IMPERIAL
Centre for Sectoral Economic Performance

University of BRISTOL

A UK Cyber Growth Action Plan

Recommendations for government and industry

An independent report from CSEP

Katie Cooper, Alex Greenwood, Chris Hankin, Lisa Kehoe, Ola Michalec, Martin Sadler, and **Simon Shiu** (Lead Author)

September 2025

Table of Contents

1. Introduction 4
2. A culture for cyber growth 9
3. Supply and demand 17
4. Places 23
5. Futures 28
6. Strategy alignment 33
7. Conclusion and next steps 38
8. Technical annex 40

This report is the output from an independent, rapid analysis to provide key insights on the interventions needed to further develop the UK's cyber security sector. Carried out by a team from the University of Bristol and Imperial College London, it builds on the Cyber security sectoral analysis 2025[1] and the UK Government's Modern Industrial Strategy[2]. It was produced in time to feed into the refresh of the National Cyber Strategy, and was laid in Parliament as a Command Paper on 19 September 2025.

The authors of this work were supported by and would like to thank the Centre for Sectoral Economic Performance at Imperial College London.

The authors are also very appreciative of the insights of the many individuals who have generously given their time to provide both challenge and support. Whether they took part in roundtables, were interviewed, or sent comments, the report refers to them all as participants.

The report focuses on growth of the UK cyber security sector, whilst paying attention to resiliency and value for money. The aim is to grow a thriving cyber security sector that enables the UK to be the safest country online, whilst recognising a persistent challenge: that those who make purchasing decisions often do not see why they should be investing in cyber security.

There are many audiences and stakeholders that take an interest in how cyber security is shaped, and the UK's cyber security community across government, the private sector and academia, is well connected, collaborative and innovative. This community is a real asset to help cyber security companies grow and attention has been paid throughout the report as to how we can build on this strength.

[1] DSIT (2025) Cyber security sectoral analysis
[2] DBT (2025) The UK's Modern Industrial Strategy

Executive Summary

This report, which is based on input from the supply and demand side of the UK cyber sector, is focused on the growth pillar of the refreshed national cyber strategy.

Cyber has been identified as a frontier technology in the Digital and Technologies sector plan of the Industrial Strategy and the UK cyber sector is growing, but so is the cyber threat. With all organisations depending more on digital infrastructures, cyber resilience is critical to enabling all sectors of the economy to grow. This wider economic growth, in turn, should help to fuel innovation and growth in the cyber sector. There is huge need and opportunity for the UK to find ways to reinforce this virtuous cycle of cyber growth and resilience.

The report highlights that to achieve this, the stakeholders in industry and government need to:

i. push this virtuous cycle of resilience and growth by stimulating informed demand and supporting businesses at all stages of their growth journeys in meeting that demand;

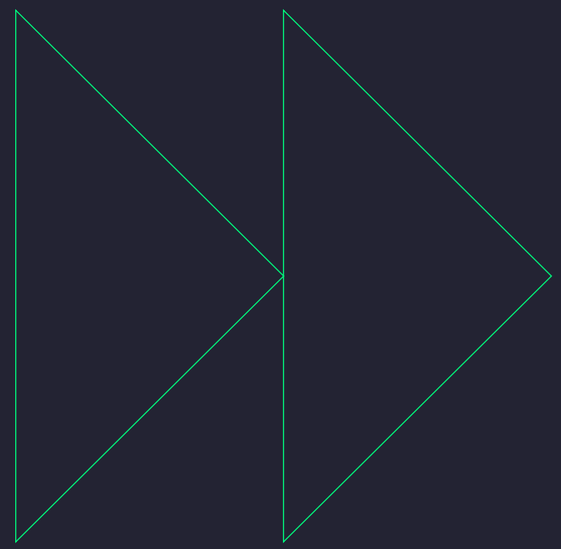
ii. make strategic choices about where to focus on technologies and sectors; and

iii. simplify and clarify the roles of government (including the National Cyber Security Centre (NCSC)) in relation to cyber resilience and growth.

The growth plan described here includes 9 recommendations and 24 associated suggestions which outline actions for all parts of the UK cyber ecosystem including government and industry. In summary they call for:

- Curating the UK's cyber culture to drive growth and public participation in cyber skills and innovation.
- Putting leadership in the right places with industry-led national and place-based cyber growth roles.
- Building on the UK's places of cyber strength to collaborate on sensitive topics, chosen technology areas and make time to create and anticipate cyber futures.

There are important roles in this growth plan for industry, government, academia, investors, and civil society. The good news is that throughout the consultation the authors found that all parts of the community were already capable, willing, and engaged on the challenges and opportunities for the UK. The plan emphasises the need for shared principles to act as one team and to both recognise and act upon the connections between cyber growth, resilience and value for money.



1. Introduction

The UK's cyber security sector continues to grow strongly, with jobs (up 11%), revenue (up 12%) and Gross Value Added (GVA) (up 21%) all increasing over the past year. The sector employed an estimated 67,300 in over 2100 companies in 2024, offering a range of products and services. There are also a large, but unquantified, number of individuals in cyber, risk, data and IT roles within organisations in every sector who perform cyber security tasks such as managing access controls, responding to incidents, and ensuring compliance with security and data protection policies. These individuals have different levels of knowledge and experience, ranging from a basic understanding to deep cyber expertise.

Organisations and individuals collect and use ever more data; our physical world is increasingly instrumented and controlled by digital systems; our systems are becoming more integrated and the technology stack more complex. The pace of these changes, not least in AI is astonishing, with much of this happening without adequate attention to cyber security. This makes keeping the UK safe both a challenge and an opportunity for cyber companies.

The challenge is considerable, with damaging cyber-attacks continuing to be in the news underlining that more needs to be done to ensure the country's economic security and resilience. From state actors to organised crime, to hacktivists and opportunists, motivations are varied. There is specialisation amongst, and marketplaces for, the various threat actors, creating an innovative economy of attack capability and services.

As organisations standardise their digital infrastructure to streamline operations, they build extensive networks of homogenous systems with shared configurations and vulnerabilities. Therefore, even without threat actors, our reliance on such systems creates opportunities for misconfigurations and poorly tested patches, meaning that a single "mistake" can lead to global consequences.

