURE

SECTION 1 DIGITAL CONNECTIVITY

1.1 BROADBAND

Background and policy framework

The Covid-19 pandemic dramatically increased the importance of business and household internet connectivity, with the provision of broadband a fundamental part of the UK’s digital infrastructure. A UK policy framework and subsidy regime to deliver broadband infrastructure has been in place for many years.

Research by the British Chambers of Commerce (BCC) in Spring 2023 sought to understand whether UK businesses felt that their local area had reliable broadband. The survey of 1,045 firms, 88% of whom were SMEs, found that overall, 28% strongly agreed that their local area had reliable broadband, while 49% somewhat agreed, 13% somewhat disagreed, and 9% strongly disagreed. This means that overall, 77% agreed and 22% disagreed.

However, the research also revealed a big divide between businesses based in urban and rural areas. 82% of firms in urban areas agreed they had reliable broadband, which fell significantly to 56% for firms in rural areas.

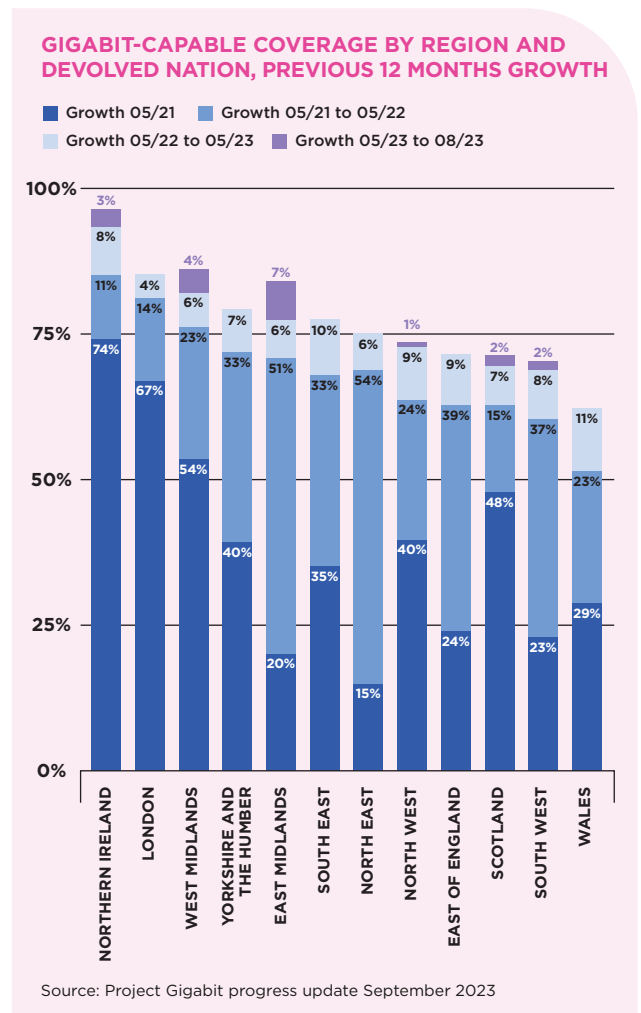
“Superfast” and “Gigabit”

The initial focus from 2010 was the roll-out of “superfast” broadband (less than 30 megabits per second (Mbps)). This was delivered to 96% of homes as of September 2021, with the private sector delivering to most of the county, and the government providing subsidies for areas not reached in this way.ⁱ The UK government is now focusing on deploying the more powerful gigabit broadband network, which provides capacity of 1 gigabit per second (Gbps), equal to 1,000 Mbps.

The policy framework for gigabit broadband follows broadly the same model as superfast. Private investment is expected to account for most of the country (around 80% of premises), with the government supporting delivery to the remaining 20%, through the Project Gigabit initiative.ⁱⁱ

Progress on rollout

Progress on providing high-speed broadband to British businesses is broadly positive, but with glaring disparities by geography. In May 2023, 51% of business premises had access to gigabit-capable broadband, comprising 28% of business premises coverage in rural areas and 55% in urban areas.ⁱⁱⁱ Looking across all premises, there is a wide variance in gigabit coverage across the UK, with the lowest coverage in Wales and the South West (see chart).



International comparisons

International comparisons do not paint the UK in the most positive light. European countries with the highest levels of gigabit coverage include Denmark, Spain, and the Netherlands, all of whom had reached over 90% of premises. As of July 2023, the

UK had 40% gigabit coverage. This was lower than all EU countries except for Greece.^{iv} The UK should take learnings from the models used successfully internationally, or risk slipping behind competitors; weak digital infrastructure makes the UK less attractive for foreign investment and limits growth in underserved areas.

Looking at a specific country example that could serve both as an aspiration and a roadmap; South Korea's broadband infrastructure is considered one of the most advanced in the world, with a penetration rate of 97.6% as of 2023. Here, digital exclusion was tackled early, with the South Korean government initiating an ambitious universal service programme for broadband from the mid-1990s. The South Korean government has also made use of public-private partnerships to deliver rural broadband, incentivising rollout by offering providers contracts that allow them to recover the investment cost per building within a reasonable period.^{vi}

The UK approach: Project Gigabit

To address these issues, the UK government introduced Project Gigabit, a £5 billion programme launched in 2021, to provide gigabit-capable broadband to over a million households and businesses across the UK, particularly those in rural and remote communities.

This approach has three main strands. First the main part of the programme is a series of procurements to subsidise the roll-out of gigabit-capable broadband in specific areas, with successful bids often including an element of match funding.^{vii} Second, the Gigabit Broadband Voucher Scheme provides up to £4,500 in funding to cover the installation costs of gigabit broadband for households and businesses. Finally, there is funding to connect public sector buildings to serve as 'GigaHubs', providing a platform for suppliers to extend connectivity in the surrounding communities.^{viii}

Project Gigabit has faced criticism. A survey by National Broadband found that just one out of the ten local authorities with the worst broadband connectivity in the UK had received any funding from the project, with the group's analysis showing that funding was primarily going to more densely populated areas where provision is easier and cheaper to provide.^{ix}

The report also found regional disparities in funding, with just £42.3 million allocated to the South-West, which has the highest count of premises unable to access landline broadband speeds surpassing 10Mbps, compared to the £250 million received by the South-East and East of England.

Separately, the Public Accounts Committee has argued that the approach taken by Project Gigabit risks perpetuating digital inequality across the UK having, in its view, failed to set out a viable plan to connect the communities that are the hardest to reach.^x

Connecting very hard to reach premises also incurs disproportionately rising costs for broadband providers; costs that providers are not required to meet when they exceed their Universal Service Obligation mandated cost-threshold (£3,400 per premise).^{xi} The government is attempting to overcome this by exploring how new technologies such as satellites can connect the 3% of premises in the most remote areas.^{xii}

Digital Inclusion

Another challenge to uptake is the price of the broadband service. Whilst the government may achieve 85% coverage by 2025, many consumers – discouraged by the higher prices of a new service – are not signing up to use the services. A survey by Citizens Advice claims that as many as million people disconnected their broadband in over a 12-month period from February 2023 last year because they could not afford it.^{xiii} This has a knock-on effect for telecommunications firms, who may not enjoy the expected returns on investment due to lower customer numbers.^{xiv}

In addition, the lack of digital skills means that many people are simply unable to take advantage of job opportunities that they could do from home. Futuredot.now estimate that almost 60% of the UK's workforce (23.4 million people) is unable to do all 20 digital tasks industry and government have defined as essential for work.^{xv} As the workforce gets older, and more of the working world becomes digitised, there must be a focus on in-work upskilling and retraining to support lifelong learning.

Finally, the availability of equipment is a major problem, deepening the digital divide, with numerous authorities and charities working on device donation and reuse schemes.^{xvi}

Broadband Infrastructure: Challenges and Solutions

Coordination of street works

Street works are a significant element of telecoms infrastructure builds. The government estimates that street works account for 70% of the cost of fibre broadband deployment.^{xvii} Currently a permit is needed for each street on which works will take place, with operators and utilities seeking permits and approvals for each hole they dig, creating pressure on utilities and local authorities.^{xviii} A solution to this is to introduce “flex-permits”; i.e. one permit to cover a number of minor and standard works in a specified area.^{xix} This had originally been the government’s intention, however it retreated from introducing flex-permits following opposition from highways authorities.^{xx}

Underground infrastructure:

Damage, Security and a Digital Twin

Each year in the UK, around four million holes are dug to install, operate, maintain and repair underground assets, with one in every 65 holes dug resulting in accidental damage to buried infrastructure (some 60,000 a year). This damage is partly due to a lack of knowledge about what assets exist underground. Currently, this type of information is held by over 700 different organisations across the UK with varying quality of record-keeping.^{xxi} The BCC strongly strongly advocates data sharing between agencies.