AI is already becoming a key part of the toolkit for both attackers and defenders, with implications that are still poorly understood[3]. There is the potential scale and sophistication of AI-driven attacks, the question of where accountability will lie should we need to rely on autonomous AI systems in defence and the possibilities of all kinds of collateral damage.

For a growing cyber security company, even with a clear market opportunity, there is a lot to navigate. In addition to the challenges common to other frontier technologies, such as raising capital, there are cyber sector-specific challenges that can slow down progress.

Early-stage product companies often face difficulties deploying solutions in representative environments to test whether proposed solutions scale effectively. Securing 'lighthouse' customers – especially government departments – can be critical for many companies but difficult to achieve. Many face strategic trade-offs, perhaps having to choose between developing sovereign solutions for national security customers or focusing on the export market. On top of this, companies must learn how to talk with business leaders about risk and the role of cyber security in fostering consumer trust, protecting reputation and supporting the reliable operation of IT systems. Many business leaders may see cyber security as a net cost rather than an opportunity and struggle to understand how a technology or service could enhance the resilience of their organisation.

There is a lot to celebrate nationally, with growing attention and momentum behind efforts to develop the skills and places from which innovative new companies can emerge. The ecosystem is rich with activity. It includes the CyberFirst programme and vibrant local cyber communities coordinated through the UK Cyber Cluster Collaboration (UKC3). The UK Cyber Security Council is leading efforts to professionalise the sector, while CyberUK plays a role in convening stakeholders across the landscape. Meanwhile, the NCSC's Research Institutes and Academic Centres of Excellence are strengthening the evidence base and training the next generation of inventors, scientists and engineers. Across the country, there is a generous, energetic, and nurturing cyber community helping individuals and companies to grow.

Yet there is more that can be done.

This report sets out a targeted action plan, developed from the insights of diverse experts in the cyber community. It is grounded in interviews and roundtables with 93 participants conducted between May and July 2025. It is based on perspectives from startup founders, security technologists, security service providers, security product vendors, Chief Information Security Officers (CISOs) from multiple sectors, large technology vendors, cyber research scientists and engineers, public interest technologists, trade, accreditation and membership associations, investors, regional leaders, and various parts of government.

Section 2 of the report looks at how cyber security companies can be better supported in their growth journeys and what additional roles the NCSC and the Department for Science, Innovation and Technology (DSIT) might play. It also considers the part played by the underlying culture of cyber and the language we use.

There are still many organisations that are not paying attention to the fundamentals or following the Government's baseline standard, Cyber Essentials. Section 3 looks at the interplay between supply and demand, and in particular the role that regulation plays in stimulating demand.

Companies grow faster when they are surrounded by others from whom they can learn. Section 4 looks at the role of places and leadership in growing the UK's cyber innovation ecosystems.

Much of the attention within government and the cyber security sector is focused on today's challenges. We also need to prepare for tomorrow. Section 5 looks at where opportunities for growth lie, focusing on AI, cyber physical systems and tools that lower the burden for organisations to have a fundamental level of security and resilience.

Policy is a lever that can help to stimulate growth, Section 6 looks at possible strategy alignment across the many policy documents that refer to cyber security.

Recommendations are brought together in Section 7, Conclusions. A technical annex outlines the methodology used in collecting evidence and suggest how growth might be measured

[3] There is emerging evidence on the rapid adoption of AI for cyber crime, e.g. Deloitte describes AI-enabled financial fraud as the biggest threat to the industry, potentially enabling fraud losses to reach $4bn in 2019, $12.3bn in 2023, projected to $40bn in 2027 (US data). Likewise, the cyber security industry itself witnesses adoption of AI with 30% of surveyed workers integrating AI tools in their workflows according to ISC2 (an international member association for cybersecurity professionals) Sources: ICS2, 2025, Survey of AI Adoption; Burton et al., 2025, AI and Serious Online Crime

1.1. Recommendations

This report makes nine recommendations organised around three pillars: culture, leadership, and places. Assessing growth can be complicated. Revenue, GVA, jobs and investment are all indicators, but they don't always move in synch. Some of the recommendations focus on growth of the cyber sector, while others aim to help with the growth of the wider economy through the emphasis on incident prevention, resilience, and creating cyber confidence. Each recommendation may have different initial impacts on job creation and productivity.

Throughout the report are suggestions for the implementation of the recommendations and areas for further research. While not exhaustive, they represent insights and options for next steps. Given the rapid nature of this review it is expected that further work will be needed to create more granular recommendations such as to target product or services growth, or how to proceed with specific places.

Each recommendation sets a direction for creating growth in the UK cyber sector. While each can be pursued individually, they are designed to be implemented in combination to maximise impact and drive systemic change.

A culture for growth

Growing cyber businesses depends on the interaction between the vendors and the CISOs and managers who procure products and services. This relationship between supply and demand is shaped by the UK cyber culture and mindset. To strengthen this, we can focus on supporting the growth journeys of cyber businesses, setting clearer expectations for how cyber risk should be managed and reported to increase informed demand, and engaging civil society on the role cyber growth plays in the UK's safety and prosperity.

Recommendation 1 – Support growth journeys

Government and industry stakeholders should review the incentives and validation routes available to cyber businesses.

The goal is to make it easier for cyber businesses to navigate the complexity of meeting cyber demand and to shift the culture to one that selects and helps winners to grow.

Recommendation 2 – Stimulate informed demand

Government should use guidance and regulations to stimulate growth by setting expectations for high quality reporting of cyber risks, consulting on mandating the use of Cyber Essentials, and encouraging usage of cyber insurance and principles-based assurance.

The goal is to encourage organisations across sectors to prioritise cyber security in alignment with their organisational risks, thereby reducing incidents, increasing resilience, supporting broader economic growth, and driving demand for more UK cyber services.

Recommendation 3 – Foster public participation in cyber skills and growth

UK cyber professionals should engage with UK civil society on the sector's role in national resilience and prosperity. This means emphasising the role cyber teams play in 'keeping the lights on' and the importance of skills initiatives from schools to professional development for cyber founders and leaders.