Another concern around underground assets is a lack of real-time information for managers as to who has gained access to them. There is currently a genuine risk that hackers could gain access to and deliberately sabotage our critical national infrastructure.

Currently the government’s response to issues has focused the first of these issues, through the National Underground Asset Registry (NUAR) project in England, Wales, and Northern Ireland (with a similar scheme, VAULT, in Scotland) to create data-sharing platform on the location and condition of underground assets. According to the project’s objectives, this will provide an interactive, standardised digital view of the underground assets in each location by the end of 2025.^{xxii}

This does not go far enough. We propose that a full Digital Twin for underground assets should be created.^{xxiii} This would create a full digital representation of the structures found underground, as well as information on the type and ownership of these assets. Digital Twins are operational in various sectors including ports and other infrastructure systems, manufacturing, healthcare, automotive and urban planning; where these systems can already display 3D and 4D spatial data in real time and incorporate augmented reality systems into built environments.^{xxiv}

When fully operational, the Digital Twin would be automatically updated with any changes to the underground assets, including alerting asset managers that there has been access to the network, and flagging which of the various owners and managers are carrying out the work. This would also be able to recognise non-authorised access. While this approach may seem like science-fiction, it is already being used elsewhere; Incheon in South Korea has a digital twin which will soon be used to manage underground assets, such as sewer systems, power grids, telecommunications, subways and even natural gas lines.^{xxv}

Ensure fair competition in the Broadband sector

The government’s view is that enabling competition is the most appropriate way of rolling out gigabit broadband infrastructure. Ministers and Ofcom have tried to reduce barriers to entry for alternative network operators (“altnets”) to build full fibre networks in competition with Openreach.

As a result, alongside Openreach’s plans to upgrade its copper network to full fibre there are now numerous altnets building competing full fibre networks. The larger operators include City Fibre and Hyperoptic, with others operating on a regional or local level, including Wildanet (South West England) Wight Fibre (Isle of Wight), and Ogi (south Wales).^{xxvi} The Openreach Fibre To The Premises (FTTP) network reached 10.3 million premises in March 2023, with AltNets (Alternative Networks) reaching over 8 million premises.^{xxvii}

Competition is regulated by Ofcom; this is important given that BT and Openreach were fully vertically integrated until 2017, when under a voluntary agreement BT and Openreach undertook commitments to safeguard competition, including introducing a degree of functional separation.

A full review of the commitments and overall competition performance of the sector is outside the scope of this report, but Ofcom's view, in summary, is that the commitments are functioning well, and that despite several issues raised by competitor networks, they have not found any reasons to investigate complaints.^{xxx}

This view is in stark contrast to the independent association representing altnets, which points to issues such as a reluctance to switch customers, and a risk of inefficient "overbuild" by Openreach in areas where altnets exist. While all sides agree that customers have benefited from greater competition, the debate over competition in the Broadband sector continues.

Business Rates Relief for new fibre broadband infrastructure

In 2017, the government introduced 100% business rates relief to new fibre infrastructure built in England for five years from April 2017 to March 2022. The relief was not extended. In contrast, the Scottish government has introduced non-domestic rates relief for new fibre broadband infrastructure in Scotland for 10 years from 1 April 2019. Given the long-term investment horizons required for the broadband rollout, a longer-term tax relief is needed. Openreach has argued that return on investment in digital infrastructure "takes decades" and that investors need a "clearer long-term commitment" from the government.

RECOMMENDATIONS

- The government should take steps to reduce the persistent continuing geographical disparities found in the rollout of gigabit broadband and ensure that Project Gigabit has a clear strategy for hard-to-reach communities, including tackling affordability issues.
- The government should explore social tariffs for lower-income areas, to enable more people to access broadband services. Social tariffs could also be made available for small businesses and charities providing access to broadband services and teaching digital skills.
- The ambition of government around the management of underground assets must be greater. There should be a full Digital Twin for underground assets. There must also be an urgent investigation into the risk of undocumented incursion into our underground infrastructure.



1.2 WIRELESS CONNECTIVITY

Introduction

Wireless connectivity will lay the foundations of a brighter digital future for the UK. 5G could be worth as much as £159 billion to the UK economy by 2035, bringing improvements to productivity and spurring the development of connected cities.^{xxxii} Businesses up and down the country recognise these potential benefits and want the 5G rollout to be accelerated so they can be unlocked. This is particularly the case in traditionally underserved and poorly connected parts of the UK, with the Country Land and Business Association finding that 80% of rural business owners had said that improved connectivity would be the single largest improvement to their business.^{xxxii}

But in the UK today, connectivity remains patchy and the 5G rollout is falling behind our competitors. The EU 5G Observatory found in Spring 2023 that the UK ranked 17th out of 28 for 5G population coverage when compared to the 27 EU nations,^{xxxiii} and Open Signal found that the UK ranks 49th out of 56 countries in terms of average download speeds, falling behind Germany, France, and the USA.^{xxxiv} Investors currently lack the certainty or incentives to invest in the cutting-edge industries of the future. This is risking the ability of businesses to maximise opportunities and could hold back the potential for Britain to be a world leader in everything from AI and machine learning to self-driving vehicles and digitally integrated hospitals.

Context: How is the UK doing?

In April 2023, the government published its Wireless Infrastructure Strategy, setting out its vision to connect the UK with the fastest, most reliable wireless coverage available.^{xxxv} The Strategy included an ambition for all populated areas to be covered by standalone 5G by 2030. The Strategy also included £40m funding to improve uptake of 5G services, including the establishment of ten '5G Innovation Regions' across the UK, and £100 million investment in the future of 6G through R&D. It also restated the government's ambition for 95% coverage of 4G by 2025 as part of the Shared Rural Network agreement.

Alongside the Strategy, DSIT also announced:

- A Rural Ten Point Plan, to support rural communities by bringing together key government actions (mobile coverage reporting, 5G adoption campaign, Project Gigabit funding, etc).
- £8 million fund to provide capital grants to connect remote premises

While the Strategy represents an important step towards creating a more attractive policy environment for investment in wireless connectivity and improving the quality of the UK's telecommunications networks, there is still a lot of work to do to realise its ambitions.

Achievements to date

The Strategy outlined progress over the last five years in the deployment of 'world class fixed and wireless networks' across the UK, including:

- Investing £5 million through Project Gigabit, to achieve gigabit broadband to at least 85% of premises by 2025.
- Reaching a £1 billion deal with mobile network operators to support rural communities to ensure that over 95% 4G coverage by 2025, through the Shared Rural Network agreement.
- Deploying 5G to achieve the goal of majority access to 5G by 2027.
- Strengthening network security by implementing the Telecommunications (Security) Act 2021 and the 5G Supply Chain Diversification Strategy.

On connectivity across the UK more broadly, Ofcom's annual 'Connected Nations' report for 2023 found that:^{xxxvi}

- 93% of UK landmass had 4G coverage from at least one operator, while 71% had 4G coverage from all operators. However, 7% had no 4G coverage.
- Coverage varies across the UK, with urban areas enjoying better coverage than rural areas. Nations and regions with high proportions of rural areas, such as Scotland, Wales, and the North East, experience the lowest 4G coverage across their landmass.
- The level of 5G coverage provided outside of premises by at least one mobile network operator rose from 67-78% in 2022, to 85-93% in 2023. 5G traffic has shown around 140% growth.

Whilst the Wireless Infrastructure Strategy and other related policy initiatives have provided welcome momentum around the deployment of wireless connectivity, there are still areas where the government and industry can, and should, collectively do more to ensure the UK remains at the forefront of the digital revolution.

There are several key challenges holding back the UK's ambitions, which the government in partnership with industry must focus on to realise the benefits of wireless connectivity:

- High costs associated with upgrading and maintaining networks – amid little progress on the deployment of OpenRAN (Open Radio Access Network) in the UK despite government commitments.
- Uncertainty with 5G demand and limited awareness of its benefits.
- The need for higher quality connectivity in national public networks.
- Persistent disparities in wireless connectivity across different parts of the country – creating a rural / urban divide.
- Access to spectrum is becoming increasingly competitive.
- The need to keep private networks secure, considering their increasing number.



5G rollout

The rollout of 5G promises faster connectivity, increased capacity, and improved latency — allowing more users and devices to access high-speed internet and handle substantial data simultaneously. It has the potential to supercharge innovation and efficiency throughout the economy, transforming business operations through greater digitisation and automation, and driving competitiveness. It can offer more secure and resilient networks and facilitate new working practices and uses such as augmented or virtual reality.

The government expects widespread adoption of 5G to bring a cumulative productivity benefit of £159 billion by 2035 – acting as the digital fabric that will underpin autonomous vehicles, smart cities, automated factories, and remote healthcare. The adoption of 5G could add as much as £6.3 billion to the value of UK manufacturing by 2030 alone.^{xxxvii}

The initial rollout of 5G marks the starting point of the journey towards advanced 5G adoption — standalone 5G or 5G plus. Standalone 5G represents a mobile network with a core infrastructure specifically designed to support 5G services, whereas current 5G offerings in the UK essentially involve integrating a 5G Radio Access Network (RAN) onto existing 4G infrastructure. While this technology surpasses 4G, it does not represent the technological leap needed for the digital revolution. In contrast, standalone 5G will deliver ultra-low latency and a significantly more capable network.

To pave the way for this future, we need a relentless focus on unlocking investment in networks, breaking down barriers to deployment, and positioning the UK as a leader in research and development of future telecommunications.

Government performance on 5G rollout

The government's performance on 5G is mixed, and any delays to the rollout could cost the UK tens of billions of pounds in lost economic output. Although the UK was among the early global adopters of 5G in 2019, it has since fallen behind pioneering nations such as South Korea and China. The density of base stations per person trails behind the EU, US, and much of Asia, and operators are facing ongoing challenges with meeting network demand, which is comparatively high in the UK.^{xxxviii}

As people use more and more data, 5G infrastructure is struggling to keep pace, preventing users from fully reaping the benefits of this technology. In December 2023, Opensignal data revealed that UK mobile users experienced the slowest average 5G download speeds among G7 countries, measuring 118.2 megabits per second between August 1 and October 29, 2023 – a 13% decline compared to the same period in 2022.^{xxxix} The challenge of meeting network demand is leading to consolidation by mobile operators and underlining the need for adequate spectrum allocation.

This decline in performance follows warnings about insufficient investment, persistent barriers to infrastructure deployment, and disruption arising from the government's ban on equipment from Huawei, prompted by national security concerns.

In 2022, the Digital Connectivity Forum and Frontier Economics found that, under current conditions, the industry is projected to invest around £9 billion in new network infrastructure by 2030.^{xl} According to the research, this falls far short of the cost of delivering full 5G – estimated to be an additional £23-25 billion. The report argued that while the projected investment will increase capacity, it will not unlock the transformative services dependent on advanced 5G. The UK government last year announced an investment package worth £150 million over the next decade to boost 5G adoption, but this lags far behind international competitors, with the US investing up to \$9 billion and South Korea set to invest \$130 million in 2024 alone in what is a much smaller market.^{xli, xlii}

However, the National Infrastructure Commission has stated that industry will deliver 5G networks across populated areas of the UK without the need for subsidised rollout in the near term.^{xliii} While the Commission recognises that the investment climate for new mobile networks is challenging, it has argued that competition between operators and announced plans for further rollout indicate there will continue to be significant network investment over the next decade.

The recent announcement of the proposed merger between Three UK and Vodafone exemplifies the ongoing trend of telecom operators consolidating to strengthen their positions in the market and pool resources for significant 5G investments. This move follows the footsteps of previous mergers, such as the consolidation between BT and EE, and Virgin Media and O2 (VMO2), highlighting the industry's strategic shift towards collaboration to navigate the challenges and capitalise on opportunities in the dynamic telecommunications landscape. As these mergers unfold, the combined entities aim to not only optimise operational effectiveness but also leverage the pool of private capital to propel the rapid deployment of cutting-edge 5G technologies.

Policy challenges

Industry is clear that the regulatory and policy landscape in the UK needs to respond to the prohibitive costs of deploying digital infrastructure if the full benefits of 5G are to be realised. Industry revenues have been in decline, and according to Vodafone, returns over the last 10 to 15 years have not enabled recovery of investments.^{xliiv} While the government's current approach has been to introduce "a range of measures" to support commercial investment, it remains unclear whether these will be enough to drive the infrastructure upgrades required.

There is also an open question as to how the rural / urban divide will be addressed in the 5G rollout. While the Shared Rural Network is focused on extending 4G coverage to rural areas, there is at present no equivalent funding programme to support the rollout of 5G. The Rural Services Network criticised the lack of direct funding in the government's Wireless Infrastructure Strategy, stating: "Even where there is a marginal commercial case rural areas will be at the end of the queue for commercial investment. Only significant government investment can hope to combat the market failure referred to".^{xlv}

The UK was one of the first countries in Europe to ban Huawei from its 5G networks in 2020. It has been a policy leader in OpenRAN – outlining a 5G Supply Chain Diversification Strategy,^{xlvi} setting a goal of having 35% of its telecom network traffic carried over OpenRAN by 2030^{xlvii}, and establishing OpenRAN principles in 2022^{xlviii}, backed by Australia, Canada, and the US. However, its allocated funding remains low – £88 million of funding to date,^{xlix} compared to \$9.1 billion investment from Nokia and Ericsson collectively in 2022. There is therefore little incentive for mobile operators to deploy interoperable 5G infrastructure, especially given the lack of consensus on the benefits in terms of lower costs.

Despite progress in areas such as reforms to planning rules to allow for taller and wider masts, mobile operators have warned that planning uncertainty and constraints continue to adversely affect network rollout, increasing the cost of infrastructure. Barriers include securing planning permissions, negotiating agreements to access land, and coordinating with local authorities to conduct street works.¹ With significant resourcing shortages, and councils spending less on planning due to funding constraints, it remains to be seen whether the planning system will be able to cope with the swathe of planning applications for new network infrastructure.

The Future Look — Fixed Wireless Access

When we invest in the future of connectivity, we should be looking to solutions that will stand up to future needs, rather than securing a minimum service that is rapidly overtaken by increasing demand. Fixed Wireless Access (FWA) may be able to form part of the solution. FWA is where an internet signal is sent from a mast providing 4G / 5G mobile broadband, to a fixed receiving point within a premises. In assessments by Analysys Mason, FWA with direct line of sight was judged to be capable of delivering gigabit speeds, even without a fixed connection.ⁱⁱ

FWA can, to some degree, ‘piggyback’ off of the rollout of 5G around the country, as the technology can use phone masts for its primary stations. While FWA does have some issues, in particular when upper capacity limits begin to be reached, it has the potential to provide a solution for some of the communities who would otherwise be most at risk of being left behind. Worldwide growth in the technology has been substantial, in particular in North America, where it has been used to great effect in more rural areas.ⁱⁱⁱ

With targeted investment and support from the government, FWA could capitalise on the rapid pace of 5G rollout to get faster, better broadband to more places, sooner than the government’s current plans. Rather than being seen as a solution ‘instead of’ the current Project Gigabit plans, it should be seen as an ‘as well as’ strategy — so that communities and businesses can benefit as quickly as possible. Good and reliable broadband reaching rural communities is essential for ensuring that opportunity is open to all, and that businesses are not disadvantaged simply by virtue of starting in the middle of ‘digital deserts’.

RECOMMENDATIONS

- The government should strive for the UK to be at the forefront of research and development, building a network that can be looked at in the early 2030s as genuinely world-leading and setting the standards for what 6G technology will look like.
- Network infrastructure should be strengthened through a pro-investment policy framework, supported by a planning regime that unlocks the UK’s 5G ambitions.
- Business rates should be introduced for 5G infrastructure development, taking a similar approach to full fibre between 2017 and 2022.