The goal is to build broader UK support for the role of cyber, making it easier for businesses to prioritise cyber, for people to learn cyber skills, and for the industry to attract, grow and maintain talent.

The need for leadership

The UK cyber community has many leaders but not many are focused on connecting supply and demand for sector growth. We recommend creating and elevating cyber leadership roles in government and places where there is research and development activity and commercial strength to drive and support growth outcomes.

Recommendation 4 – Appoint a UK cyber growth leader

Government should appoint a leader to provide expertise and drive coordinated action across the cyber security industry and within Whitehall. This role would encompass some of the previous Cyber Ambassador's responsibilities in advancing export growth and supporting national security objectives. It would also include responsibility for driving this growth plan forward.

The goal is to ensure cyber growth is prioritised and integrated across several policy areas.

Recommendation 5 – Appoint growth leaders in places of cyber strength

Appoint place-based leaders to be responsible for convening and driving cyber growth initiatives and outcomes. These leaders should have industry experience, support the UK cyber growth leader and be independent from central and regional government.

The goal is to ensure places use their strengths to grow, create, and attract more cyber businesses.

Recommendation 6 – Expand the NCSC role

The Government should expand and appropriately resource the NCSC to help drive cyber growth. The NCSC is a 'crown jewel' for cyber resilience, which is their primary mission. They also have the capability to guide and steer for growth outcomes. Given the importance of resilience, growth should be added without diverting attention from their existing priorities.

The goal is to use the deep expertise of NCSC in support of cyber growth, guiding and validating cyber businesses, research, futures, and technologies.

The role of places

Places play a vital role in innovation and growth – attracting investors, shaping Research and Development (R&D), and building the relationships needed for cyber businesses to start and grow.

Recommendation 7 – Develop futures-oriented communities

Place-based leaders should use their convening role to look forward and shape future markets. To do this, they should bring together CISOs, academia, small and large industry, government, and other stakeholders to share perspectives on, and pursue solutions to emerging cyber challenges.

The goal is to drive initiation, co-creation and delivery of innovative projects into the market, and to build a culture of anticipation.

Recommendation 8 – Places to nurture distinct tech areas

Places should be strategic in prioritising technologies and application areas based on their cyber strengths and sector connections in alignment with the Industrial Strategy and the UK Government Resilience Action Plan. Cyber innovation in AI, cyber-physical systems, and tooling for fundamentals should be considered as initial priority areas.

The goal is for the UK to have place-based cyber strengths that are more than the sum of their parts, each contributing to UK cyber growth.

Recommendation 9 – Places to provide safe environments

Create safe havens with infrastructure and data for multiple groups of stakeholders (not just those with security clearances) to explore, 'role-play', co-create and share how to assemble and test solutions to current and emerging challenges.

The goal is to build broader cyber resilience capability, which will both serve in moments of crisis and be a pool of talent for cyber growth.

Underpinning principles

To realise the opportunity for cyber growth, these recommendations should be underpinned by a set of principles that should be held in mind by all stakeholders.

Underpinning principle 1 – The UK cyber sector should act as one team

Many stakeholder groups have overlapping but distinct interests, and there are plenty of examples where they have built trust and supported each other. Collecting from the above recommendations, the community should start to operate as a single team growing cyber in the UK. This starts with celebrating, building on and catalysing the social capital in the UK cyber community.

Underpinning principle 2 – Growth + resilience + value for money

The broader benefits of cyber resilience and growth should be recognised as part of 'value for money'. Too often, purchasing and investment decisions are driven by a cost-based view of 'value', missing, the wider importance of UK cyber innovation for future resilience, sovereignty, and growth.

2. A culture for cyber growth

The UK cyber sector is a strong and willing community. However, it needs to broaden and expand if the UK is to achieve cyber resilience. This section examines the current UK cyber culture in three parts.

The first subsection considers the environment businesses currently need to navigate to grow. It reports on participants' experiences with seed funding, accelerator programmes, venture capital and exports. Recognising the views of starts ups and mature businesses alike, it unpacks how to address the recommendation on 'supporting growth journeys'.

The second subsection looks at the programmes in place from schools and professional development through to the entrepreneurial skills needed to grow companies. It discusses the role of culture and language in cyber skills training and development, while bringing attention to recent successful initiatives like Cyber First (now Tech First), Board Toolkits and Exercise in a Box.

The third subsection discusses the role of communication and engagement of civil society beyond the circle of cyber experts. It discusses the wider challenges of conveying the value of cyber and building public trust in technologies and institutions. The subsection concludes with linking the importance of maintaining a healthy public dialogue on the roles of technology in society. It discusses public engagement as an enabler of skills development and growth for all businesses.

2.1. Supporting cyber growth journeys

Participants shared a range of perspectives on the strengths and challenges facing the UK's cyber innovation and scale-up landscape. Many acknowledged that cyber remains a national success story, highlighting security products and services as one of the UK's leading export sectors. This achievement is underpinned by the country's reputation for rule of law and high-value service provision. Relationships and brand association, especially the NCSC and the role of the Cyber Security Ambassador, were seen as some of the most valuable enablers of commercial success. However, participants expressed disappointment about the lack of renewal of the Cyber Security Ambassador role.

The UK has technical talent in universities, government agencies and industry. Across critical national infrastructure, financial services, and other sectors there are people and networks with significant experience and knowledge maintaining cyber resilience. Some cyber businesses do start and scale, but most participants felt that the UK could do better, and that culture is essential to this ambition.

Matching other views on the UK startup culture[4], many participants highlighted that there are too many startups taking too long to fail or pivot. The public R&D funding was described as too small, fragmented, overly focused on early-stage R&D and limited in supporting commercialisation. Being incentivised to go for grants can 'leave startups in campaign mode' and prevent them from focusing on priorities such as validating markets or growing sales. Some participants described how this incentive can move businesses away from product innovation towards providing specialised services, which has consequences for the kind of growth (scale, GVA or jobs) they create.

Other participants, particularly those with experience of investment and risk capital, pointed out that the UK has a way to go to match the ambitions, involvement of CISOs, and the risk appetite of other parts of the world. This starts with encouraging and supporting potential cyber founders. Participants talked of still seeing the cliché of technology solutions looking for funding without the entrepreneurial mindset to focus on customers. Programmes like Cyber Runway and Cyber ASAP have been good for training cohorts in addressing this but, given the challenges, more support is needed[5].