SECTION 2

CYBER SECURITY

Introduction

From global supply chains to micro-businesses, the modern economy simply cannot function without a safe and resilient digital environment. It is therefore concerning that, in 2022, the UK was the most digitally attacked country in Europe, accounting for 43% of cases, with around a third of businesses reporting a cyber security breach or attack.^{lviii} BCC research shows that more than half of UK firms believe their exposure to cyber attack has increased due to working from home arrangements. As AI further increases the surface area of the digital world, immediate action must be taken to protect against cyber crime and get ahead of the threat.

Cyber security is both a daunting prospect and pressing risk for business. According to the House of Commons Justice Committee, cyber-enabled fraud represents 22% of all reported crime and yet just 2% of police resources are allocated to investigating it.^{lv} Businesses perceive their exposure to cyber crime to be much higher than to physical risks such as drought and flooding; BCC survey data shows that just 2% of businesses do not feel at all exposed to the threat of cyber crime, compared to 45% who do not feel exposed to flooding and 58% who do not feel exposed to drought.^{lvi}

Large companies risk greater financial losses through a cyber attack, however smaller companies are often more exposed due to comparatively fewer protections. There is a misconception that cyber attacks are targeted at an individual or business. However, they target vulnerabilities – any business, regardless of size, with that vulnerability can become a victim.

Meanwhile, shifting geopolitical and technological forces have led to a rise in rogue states and malicious actors targeting our digital world. Critical

national infrastructure (CNI) and supply chains are key targets for cyber attacks, leaving the UK economy exposed to large-scale shocks if adequate protections are not put in place in the event of systemic attack. In December 2023, Parliament's Joint Committee on the National Security Strategy (JCNSS) published a report warning that the UK is unprepared for the "high risk" of a catastrophic ransomware attack "at any moment", and that there would be "no excuse" for the current failure to invest sufficiently to prevent a major crisis.^{lvii}

However, this emerging threat also creates an opportunity for the UK to become a world leader in cyber security and the safest place to do business. To grasp this opportunity, the government must safeguard growth by building resilience to cyber threats and supporting business to face cyber security head on. Businesses must have confidence in the UK's digital infrastructure, and that there is protection in the economy for when things go wrong. Firms must also be supported to understand their responsibilities in ensuring the cyber security of their customers.

Government-backed cyber reinsurance scheme

The UK has been subject to multiple economic shocks in the last two decades which have caused significant upheaval. The necessity of bailouts and huge government interventions during the collapse of the banks, the Covid-19 pandemic and the energy crisis have greatly increased the UK's debt. The Institute for Fiscal Studies has warned that "high levels of debt can bring risks – pushing up the cost of servicing that debt and reducing the government's available fiscal space to respond to adverse shocks in future".^{lviii} This highlights the need for the government to take preventative measures to increase economic resilience in the face of such shocks.

A catastrophic cyber attack has the potential to bankrupt thousands of businesses and destabilise the UK economy. Currently, many insurance companies are unwilling to offer cyber insurance, and those that do exclude the most worrying events such as CNI failure. Insurance policies also typically exclude ‘acts of war’, which further limit the success of the insurance market as many of the most critical cyber attacks are conducted by actors affiliated with a hostile government. Furthermore, the cost of cyber insurance that is available is prohibitively high for many small businesses and so penetration is low – only 7% of all businesses in the UK have a specific cyber security policy, and the figure is likely to be even lower for SMEs.^{lix}

On the demand side, SMEs have low awareness of the risk mitigation and protection that is available to them. Those that do attempt to purchase cyber protection find the insurance application process complicated and unstandardised, representing a barrier to take-up.

On the supply side, large companies are not able to obtain cover proportionate to the threat that a cyber attack poses to their business. Furthermore, large companies lose a far greater amount on average than their smaller counterparts when they are the victims of cyber crime such as fraud.

This situation represents a market failure to provide the possibility of adequate protection to the UK business community from both an insurance and cyber security perspective. Where the private sector is unable to provide adequate insurance, the state becomes the de facto insurer; in the event of a catastrophic attack, the government alone would face political pressure necessitating action potentially costing billions of pounds. A recent OBR scenario modelled an economic impact of £29 billion for an attack on the UK electricity grid,^{lx} and the National Risk Register 2023 categorised a failure of the grid as the second most likely risk to manifest in the top ‘catastrophic’ impact bracket, behind only a pandemic.^{lxi}

To give the private insurance market the confidence to provide affordable and comprehensive cover, and to distance the taxpayer from the potential cost of a catastrophic cyber security breach, the BCC recommends a government-backed cyber reinsurance scheme. This would make the government the insurer of last resort, transferring risk to insurance companies while allowing the insurance companies to provide more innovative products as they do not need to hold the capital necessary to cover a systemic attack.

Insurance has the potential to directly improve resilience by incentivising policy holders to take preventative measures in return, for example, for cheaper cover. A reinsurance pool would not only reduce the potential impact of a catastrophic attack on the UK economy but would make cyber attacks less frequent through prevention – by definition lowering the risk of cyber attack and further reducing insurance premiums.

In December 2023, the Joint Committee on the National Security Strategy (JCNSS) recommended “the government should work with the insurance sector to establish a reinsurance scheme for major cyber attacks [...] to ensure the sustainability and accessibility of the market”.^{lxii} The government has previously stated it believes that the private market is providing adequate cover. This is simply not the case, and premiums will only become less accessible to business as the frequency and impact of cyber attacks increase.

The Joint Committee is not alone in this recommendation. In the US, the Treasury has confirmed its intention to explore options for a public-private partnership that would provide a federal backstop against a catastrophic cyber incident. Within the UK insurance industry, companies want a reinsurance scheme as this allows for business expansion and greater protection from risk.

As consensus builds across the insurance industry and governments around the globe, the UK should act quickly to be a global leader in cyber security insurance and become the safest place to do business in the world, with the most resilient growth.

CASE STUDY

REINSURANCE SCHEME MODELS AND PRECEDENTS

Pool Re is the insurance industry's mutual for reinsuring terrorism risk in Great Britain. It was founded as a public-private response to the market failure prompted by the IRA bombings in the early 1990s and has since re-established a private terrorism insurance market which makes comprehensive commercial property cover available to any business in Great Britain.

Today, the pool provides reinsurance cover to £2.2 trillion of UK assets and businesses, from shopping centres and local traders, to airports and power grids, across sectors of the economy including real estate, transport, construction, and energy.

Through the fund it has built up over its history, the scheme can meet the economic impacts of terrorism incidents up to around £12 billion. After that, the scheme is backed by a government guarantee, or loan facility, which it has never called upon in its history despite settling over £1 billion in claims.

By assuming the tail-end of an extreme risk for which it is in any case the insurer of last resort, the government enables commercial (re) insurers and capital investors to re-enter the market, stimulating innovation, resilience, and the provision of insurance protection to businesses which would not be possible otherwise.

In exchange for the government-backed loan facility, Pool Re pays a dividend to the Treasury (HMT), funded by its premium receipts and investment income. Since 2018, the scheme has contributed approximately £1.2 billion in revenue to the government.

Pool Re's £12 billion+ private financing structure insulates HMT and the taxpayer from all but the most extreme financial consequences of terrorism; the probability of the guarantee being called upon in any given year is estimated at 1 in 1,500 years.

Pool Re is an Arm's Length Body (ALB) of HMT, staffed by experienced (re)insurance

professionals, actuaries, and counter-terrorism experts who are able to deliver the government's economic and national security objectives. A proportion of the Pool Re fund is invested in national resilience schemes, meaning not only are preventative measures encouraged by the insurance industry offering better coverage, but the scheme invests directly in national mitigation measures through the Home Office.

Other options are possible, and other models of reinsurance pools have been successful. For example, Flood Re, which reinsures flood risk allowing homeowners at a high risk of flooding to access flood insurance. This model operates through a levy on all UK household insurers, allowing the scheme to effectively operate with a loss despite being entirely self-funded.

Two shorter schemes were introduced during the Covid-19 pandemic. The Trade Credit Reinsurance (TCR) Scheme was introduced when up to 55% of trade credit insurance was expected to be withdrawn after disruptions to global supply chains. The government's evaluation of TCR found that reinsurance is an effective intervention to ensure policy holders are protected, while the Scheme resulted in a net surplus for HMT.^{lxiii}

The Live Events Reinsurance Scheme gave event organisers the confidence to continue with business operations in the later stages of the Covid-19 pandemic, as they were able to access cancellation cover which the insurance market was not providing. The scheme supported over 14,000 jobs in the events industry.^{lxiv}

Supporting businesses to protect themselves

There is an increasing amount of cyber security training and guidance available for businesses from both the government and private sector; however, awareness and confidence are still low. Evidence from our network of 52 Chambers suggests that small businesses are at risk of being more exposed than larger businesses as they perceive cyber security precautions to be too difficult or expensive to keep up with. Research produced by the BCC in 2022 revealed four out of five UK firms did not have accredited cyber security measures in place to protect against attacks.

Many cyber crimes can be prevented by small steps such as good password management and installing anti-virus software. However, businesses do not know where to start in taking steps to protect themselves and can be put off by additional costs. Prevention and precautions could be incentivised by reducing the cost burden of software and training.

From a communications perspective, cyber security should be reframed as an investment to emphasise the business case for taking steps to reduce exposure to cyber threats, both for financial and reputational risk mitigation. This must be an ongoing campaign as there is no end point where society is fully protected from attack – cyber criminals become more sophisticated and technology becomes further embedded in the economy, necessitating constant vigilance.

Furthermore, businesses who have good cyber security will be more insulated from the threat, and therefore may not feel at risk as they think they have not been attacked. This could lead to budget-stretched businesses cutting cyber protections when under financial stress, and then becoming exposed to cyber attacks. The narrative of constant cyber protection as an ongoing investment for the future should be highlighted in as many communication channels with businesses as possible.

Local Chambers of Commerce already act as sources of trusted support for business, and the Chamber network could be utilised as an intermediary body to improve the uptake of cyber security precautions. For example, the Chamber network offers the National Cyber Security Centre (NCSC) accreditation scheme at a discounted rate to over 50,000 member businesses. The potential reach and impact of this B2B network support in improving cyber resilience is a valuable resource to draw on, as the Cyber Security Breaches Survey 2023 shows that around two thirds (66%) of businesses with Cyber Essentials have a formal cyber incident response plan, compared to just 18% who do not.^{lxv}

Improving demand for cyber security products could also drive a virtuous cycle of supply and demand improvements in the cyber insurance market; businesses who are more aware of the cyber threat will be more likely to purchase insurance, and insurance incentivises behaviour change such as installation of protective software.

The responsibility of business

Where businesses are the victims of cyber crime, their customers and contacts can also suffer. Businesses want to work with the government to have clarity and certainty about what their responsibilities are to customers before, during and after a cyber attack.

The Department for Culture, Media and Sport (DCMS) 2022 cyber security incentives and regulation review concluded that “the government is considering ways in which we can mandate large companies to appropriately assess and address the cyber risks they face”.^{lxvi}

At present, the private market is incentivising better cyber security practices through supply chain contract requirements to have accreditations such as Cyber Essentials. Any official government measures taken, such as placing a requirement on businesses to install cyber protections, must be achievable and affordable, recognising that the business is also the victim in the event of a cyber crime.

RECOMMENDATIONS

- The government should work with the insurance industry to create a reinsurance pool that underwrites cyber risk and promotes effective cyber security practices for all UK businesses.
- The government should increase business awareness of and access to cyber security training. This will provide them with digital confidence to tackle security concerns and prevent imbalances in how resilient firms of all sizes are to the threat of cyber crime.
- Government guidelines should represent a clear standard for businesses to aspire to rather than a burden on small and resource-strained companies.



SECTION 3

ARTIFICIAL INTELLIGENCE

Introduction: Definitions and use-cases

Artificial Intelligence (AI) is an umbrella term that includes natural language processing, machine learning, deep learning, machine vision, robotics, and other logic-based reasoning algorithms.^{lxvii} Some AI technologies have the potential to reproduce or surpass abilities (in computational systems) that would require intelligence if humans were to perform them. These include learning and adaptation; sensory understanding and interaction; reasoning and planning; search and optimisation; autonomy and creativity.^{lxviii}

Much of the public debate and media coverage of AI tends to focus on the potential risks of “frontier” AI models, which are defined by the UK government as “highly capable general-purpose AI models that can perform a wide variety of tasks and match or exceed the capabilities present in today’s most advanced models”.^{lxix} The risks include “hallucinations” (plausible but incorrect answers); reduced reliability when carrying longer-term tasks; biases; and lack of detailed context.^{lxx} In addition, there is increasing discussion around generative AI, a specialised form of AI, which is defined as being able to “interpret and generate high-quality outputs including text and images.”^{lxxi} This report explores ways in which businesses are adopting AI and how businesses can use this technology to boost productivity in a safe and secure way.

In our conversations with businesses and experts, we have found many examples of AI improving efficiency and productivity, helping to gain a competitive advantage. In the computer science field, for example, AI provides a productivity boost by helping find solutions to coding problems. Other examples highlighted by businesses include a small marketing firm using AI to help analyse and categorise large volumes of text, as well as a small hospitality firm using AI to help write letters and social media posts. However, there is still a requirement for a knowledgeable user to interpret and implement the results. There are many other economically useful tasks that AI systems can do (with varying degrees of success), including translating between multiple languages, conversing fluently, and summarising lengthy documents.^{lxxii} A more general overview of use-cases of AI is shown on the next page.

Looking ahead, Bloomberg Intelligence forecast that the growth of AI will be driven first by training infrastructure, then shifting to inference devices for large language models, digital advertisements, specialised software, services, and the integration of AI technology into applications used by businesses.^{lxxiii} Bloomberg estimates that the generative AI market is likely to grow to \$1.3 trillion globally over the next 10 years, from a market size of \$40 billion in 2022.



USE-CASES OF AI

The Future of Privacy Forum, who works to encourage greater public understanding of AI, has produced sectoral use-cases to illustrate how AI is likely to be adopted in the future. These include:

Finance

Tax Compliance programmes that allow you to fill out tax forms and ensure information is included and provided in a way that is within current legal requirements of the tax code.

Healthcare

Ambient Charting, where conversations between doctors and patients are recorded and added to the patient record as they happen, with key words and follow-ups noted as appropriate.

Tracking

As used in Workplace Monitoring to provide both physical and digital accountability, while enforcing security policies.

Mobility and Transportation

Intelligent Navigation provides route scheduling and real-time guidance through traffic, supporting cost reduction and considering many variables such as weather, prediction of congestions, etc.

Social Media

Platforms use AI to face the challenges around appropriate and effective Speech or Content Moderation.

Forecasting

Supply Chain Management has reached new levels of efficiency and accuracy with AI-based modelling and predictions.

Source: Future of Privacy Forum, <https://fpf.org/blog/the-spectrum-of-artificial-intelligence-an-infographic-tool>

BCC Insights: Business uptake and use of AI

In August 2023, the BCC undertook a survey of more than 700 firms, mostly SMEs, to understand the take-up of AI, and the reasons why firms were or were not using the technology.^{lxxiv} The research also highlights the perceptions, barriers, and opportunities that this technology provides.

Business uptake

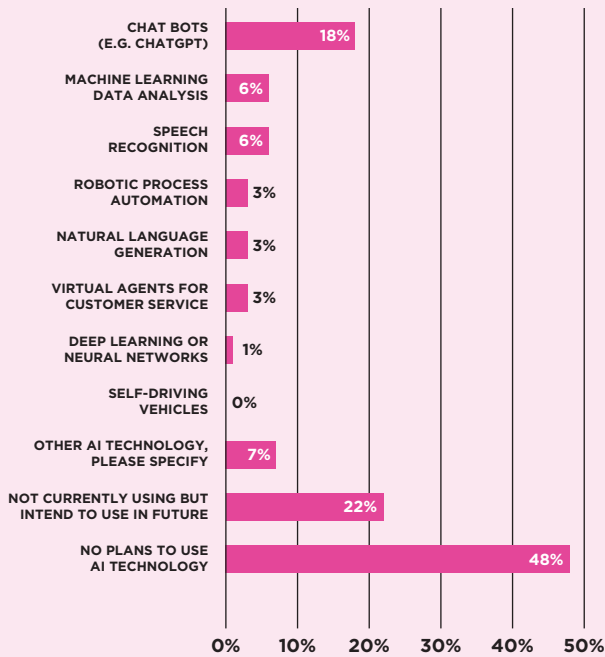
The research found very low levels of intended usage of AI technologies, indicating that firms may be missing opportunities to innovate:

- Almost half of all respondents (48%) have no plans to use AI technology, with a further 22% not currently using AI but intending to use in future.
- Customer facing businesses (B2C), such as hospitality and retail firms, are less likely to use AI, with 58% stating they have no plans to use it.
- Business facing businesses (B2B) such as finance, legal, and marketing firms are slightly more likely to be using AI, with only 39% saying they have no plans to use it.
- One in four respondents (26%) think AI is going to lead to a net decrease in jobs in their sector, while 12% expect a net increase. The rest either expect no change or don't know at this stage.