Growing cyber businesses does have specific challenges. Several CISOs shared that budget constraints limit their ability to invest in innovative products. In a risk-averse climate, most security buyers will rely on sector incumbents and well recognised brands. CISOs are dealing with complex people, process, and technology problems. They have seen many cyber solutions dressed as silver bullets, which are usually not as novel as the vendor claims and underestimate the deployment or integration effort. It takes time and deep understanding of buyers' problems for founders to gain credibility with their solution.

Although there are venture capitalists and angel investors with cyber expertise and a growing cohort of successful founders, some participants highlighted issues with accessing investors who are aware and interested in cyber security. This could reflect that the culture of hype in the startup ecosystem still needs to be navigated. This is echoed in the industry literature, which points out a gap in venture capital investment between 'trendy' areas like Generative AI and more operational ones, like cyber security.[6]

Previous research that explored commercialisation of cyber in Academic Centres of Excellence in Cyber Security Research universities, highlighted the need for strong personal and community bonds and that only those academics who seek to come through some institutional barriers are likely to succeed. This exemplifies the need for universities and R&D centres to build teams of domain-specific commercialisation practitioners who can work together to attract venture capital and position products[7].

Participants, including successful cyber founders, highlighted that more could be done to connect startups with CISOs. The idea is expanded in the blog on 'The UK fly wheel: time to win'[8]. Having 'UK flag carrying brands' supporting startups can help businesses grow and gain credibility and participants pointed to financial services and the large mid-market as areas of strength.

Many highlighted that the UK Government has huge demand for cyber security, enough to sustain many startups, but that government can be difficult to work with. There have been many attempts to fix this, but the problems run deep with cyber being treated as 'one more item on the procurement checklist'. Participants highlighted the potential for DSIT and the NCSC to work together with government departments and procurement leads to stimulate the UK cyber market.

Many pointed out the capability in the NCSC both for spinning out technologists and IP, and for working with Small and Medium Size Enterprises (SMEs). The NCSC for Startups[9] was a selective programme that gave great networking and visibility opportunities for over 70 UK cyber startups. This example of picking and helping 'winners' was clearly beneficial, but has so far stopped short of government procurement leads.

The NCSC does publish a research problem book[10] where they describe what they see as the most significant problems that should be the focus of R&D. Some participants suggested using the NCSC more in pre-commercial problem co-creation, modelled on programmes such as His Majesty's Government Communications Centre (HMGCC) co-creation model[11] and with funding as investment from the British Business Bank much like the National Security Strategic Investment Fund (NSSIF)[12].

From the NSSIF website: 'NSSIF invests commercially, alongside other investors, in innovative startups, whose advanced dual-use technologies have potential applications both in the private sector and in the National Security and Defence community. This is done through direct investments where there is a strong strategic case, and investment into aligned venture capital funds.'

Participants liked this combination of government investment and convening, and they expressed enthusiasm for the idea of CISOs or other leaders with budgets from large organisations bringing cyber problems to similar programmes not restricted to national security. These kinds of convening models have been attempted before, but it remains a challenge to bring in the demand side in ways that lead to opportunities to validate problems and solutions.

Case study: The Jericho Forum

The Jericho Forum was a group of largely UK based CISOs that formed in 2002 to highlight that securing business and working practices by enforcing network boundaries was becoming increasingly difficult and less effective. They successfully argued for a 'de-perimeterised security model' to secure data and systems regardless of network location. This laid the groundwork for 'Zero Trust' architecture, which assumes no implicit trust based on network location and instead focuses on verification of assets and users[13,14].

The Jericho Forum is an example of anticipatory demand-led thinking and acting as 'one team'. It brought together UK customers and security leaders to collaborate, validate, and advocate for new approaches – demonstrating how user-led communities can shape global standards. It is a reminder that to compete globally the UK security community needs the strong input of UK customers to collaborate, validate and promote UK solutions.

[4] Federation of Small Businesses (2024) UK entrepreneurs should learn how to 'fail well' like their US counterparts, says Karen Mills, former Barack Obama Cabinet member
[5] DSIT (2023) Evaluation of the Cyber Runway programme
[6] World Economic Forum (2024) This is venture capital's key role in driving global cyber resilience
[7] Dwyer (2015) Academic Cyber Security Research: Best Practice for Commercialisation

[8] Paterson (2025) The UK Fly Wheel: Time to Win
[9] NCSC(2024) NCSC For Startups: Everything you need to know
[10] NCSC (2024) The NCSC research problem book
[11] His Majesty's Government Communications Centre - HMGCC (2025) Co-Creation
[12] British Business Bank (2025) National Security Strategic Investment Fund
[13] Spencer and Pizio (2023) The de-perimeterisation of information security: The Jericho Forum, zero trust, and narrativity
[14] Microsoft (2020) Back to the future: What the Jericho Forum taught us about modern security | Microsoft Security Blog

Participants highlighted that for deeper impact on cyber security innovation, there is benefit in regular 'upstream' meetings, between potential future suppliers and those managing cyber teams and functions, taking place before any procurement is undertaken. Participants told us that it can be difficult for CISOs that don't hold innovation budgets to prioritise time and investment in innovation. It was suggested that giving this group the opportunity to use funds to support innovation in their environment could be attractive.

While departments may struggle to find money for cyber growth and the HMGCC and NSSIF models offer some cyber opportunities, it was suggested that UKRI and the British Business Bank should identify funding to support pre-procurement work. This would help cyber businesses navigate government and commercial opportunities to address genuine demand-side needs without running out of cash on the way.

Growth challenges exist at all stages. Scaleups need help setting up processes and acquiring talent, medium sized businesses can get caught with the levels of bureaucracy of large businesses, many highlighted the value of the Department for Business and Trade (DBT) in supporting business development and exports. There are challenges with sovereignty and there is always the challenge of competing with or integrating into the wider cyber ecosystem[15]. This is an end-to-end problem with significant further attention warranted to create a larger funnel of 'picked winners'.

Recommendation 1 – Support growth journeys

Government and industry stakeholders should review the incentives and validation routes available to cyber businesses.