Businesses were asked what types of AI they were currently using, with chatbots, such as ChatGPT, cited as the most popular application (by 18% of all respondents). Machine learning data analysis came in a distant second place (6%). Other technologies cited included speech recognition, and process automation (see Chart 1 on the next page). The data also showed that companies with more than 50 employees were more likely to be currently using AI than smaller firms, with 24% using chatbots, and only 37% stating they had no plans to use it at all.

Of the respondents currently using AI, common uses included coding, data analysis, language translation, content creation, and as a sounding board for ideas. By contrast, of the respondents who have no plans to use cited the following barriers: lack of relevance, investment cost, reliability, lack of understanding, and risks around scams or privacy. A selection of survey responses to illustrate these points are included in the Appendix.

CHART 1
IS YOUR ORGANISATION CURRENTLY USING ANY OF THE FOLLOWING AI TECHNOLOGIES?



Total: N = 715; Manufacturing: N = 236; B2B services: N = 302; B2C services: N = 140

Impact on jobs

There is an active debate around the extent to which AI will impact on the workplace, and which sectors and roles will be most impacted. There appears to be no clear consensus, yet, on the net effect of AI, and whether jobs lost through automation will be offset by new jobs created.^{ixv} Our research found that 36% of businesses thought it was still too early to predict the impact of AI on jobs. Interestingly, just one in eight firms (12%) thought it would lead to an overall net increase in jobs in their sector (see Chart 2 to the right).

The impact on employment and customer service were raised in the qualitative survey responses as a reason why AI was not being used. Examples included:

“We don’t need it and it will decrease people employed. Also customers require face to face conversation”

Small logistics firm in Staffordshire

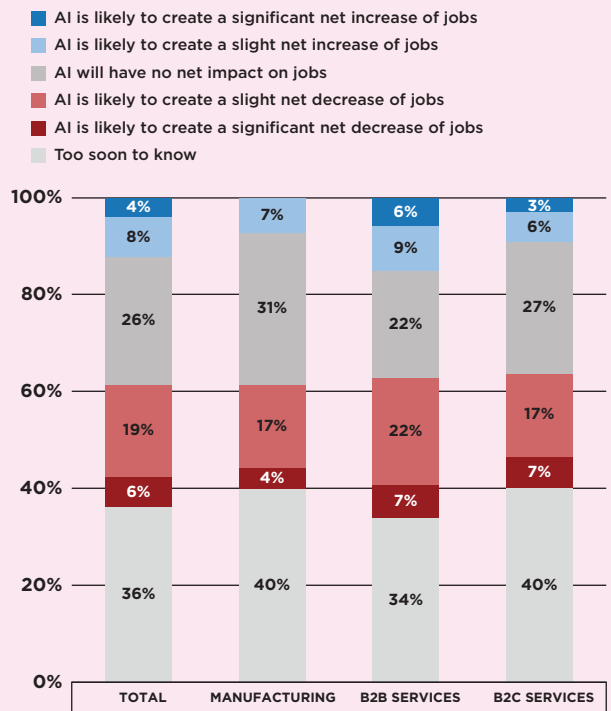
“Customers prefer the human touch and interaction”

Micro hospitality firm in Staffordshire

“Our business is in the creative sector. Replacing good, creative people with AI technology is the start of a dangerous slippery slope which could eventually see human creativity stifled to the point of extinction in the long term.”

Small marketing firm in Norfolk

CHART 2
OVER THE NEXT THREE YEARS, DO YOU EXPECT TO SEE A NET INCREASE OR DECREASE IN THE NUMBER OF JOBS CREATED BY AI TECHNOLOGY IN YOUR SECTOR?



BASE: (Total: N = 694; Manufacturing: N = 229; B2B services: N = 295; B2C services: N = 134)

Business Views and Use of AI: Input from our expert group

We have complemented our research work with discussion with industry and stakeholders in the AI sector, convened as our Digital Revolution Challenge group. They have identified further ways in which businesses in different sectors are approaching AI.

Formal and Informal Use:

- There is not always a single business view on AI; sometimes it is adopted as a leadership decision, but in other cases employees may be using AI without leadership buy-in, or perhaps with managers not even being aware.

Negative perceptions:

- Some larger businesses are operating in-house generated AI rather than external systems, as they consider this necessary to fully safeguard to protect their security.
- There was some scepticism in a large media organisation as to whether AI could ever have a significant impact on their organisation due to concerns over accuracy.
- ChatGPT is seen by some businesses as likely to be less useful over time, as organisations remove information from the stream available to the system.

GDPR can offer learning points for AI adoption

- GDPR changes were driven by regulations rather than innovation, the need to scrutinise processes and ensure security was similar in concept to onboarding a new AI based work system.
- It will be interesting to see if, in the future, those businesses who have taken a thorough, in-depth approach to being GDPR compliant are also those who become the most confident users of AI.

Types of AI business user

Based on the research summarised above, we have developed four broad categories of business user, to simplify understanding of how businesses use and interact with AI:

1. Cautious

Many firms, particularly small businesses, are wary of AI and choose not to engage with it, for reasons including perceived security risks, and the potential for scams. These businesses are not taking full advantage of the opportunities for productivity gain that AI can provide.

2. Too Trusting

Some staff who are comfortable using digital and social media may be too trusting in the veracity and accuracy of some AI applications. They may be unaware, or too dismissive of, some of the genuine concerns around AI, such as applications that are known to provide inaccurate or misleading results.

3. Unaware

Some businesses are unaware that they are using AI because software producers are increasingly incorporating AI into their products. This can create unforeseen risks, such as inadvertently using systems that have not been externally validated and produce inaccurate results. This trend is set to continue, with Bloomberg Intelligence viewing this area of embedded AI as a crucial part of this sector's growth.

4. Effective Implementers

Those that are comfortable in using AI technology and have assessed the utility and risks and limitations. Organisations within different sectors will have different approaches to effective implementation.

Using our categories of AI uptake

The four user types can be used to frame interventions to help businesses meet these goals. For example, the “Too Trusting” group may need guidelines on ethical and accurate use of AI systems. The “Cautious” and “Unaware” groups may need help on reporting, transparency process and verifying accuracy.

All groups need to be able to access training to ensure staff have the skills they need to use AI in the most appropriate way. Given the rapid development of technology in this space, these categories are fluid and businesses that are unaware may upskill relatively quickly, or businesses that are effective implementors may fall behind as the technology evolves.

Helping businesses become “Effective Implementers” of AI

A key objective for both the private sector and the government should be for businesses to become “Effective Implementers”. Businesses should be able to identify use-cases that will provide business benefits, e.g. productivity gains; gain the skills required to use the right AI application for their business need and to be aware of and overcome risks that stand in the way of confident usage.



AI Regulation: Creating a Framework for Trust

There is an active debate over whether regulation is necessary in the AI space. In general, effective regulation is beneficial to the development of innovative sectors, provided it is based on facts and is designed to foster, not stifle, innovation. The creation of a level playing field, clear rules, and fair competition, overseen by a robust and impartial regulator, are often vital to the development of competitive economies.