The goal is to make it easier for cyber businesses to navigate the complexity of meeting cyber demand and to shift the culture to one that selects and helps winners to grow.

The following suggestions[16] are aligned with Recommendation 1 to support growth journeys.

Suggestion 1 – Pilot programmes that allow NCSC and DSIT to qualify and connect cyber startups with government departments

NCSC and DSIT should be allowed to explore ambitious and experimental ways of reforming procurement, linking early-stage R&D opportunities to commercial tenders in more mature settings. This could be a joined-up government effort to use NCSC to qualify the technical credentials of cyber businesses, DSIT to connect them to departments, and to work with procurement and departments on the value for money and incentives to make this work.

Suggestion 2 – Expand the co-creation and government investment models for wider commercial participation

The NSSIF funding model and HMGCC co-creation model should serve as examples for convening and funding cyber ideas. Place-based leadership should seek to use this to incentivise startup and CISO involvement in pre-procurement workshops on problem co-creation with the NCSC.

[15] Supported by the DSIT (2025) Cyber Security Sectoral analysis. See. ' the data does highlight a range of international acquisitions of UK cyber security firms, particularly by US investors, which may raise important considerations for long-term market development. While such investment demonstrates the quality and attractiveness of the UK cyber sector, it demonstrates a clear need to support early-stage firms at the start of the growth pipeline and the delivery of infrastructure to help UK firms scale domestically and secure capital. This is particularly important given the strategic nature of cyber security capability and the need to maintain sovereign capacity in key technology areas.'

[16] The full mapping of recommendations and suggestions is shown in the table in the Technical Annex.

2.2. Developing the UK cyber workforce

Most participants highlighted skills as a major challenge. As one participant put it 'there is no point mandating higher standards of security if most organisations do not have the knowledge or capacity to meet them'.

2.2.1. Cyber in schools

Many participants highlighted that cyber skills education needs to start early, in schools. Cyber First[17,18] has been effective in enhancing cyber security awareness and providing learning experiences for students[19]. Building on its success the government has recently announced Tech First, expanding the scope of the programme to include digital skills more broadly[20]. Going forward, challenges for this programme include ensuring cyber is well integrated into emerging technology programmes (such as AI), on preserving the distinctive parts of the Cyber First programme, and building the capacity to deliver training more consistently. Tech First is a good step, but we also need to move beyond 'bolt-on' solutions to education if the UK is to keep pace with other countries that are building informatics programmes[21] or otherwise prioritising technical education[22].

Beyond technical skills, it is also important to engage young people in understanding what cyber is. This should align with and support initiatives to help children with online safety such as the refresh of the Online Safety Act and programmes like Digital Compass[23].

2.2.2. Entry points to cyber security jobs

Participants said that although many people would like to move into cyber roles, there are not many openings, especially for entry level roles. This is supported by data from the DSIT cyber skills 2025 survey[24]. On the one hand, the survey reports a 20% increase in cyber graduates in the most recent available data (2021/22 to 2022/23 academic years) and a finding that 49% of businesses have cyber skills gaps in a basic technical area in 2024. On the other, it shows core cyber job postings decreasing by 33% between 2023 and 2024.

This discrepancy between the skills gap and apparently decreasing demand for cyber could be explained in several ways. First, the ONS data shows a steady fall in vacancies across the UK since 2022[25]. Alternatively, it could also relate to whether the UK culture as represented by state, industry, and civil society, is sufficiently engaged in how cyber contributes to people's lives and how sectors prioritise cyber resilience as a core part of their operations. Regardless of the explanation for a decrease in cyber security job openings, the data highlights that if more organisations were to prioritise cyber resilience, there is a talent pool ready and willing to step into roles. This is consistent with the positive impact seen when Cyber Essentials was mandated in defence procurement, which has built capability and created jobs in small businesses[26].

2.2.3. Cyber security as a profession

The Cyber Security Council and numerous membership organisations continue to develop cyber security as a profession, with pathways, specialisms, and accredited qualifications. Maintaining a register of security professionals will become even more important, but also challenging to keep current as cyber grows in complexity, both with emerging technology and its relationship to business risk and resilience.

Many participants highlighted the critical and challenging role played by CISOs. Whether they sit in the IT department or on an organisation's board, the challenge is often how to ensure shared understanding and appropriate accountability for cyber risks. Participants said both that 'we need more business leaders with better understanding of cyber', and conversely 'we need more cyber leaders with better understanding of the operational risks for business', reflecting that in some cases not being able to talk about business risk means that cyber expertise is not 'in the room'.

Participants noted that the NCSC Board Toolkit[27] is a valuable resource for facilitating strategic discussions between boards and CISOs. However, they also highlighted that the role of the CISO varies significantly depending on the organisation's size and sector.

2.2.4. Equipping cyber entrepreneurs

From category creation and enterprise sales to building teams to validate, pivot and fail fast, starting businesses takes a lot of entrepreneurial drive and skill. Building cyber products requires knowledge of the priorities of customers and the threats they face.

Programmes like Cyber Runway[28] and CyberASAP[29] play an important role in broadening skills for would be founders. The valuable secondary effects of connecting people through programmes like Cyber Accelerators[30], LORCA[31] and CyLon[32] were highlighted positively by participants.

Participants said that the UK has strong technical talent with many innovative ideas for cyber. However, there are only a small number of UK founders and investors who have experience of scaling businesses, and where they do, that experience is typically gained in the US. Several participants pointed out the value of events that allow more focussed convening between founders and customers looking to innovate in cyber[33] but also with the few UK people experienced in cyber security product management.

2.2.5. Supporting cyber growth leaders

UK cyber culture impacts business and investment choices too. Although some sectors and organisations do it well, it can be difficult to discuss how cyber impacts organisational risk. The danger is that cyber is siloed into IT, rather than being linked with operational, legal and financial risks that carry executive level accountability.

Similarly, cyber founders steeped in technology can struggle to communicate commercial value to investors. This was primarily expressed as the need to develop customer validation and enterprise sales skills and framings but also that UK funding is more steeped in traditional business cases as opposed to a 'tech first' category creation mindset more prevalent in US.