The EU recently concluded political negotiations on an AI Act in December 2023. This includes safeguards on general purpose artificial intelligence; bans on social scoring and AI used to manipulate or exploit user vulnerabilities; a new right for consumers to launch complaints and receive meaningful explanations; with potential fines ranging from 35 million euro or 7% of global turnover to 7.5 million or 1.5% of turnover.^{lxxvi}

In the USA, President Biden's administration issued an Executive Order on AI in October 2023^{lxxvii} which set out a variety of measures on AI including safety and security, consumer protection, supporting workers and promoting innovation and competition (including helping small businesses commercialize AI breakthroughs). A key theme of the White House approach is to develop standards, tools, and tests to help ensure that AI systems are safe, secure, and trustworthy.^{lxxviii}

In Canada, the government aims for a "responsible AI framework" via a new AI and Data Act (AIDA), which would require high-impact AI systems to meet safety and human rights expectations; to create a new AI and Data Commissioner to enable policy and enforcement to move together as the technology evolves, and to prohibit reckless and malicious uses of AI. Similar to the USA, AIDA follows on from a voluntary code of conduct approach and, provided it is agreed by legislators, could come into force in 2025.^{lxxix}

The UK is taking a different approach. Rather than introducing specific AI regulation, it is requiring regulators to publish plans on how they are responding to AI risks and opportunities and providing them with funding to expand their AI capabilities. The government has also committed to consulting on its cross-economy AI risk register and will assess and consult on its future regulatory framework.^{lxxx}

Other initiatives include the AI Opportunity Forum, to encourage adoption of AI across the private sector^{lxxxi}; and the AI Safety Institute which is focused on advanced AI safety for the public interest.^{lxxxii} Our view is that the UK approach is, broadly, the most appropriate way forward for regulation in the UK sector. It is right to work with, and expand the capabilities of, existing regulators rather than introducing bespoke AI regulation currently, but recommend additional steps the government should take to help create a comprehensive framework of trust (see below).

RECOMMENDATIONS

- The government should create a Small and Medium-sized Business AI Programme to inform business owners about practical ways AI can enhance their operations, and also appoint a business AI Champion.
- The government should support the development of long-term AI, data science and digital skills by providing specific funding for AI apprenticeships (including both young people and to support lifelong learning), and to make these available to at-risk industries such as the creative sector.
- The government should champion UK business AI adopters abroad through the GREAT Campaign and set up a specific programme to support UK businesses to export AI products to international markets.



APPENDIX

QUALITATIVE DATA: WHY ARE FIRMS USING, OR NOT USING, ARTIFICIAL INTELLIGENCE?

WHY FIRMS ARE USING AI

“As a small business we use AI as a personal assistant and as a sounding board. It helps us to improve communication with customers and create marketing materials”
Small retailer in Yorkshire.

“Writing letters and social media posts”
Small hospitality firm in Cheshire.

“Generating reports and marketing materials”
Medium sized education provider in Norfolk.

“Chatbots for Internal support services and customer facing websites”
Medium sized manufacturer in Lincolnshire.

“Support with research and content creation”
Consultancy in Dorset.

“Drafting blogs and data analysis”
Consultancy in the East Midlands.

“Intelligent resource for building commercial documentation and reports together with policies and helping to cut through difficult commercial problems that would ordinarily all require immediate specialist advice at a significant cost where no internal or existing knowledge was available”
Mid-sized retailer in Staffordshire.

“Analysis and categorisation of large volumes of text”
Small marketing firm in Cornwall.

WHY FIRMS ARE NOT USING AI

Relevance and Applicability

“No relevant applications to our production”
Micro manufacturer in Doncaster.

“No opportunities identified”
Small construction firm in Essex.

“Do not see opportunities at this time for a company of our size and type”
Small logistics firm in the Black Country.

Cost and Value Concerns

“Too expensive and will be obsolete too quickly”
Micro marketing firm in Wales.

“Business is too small to incur the implementation costs”
Small manufacturer in the North East.

“Too costly for a small business like mine”
Retail or wholesale sole trader in the East Midlands.

“Not sure I see the value in hospitality”
Medium sized hospitality firm in Wales.

Lack of Knowledge and Understanding

“Don’t know anything about it or whether any AI products are relevant to us”
Small accounting firm in Worcestershire.

“Don’t understand it”
Consultancy firm in Kent.

REFERENCES

- i. Gigabit broadband in the UK: Government targets, policy, and funding. Commons Library Research Briefing, 3 July 2023
- ii. Gigabit broadband in the UK: Government targets, policy, and funding. Commons Library Research Briefing, 3 July 2023
- iii. Project Gigabit progress update September 2023
- iv. Gigabit broadband in the UK: Government targets, policy, and funding. Commons Library Research Briefing, 3 July 2023
- v. <https://datareportal.com/reports/digital-2023-south-korea>
- vi. <https://www.sciencedirect.com/science/article/pii/S0308596123000174>
- vii. <https://cityfibre.com/news/project-gigabit-contract-award-unlocks-500-000-home-expansion-of-cityfibres-networks-in-norfolk-suffolk-and-hampshire>
- viii. <https://researchbriefings.files.parliament.uk/documents/CBP-8392/CBP-8392.pdf>
- ix. <https://www.national-broadband.co.uk/best-rural-broadband/project-gigabit-uncovered>
- x. <https://committees.parliament.uk/publications/8513/documents/86177/default/>
- xi. <https://www.gov.uk/government/consultations/improving-broadband-for-very-hard-to-reach-premises/outcome/improving-broadband-for-very-hard-to-reach-premises-government-response>
- xii. <https://www.gov.uk/government/consultations/improving-broadband-for-very-hard-to-reach>
- xiii. <https://www.citizensadvice.org.uk/about-us/about-us1/media/press-releases/one-million-lose-broadband-access-as-cost-of-living-crisis-bites/>
- xiv. <https://www.ispreview.co.uk/index.php/2020/06/report-reveals-the-barriers-to-uk-gigabit-broadband-adoption.html>
- xv. The UK workforce digital skills gap Why closing it matters and a roadmap for action, Futuredot.now
- xvi. Web searches for this report found pages of organisations across the UK offering device donation and reuse services, mainly local authorities and charities
- xvii. Building broadband and mobile infrastructure, Commons Library Research Briefing, 7 December 2022
- xviii. Digging Down to Level Up Report, Streetworks UK, November 2022
- xix. Government response to street and road works further reforms. DfT, May 2022
- xx. Building broadband and mobile infrastructure, Commons Library Research Briefing, 7 December 2022
- xxi. <https://www.gov.uk/government/publications/uk-geospatial-strategy-2030>
- xxii. <https://www.gov.uk/government/publications/uk-geospatial-strategy-2030>
- xxiii. A digital twin is defined by McKinsey as “a digital representation of a physical object, person, or process, contextualized in a digital version of its environment. Digital twins can help an organization simulate real situations and their outcomes, ultimately allowing it to make better decisions” <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-twin-technology>
- xxiv. <https://www.ibm.com/topics/what-is-a-digital-twin>
- xxv. <https://www.esri.com/about/newsroom/arcuser/south-korean-city-uses-a-digital-twin-to-meet-challenges/>
- xxvi. Building broadband and mobile infrastructure, Commons Library Research Briefing, 7 December 2022
- xxvii. Openreach monitoring report Ensuring an independent Openreach committed to fair competition
- xxviii. Openreach monitoring report Ensuring an independent Openreach committed to fair competition