There were mixed views on recommendations here as the UK can't simply adopt the culture and mindset of another country, but it was suggested that the UK needs to encourage more ambition and tolerance of failing fast and pivoting.

2.2.6. Shifting from a blame culture to a supportive culture

Participants reported that some cyber language can set the wrong tone. This included using phrases like 'doing the basics', which may downplay the complexity of maintaining best practices and fundamentals. There were also references to cyber having a 'blame culture' whereby employees and even victims face reprimand rather than support. This problem was related to the difficulties of sharing sensitive cyber information and was contrasted with safety industries (such as air travel) where sharing mistakes is culturally embedded and legally mandated.

2.3. Developing a UK cyber resilience mindset

2.3.1. Communicating the value of cyber for the UK's prosperity

The UK cyber sector is shaped by the people, culture and values of the wider UK population. Beyond technical skills, there is the need to foster inclusive, society-wide conversations about the role of the cyber sector in UK prosperity – in schools, organisations, and civil society.

Unlike healthcare, education and policing, the role of cyber professionals is much less visible and often poorly understood by the public. This highlights the need to bring civil society into the cyber security conversations[34], and to ensure that engagement leaves people informed and invested in the role the sector plays in national resilience and prosperity[35].

Participants highlighted that while cyber incidents are analysed and discussed in the cyber community, less effort goes into sharing with the wider public how incident teams across sectors and government have responded to contain and recover from these events. This misses an opportunity for cyber leaders to bring to life in schools and the media the positive and critical role being played by cyber professionals and so develop wider interest and understanding.

[17] NCSC (2025) CyberFirst overview
[18] DCMS and NCSC (2021) CyberFirst Evaluation
[19] CyberFirst Social Value Report 2025
[20] Primer Minister's Office (2025) PM launches national skills drive to unlock opportunities for young people in tech - GOV.UK
[21] Sampson et al (2025) Towards high-quality informatics K-12 education in Europe: key insights from the literature
[22] Education Policy Institute (2020) An international comparison of technical education funding systems: What can England learn from successful countries?
[23] The Behavioural Insights Team et al (n.d.) Digital Compass
[24] DSIT (2025) Cyber security skills in the UK labour market
[25] The Office for National Statistics (2025) Labour market overview, UK, July 2025
[26] IASME Consortium (2025) The benefits of Cyber Essentials certification
[27] NCSC (2025) Cyber Security Toolkit for Boards
[28] DSIT (2023) Evaluation of the Cyber Runway programme
[29] Innovate UK (2025) CyberASAP
[30] NCSC and Plexal (2025) NCSC For Startups
[31] Plexal (2025) LORCA: The London Office for Rapid Cyber Security Advancement
[32] CyLon Ventures (2025) Home
[33] Paterson (2025) The UK Fly Wheel: Time to Win
[34] World Economic Forum (2021) 'Leave No One Behind: How to Include Civil Society in the Cybersecurity Debate'
[35] Liveley (2022) Stories of Cyber Security

Recent research flags the risk of 'mystifying' cyber security. This pertains primarily to the buyers of cyber in organisations but also, to some extent, to members of the public. Romanticising and mystifying the expertise of cyber professionals and attackers contributes to the separation of cyber from other domains, for example making it less relatable to board members[36]. Marketing strategies (such as duplicating naming systems for adversaries and malware used by cyber security companies) are commonly playing to the tropes of deviance and edginess, inducing fear and helplessness. This can happen at the expense of coordinating information on cyber crime[37].

2.3.2. The importance of actively engaged civil society

There were diverse inputs amongst the participants on how privacy, harms and resilience should be balanced, reflecting the very different views of the state, industry sectors and various parts of civil society. AI is currently challenging the norms for copyright and privacy in the digital realm[38], and cyber-physical systems bring more of the digital to the physical world, creating the need to harmonise cyber and physical safety best practice[39]. As technology advances, stakeholders will continually have to re-frame and re-negotiate their perspectives in a digitally integrated society.

Participants asserted that involving civil society is a matter of both cyber growth and cyber resilience. Cyber security products should reflect the diverse needs of their users as a matter of ethical responsibility. There has been recent progress on inclusive security design, e.g. for the survivors of domestic abuse seeking protection from spyware[40] or for visually impaired individuals relying on voice-controlled devices[41]. On a larger scale, public trust in institutions is essential for successful mass adoption of digital technologies, especially in publicly funded programmes[42]. If users feel excluded, targeted or inadequately protected, adoption stalls risking that intended public benefits of technologies will fail to materialise[43].

Recent research suggests that cyber security should be framed as a quest, 'involving fundamentally optimistic, future-focused, and heroic plot centring around strong and collaborative leadership, individual and collective heroism, teamwork, and innovation (acknowledging that quests can also involve leadership contests, and internal rivalries)'[44]. It is important the people of the UK have an opportunity to express their needs in technology development, while gaining wider understanding of the contribution cyber makes to UK resilience. From business, state and civil society leaders to children and pensioners, the UK needs an informed and engaged community to give the sector skills and the mandate to navigate the changing risk landscape.

Case study: Cyber exercise in a box

Exercise in a Box[45] is a free, scenario-based tool developed by the NCSC to help organisations rehearse their response to common cyber threats in a safe environment.

Originally designed for small and medium-sized enterprises, local authorities, and public sector bodies, Exercise in a Box has been adopted to run tabletop exercises focused on threats such as ransomware, phishing, and videoconferencing attacks (e.g. 'zoom bombing'). Participants are guided through realistic scenarios and prompted to discuss their preparedness, response strategies and gaps in policy or practice.

The accessible format of Exercise in a Box is particularly valuable for organisations with limited in-house cyber expertise and resources. Looking ahead, Exercise in a Box could be extended to the wider public by adapting content for community organisations and schools, offering tailored scenarios around personal data breaches, social media use, or smart home security. Tailored versions could also be distributed through public libraries, or digital inclusion programmes to build everyday cyber resilience across society[46].