- xxix. Securing long-term benefits for broadband customers Embedding infrastructure competition in the UK, INCA, 13 September 2013
- xxx. Gigabit broadband in the UK: Government targets, policy, and funding. Commons Library Research Briefing, 3 July 2023
- xxxi. Cambridge Econometrics (2021), Realising the Benefits of 5G, https://assets.publishing.service.gov.uk/media/6426a1f43d885d000cdadff3/realising_the_benefits_of_5G.pdf
- xxxii. APPG for Rural Business and the Rural Powerhouse (2022), Levelling up the rural economy, https://media.cla.org.uk/documents/Levelling_up_the_rural_economy_-_APPG_report_2022_ONLINE_pdf.pdf
- xxxiii. EU 5G Observatory (2023), Biannual Report, https://5gobservatory.eu/wp-content/uploads/2023/06/BR-18_draft_11.05.2023_CLEAN_Final-EC.pdf
- xxxiv. OpenSignal (2023), Benchmarking the Global 5G Experience, <https://www.opensignal.com/2023/06/30/benchmarking-the-global-5g-experience-june-2023>
- xxxv. Department for Science, Innovation and Technology (2023), UK Wireless Infrastructure Strategy, <https://www.gov.uk/government/publications/uk-wireless-infrastructure-strategy/uk-wireless-infrastructure-strategy>
- xxxvi. Ofcom (2023), Connected Nations, <https://www.ofcom.org.uk/research-and-data/multi-sector-research/infrastructure-research/connected-nations-2023>
- xxxvii. Vodafone (2021), Powering Up Manufacturing, Levelling Up Britain, <https://newscentre.vodafone.co.uk/app/uploads/2021/07/5G-Manufacturing-Report-210726-1.pdf>
- xxxviii. GSMA (2023), European 5G Performance Trails its International Peers, https://www.gsma.com/get-involved/gsma-membership/gsma_resources/european-5g-performance-trails-its-international-peers/
- xxxix. Financial Times (2023), UK mobile users had slowest 5G download speeds in G7 in 2023, <https://www.ft.com/content/2f202d15-d1ae-40bd-83f5-e0ad3a786c49>
- xl. Frontier Economics (2022), The Investment Gap to Full 5G Rollout, <https://www.connectivityuk.org/wp-content/uploads/2022/09/The-Investment-Gap-to-Full-5G-Rollout.pdf>
- xli. TechRepublic (2023), UK government invests £40 million in 5G, <https://www.techrepublic.com/article/uk-government-5g-investment/>
- xl.ii. 6G World (2024), South Korea to Invest USD 130 Million in 5G and 6G in 2024, <https://www.6gworld.com/exclusives/south-korea-to-invest-usd-130-million-in-5g-and-6g-in-2024>
- xl.iii. National Infrastructure Commission (2023), The Second National Infrastructure Assessment, <https://nic.org.uk/app/uploads/Final-NIA-2-Full-Document.pdf>
- xl.ii. National Infrastructure Commission (2023), Vodafone UK's Response to National Infrastructure Committee Call for Evidence, <https://nic.org.uk/app/uploads/Vodafone-NIC-response.pdf>
- xl.v. Rural Services Network (2023), UK Wireless Infrastructure Strategy, <https://rsnonline.org.uk/images/rural-lens/uk-wireless-infrastructure-strategy-rural-lens-review.pdf>
- xl.vi. Department for Digital, Culture, Media and Sport (2020), 5G Supply Chain Diversification Strategy, <https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy>
- xl.vii. Department for Science, Innovation and Technology (2023), Open RAN in high demand density environments: technical guidance , <https://www.gov.uk/government/publications/open-ran-in-high-demand-density-environments-technical-guidance>
- xl.viii. Department for Science, Innovation and Technology (2023), Open RAN principles: memorandum of understanding between government and industry, <https://www.gov.uk/government/publications/open-ran-principles-memorandum-of-understanding-between-government-and-industry>

- xlix. Department for Science, Innovation and Technology (2023), £88 million research and development boost for innovative connectivity to future proof UK mobile network, <https://www.gov.uk/government/news/88-million-research-and-development-boost-for-innovative-connectivity-to-future-proof-uk-mobile-network>
- I. FarrPoint (2024), FarrPoint Digital Connectivity Survey 2024, https://www.farrpoint.com/uploads/store/mediaupload/1274/file/Connectivity_Survey_Report_2024.pdf
- li. Analysys Mason (2021), Research on Very Hard to Reach Premises: technical and commercial analysis - report for the Broadband Stakeholder Group, https://www.connectivityuk.org/wp-content/uploads/2021/09/Analysys-Mason_Report-for-BSG_Research-on-VHtRPs_technical-and-commercial-analysis_12-August-2021nc_v2.pdf
- lii. Ericsson (2024), The 5G FWA Growth Opportunity, <https://www.ericsson.com/en/reports-and-papers/mobility-report/articles/realizing-the-5g-fwa-growth-opportunity>
- liii. Department for Science, Innovation and Technology (2023), Cyber security breaches survey 2023, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>
- liv. British Chambers of Commerce (2022), <https://www.britishchambers.org.uk/news/2022/01/bcc-finds-rising-cyber-attack-fears-in-hybrid-working-world/>
- lv. House of Commons Justice Committee (2022), Fraud and the Justice System, <https://committees.parliament.uk/publications/30328/documents/175363/default/>
- lvi. British Chambers of Commerce (2019), Infrastructure Survey
- lvii. Joint Committee on the National Security Strategy (2023), A hostage to fortune: ransomware and UK national security, <https://committees.parliament.uk/publications/42493/documents/211438/default/>
- lviii. Emmerson et al. (2024), Constraints and trade-offs for the next government, <https://ifs.org.uk/publications/constraints-and-trade-offs-next-government#:~:text=High%20levels%20of%20debt%20can,to%20adverse%20shocks%20in%20future.>
- lix. Department for Science, Innovation and Technology (2023), Cyber security breaches survey 2023, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>
- lx. Office for Budget Responsibility (2022), Fiscal risks and sustainability - July 2022, <https://obr.uk/frs/fiscal-risks-and-sustainability-july-2022/>
- lxi. HM Government (2023), National Risk Register 2023, https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf
- lxii. Joint Committee on the National Security Strategy (2023), A hostage to fortune: ransomware and UK national security, <https://committees.parliament.uk/publications/42493/documents/211438/default/>
- lxiii. Department for Business, Energy and Industrial Strategy (2023), Evaluation of the Trade Credit Reinsurance (TCR) scheme, <https://assets.publishing.service.gov.uk/media/64ad6f20fe36e0000d6fa6b7/evaluation-of-tcr-scheme-final-report.pdf>
- lxiv. Department for Digital, Culture, Media and Sport (2022), Live Events Reinsurance Scheme: Statistics (May 2022), <https://www.gov.uk/government/publications/live-events-reinsurance-scheme/live-events-reinsurance-scheme-statistics-may-2022>
- lxv. Department for Science, Innovation and Technology (2023), Cyber security breaches survey 2023, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>

- lxvi. Department for Digital, Culture, Media and Sport; Department for Science, Innovation and Technology (2022), 2022 cyber security incentives and regulation review, <https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-security-incentives-and-regulation-review#contents>
- lxvii. For an overview of the differences between types of AI and the role and applications in the business world see <https://www.turing.com/blog/artificial-intelligence-vs-machine-learning-vs-deep-learning/>
- lxviii. <https://www.ukri.org/what-we-do/our-main-funds-and-areas-of-support/browse-our-areas-of-investment-and-support/artificial-intelligence-technologies>
- lix. Capabilities and risks from frontier AI: A discussion paper on the need for further research into AI risk, DSIT, September 2023
- lxx. Capabilities and risks from frontier AI: A discussion paper on the need for further research into AI risk, DSIT, September 2023
- lxxi. Generative AI Framework for HMG, Cabinet Office, 18 January 2024
- lxxii. Capabilities and risks from frontier AI: A discussion paper on the need for further research into AI risk, DSIT, September 2023
- lxxiii. 2023 Generative AI Growth, Bloomberg Intelligence, June 2023. Quoted in Bloomberg press release Generative AI to Become a \$1.3 Trillion Market by 2032, Research Finds, June 01, 2023
- lxxiv. Businesses may be using AI indirectly through software which has it already built in, but this survey tested their own perception of direct use.
- lxxv. See for example Capabilities and risks from frontier AI, DSIT 2023, and The Potential Impact of Artificial Intelligence on UK Employment and the Demand for Skills, BEIS, 2021
- lxxvi. <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>
- lxxvii. <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>
- lxxviii. For a summary of the AI Executive Order see White House Factsheet: <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/>
- lxxix. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>
- lxxx. <https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response>
- lxxxi. <https://www.gov.uk/government/news/ai-opportunity-forum-holds-first-meeting>
- lxxxii. <https://www.gov.uk/government/publications/ai-safety-institute-overview/introducing-the-ai-safety-institute>

CONTRIBUTORS

We are pleased to thank the following stakeholders who contributed to our report:

Chair - Priya Guha MBE, Venture Partner at Merian Ventures and former UK Consul General to San Francisco

Dr Matthew Forshaw, The Alan Turing Institute and Newcastle University

De Montfort University

Intuit

Market Research Society

Pool Re

Wildanet