[36] Liveley (2022) Stories of Cyber Security Combined Report
[37] Collier, B. & Clayton, R. (2025)'Not just BANAL: How branding shapes cybercrime ecosystems'.
[38] Liebig et al (2024) Situating AI policy: Controversies covered and the normalisation of AI
[39] Michalec et al (2022) When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?
[40] Slupska and Tanczer (2021) Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things.
[41] NCSC (2023) Accessibility as a cyber security priority
[42] an example here is the rollout of contact tracing apps for COVID, with serious challenges to adoption experienced across the UK, Norway and France. Concerns about cyber security and public trust were frequently highlighted in these cases, see Altman et al (2020) Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study
[43] Renaud and Coles-Kemp (2022) Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge
[44] Liveley (2022) Stories of Cyber Security Combined Report
[45] NCSC (n.d.) Exercise in a Box

2.3.3. Language and mindsets

Many conversations highlighted how the cyber security sector is held back by misconceptions and stereotypes. Cyber often conjures up images of binary code flashing across screens in otherwise darkened rooms. Whereas cyber is actually a modern profession, requiring broad understanding of organisations, supply chains, people, technology and risks. Misunderstandings of the role of cyber in building strong and resilient businesses may put some people off the profession.

It has been suggested that we should start again with a complete rebrand. But the cyber community doesn't control the use of the term 'cyber', it is already embedded in public discourse. Rather than arguing for new terms, the cyber community should focus on shifting how cyber is understood, emphasising its relevance to enabling the UK's modern digital society.

The Cyber Security Sectoral Analysis 2025[48] identified that women make up just 17% of the cyber workforce. Participants connected this underrepresentation to misogynistic behaviour in workplaces and at large conferences, which often goes unchallenged. Others highlighted that the cyber industry often uses jargon laced with quasi-military language and glamourised names for adversaries, which creates fear, uncertainty, and doubt rather than the shared understanding and 'buy-in' needed for trusting relationships.

A tension here is that much of cyber is about contesting adversaries using offensive approaches. Training people to defend without ever trying to attack is a bit like learning to fight without an opponent. You can develop skills, but you are likely to be exposed when you face a real opponent. The UK needs to be comfortable developing offensive skills within regulatory frameworks defining legal and ethical uses of tactics like deception or breaking into systems. Ultimately, both offensive and defensive cyber security have a role to play in resilience and sectoral growth. As an example of the problem, one participant highlighted challenges businesses have selling 'cyber deception' even though it is considered an effective approach, since many customers are uncomfortable with the language.

Finding the balance is challenging, some participants highlighted the debates on the Computer Misuse Act (CMA)[49], which criminalises unauthorised use of computers. The Cyber Up campaign[50] highlighted the impact of uncertainty on crossing legal lines, meaning many are put off learning the skills needed, leaving the UK at a competitive disadvantage internationally.

For those dealing with cyber security issues regularly, the language is perhaps well suited to discussing the contested nature of digitalisation. It is important to be clear about organised criminals stealing and racketeering, about nations states (and pseudo state actors) spying and disrupting critical infrastructure, and how all this impacts economic prosperity and national security.

The participants were primarily members of the cyber community, which may be a biased sample. For the wider non-cyber community to have a say and stake in cyber growth and resilience, the sector needs language and framings that create an informed and unbiased debate.

Recommendation 3 – Foster public participation in cyber skills and growth

UK cyber professionals should engage with UK civil society on the sector's role in national resilience and prosperity. This means emphasising the role cyber teams play in 'keeping the lights on' and the importance of skills initiatives from schools to professional development for cyber founders and leaders.

The goal is to build broader UK support for the role of cyber, making it easier for businesses to prioritise cyber, people to learn cyber skills, and for the industry to attract more talent.

[46] Example of Scottish Business Resilience Centre applying 'exercise in a box' to upskill organisations – see Cyber and Fraud Centre Scotland (2022) SBRC to extend 'Exercise in a Box' programme for third year
[47] Another example is discussed in the RISCS blog on Panorama's Fighting Cyber Criminals, see Responding to BBC Panorama's 'Fighting Cyber Criminals' – Lucy Davies – Research Institute for Sociotechnical Cyber Security
[48] DSIT (2025) Cyber security sectoral analysis
[49] Home Office (2023) Review of the Computer Misuse Act 1990. Analysis of responses
[50] CyberUp Campaign (2025) Campaign responds to withdrawal of amendment to update Computer Misuse Act

The implementation of Recommendation 3 requires inclusive language and engagement approaches to enable consultation beyond the cyber sector. As outlined in 2.2 there is also a need to focus on pathways to cyber careers and embed cyber skills and expertise in organisations

Suggestion 3 – Include marginalised demographics in product development

Cyber technologists developing products and services to engage with marginalised demographics e.g. via representative organisations such as Age UK for elderly people. This will enable better understanding of user's product needs, whether as a business imperative or commitment to responsible innovation.

Suggestion 4 – Convene 'cyber in the public interest' events

DSIT, cyber businesses and civil society organisations to convene a forum on developing cyber technologies in the public interest[51]. These could be modelled on similar efforts by the Finnish authorities[52]. The goal here is to co-create technologies developed in the public interest and prevent wasted public spending caused by low adoption rates or delays in technology rollout.

Suggestion 5 – Use immersive methods to engage civil society

Leading third sector organisations and small business associations to adapt and use immersive methods (similar but not exclusive to the 'Exercise in a box') to engage civil society in the challenges and roles of cyber professionals.

Suggestion 6 – Focus on the way cyber language is used with the public

From marketing departments advertising cyber conferences, Human Resources leads recruiting for new roles to journalists reporting on emerging incidents, everyone has a role in shaping the language we use. The cyber community should adopt language reflecting the positive role cyber security plays in wider society. This could be achieved in conjunction with commissioning studies on the role of language in engaging diverse communities.

Suggestion 7 – Incentivise organisations to create cyber career entry roles

DSIT should consider introducing incentives to help organisations hire and train less experienced people in cyber roles. This could be through developing components of Tech First, apprenticeship schemes and graduate programmes. These incentives could be linked to policies for stimulating informed demand for cyber.

Suggestion 8 – Double down on skills

Developing cyber skills needs to be embedded more deeply in more places. Building on the NCSC materials, cyber leaders (across DSIT, DBT, Department for Education, and regionally) need to keep supporting and communicating the value of all of the initiatives, from schools programmes and professional development to mentoring cyber founders.

Suggestion 9 – Review the Computer Misuse Act

Recognising there is an enforcement challenge, the Government should review whether amendments to the Computer Misuse Act can be made to address the negative impact it has on skills development and broadening UK cyber growth and resilience.

[51]This relates to publicly funded IT solutions like the Government Digital Services, smart meters, or data sharing environments and consent mechanisms in sectors like health or energy

[52]All Tech Is Human (2024) All Tech Is Human and the Consulate General of Finland Present Strengthening the Information Ecosystem on March 6, 2024

3. Supply and demand

In an increasingly volatile geopolitical climate, market failures, cyber threats, and shifting alliances pose growing risks to national security and economic stability. In this context, organisations are facing resilience risks that may not be directly related to the priorities of their business. Identifying and addressing these risks and strengthening the demand for UK-based cyber security services and products is essential to ensure resilient digital infrastructures across all sectors, enhancing the nation's sovereign capabilities, and enabling stable conditions for business and investment.

It is already well recognised that the cyber security supply sector contributes to the UK's economic growth. It also serves a wider socio-economic purpose, producing 'multiplier effects'[53]. Namely, investment in the cyber sector drives job creation, innovation, improvements in the quality of products, and, ultimately, greater public trust in technology and institutions, helping to future-proof the UK economy in uncertain times.

This section reviews the characteristics of supply and demand for the cyber security industry in the UK, based on a brief market overview, a rapid review of published evidence and participant insights.

The 'demand' subsection focuses on two crucial challenges. First, mandating greater cyber security uptake among organisations often seen as 'lagging behind', such as supply chains to critical infrastructure, SMEs, and local authorities. In particular, Cyber Essentials has been identified as an important tool for improving resilience, and is an example of stimulating demand to create cyber growth[54]. Second, supporting UK-based cyber security SMEs, which frequently face barriers in selling products and services to government departments. Here, the report highlights the need for interventions in public procurement systems to stimulate demand for the domestic cyber security sector.

The 'supply' subsection addresses the pressing challenge of enhancing the availability of high-quality cyber security products and services, recognising that insufficient understanding among buyers contributes to lower market standards[55]. The report highlights recent initiatives calling for improvements to the assurance process to address this issue.

3.1. State of the sector supply and demand: facts and figures

- In 2024 the UK cyber security products and services sector grew by 12% to £13.2 billion and the sector employed ~67,300 Full Time Equivalents (FTEs), up by 11% from the previous year[56].
- The UK is home to 2165 active cyber businesses, just over half being micro-businesses[56].
- During 2024, £206 million investment was raised by dedicated cyber security businesses. This is less than recent years, but it is seen as a return to 'pre-pandemic' 2018-19 levels, rather than loss of investor confidence or engagement[56].
- The Cyber Essentials scheme has been in operation for over a decade, with a steady increase in uptake, and emerging evidence on its effectiveness. According to the NCSC report, 89% of Cyber Essentials-certified organisations would recommend the scheme and 69% believe it made them more competitive. The uptake of the scheme has seen an upward trajectory over the past several years, with over 33,000 certificates awarded in the past year, representing a 20% increase from the previous year. However, this still represents a fraction of businesses, as the UK is home to 5.5 million private businesses. Only 11% of organisations review cyber security risk in their supply chains[57].
- Despite the rise in supply and demand for cyber, incidents are also more frequent. In 2024, the NCSC responded to 50% more nationally significant incidents compared to the previous year and reported a threefold increase in severe incidents[58].
- The UK is the third largest exporter of security services and expertise worldwide with total value of exports approaching £11.0 billion in 2023. Security services include a range of technologies, e.g. fire equipment, managed services, personal protective equipment and others. Within that, cyber security was valued at £7.2 billion, an increase of 18% from 2022[59].

[53]Pakes and Pitts (2023) Securonomics
[54]Cyber Essentials impact evaluation - GOV.UK
[55]Debate Security (2020) Cybersecurity Technology Efficacy: Is cybersecurity the new market for lemons?
[56]DSIT (2025) Cyber security sectoral analysis
[57]NCSC (2024) 10 years of Cyber Essentials
[58]NCSC (2024) NCSC warns of widening gap between cyber threats and defence capabilities. The NCSC defines 'nationally significant' as having a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy
[59]Department for Business and Trade (2023) UK security export statistics 2023. The international comparisons ought to be treated carefully due to diverse methodologies used to calculate total exports for different countries

3.2. Stimulating demand and reducing burden

3.2.1. Mandating the fundamentals of cyber security

The majority of participants stated a clear need for UK organisations to strengthen their cyber security fundamentals, the core practices with the strongest evidence base for improving resilience. These include measures such as timely patching, implementing multi-factor authentication, and managing the attack surface effectively[60]. This need is particularly acute among SMEs, charities, and local authorities, which are often under-resourced and face significant challenges in maintaining robust cyber security.

Many participants spoke about Cyber Essentials and the role and future of this programme. Cyber Essentials has been described as a valuable, low-cost intervention that has helped to reduce vulnerabilities and lower incident rates, particularly benefiting smaller businesses when trying to gain access to some procurement frameworks. The evidence base suggests that Cyber Essentials controls could effectively mitigate most attacks during the initial phases but many organisations will require additional measures such as back-ups, security awareness training, logging and monitoring[61]. A major concern raised was the low uptake of Cyber Essentials among SMEs embedded in the supply chains of large organisations and critical infrastructures, thereby posing systemic risks to the nation's cyber resilience.

Cyber risks are recognised as complex and distributed, with supply chain security identified as one of the most significant challenges. Addressing this requires a stronger mandate for cyber security improvements. Recent research highlights varied interpretations of 'supply chains', which has led to inconsistencies in the quantity and quality of guidance provided by national authorities and across sectors. This is further complicated by the absence of a shared taxonomy to support procurement and risk management[62].

Participants generally supported the idea of a Cyber Essentials refresh while highlighting the need for a precise intervention, rather than a major overhaul. They cautioned that mandating cyber requirements to all organisations could create barriers for smaller domestic businesses or discourage international companies from operating in the UK. In addition, the insufficiency of 'checklist-based' approaches could stagnate progress for more cyber-mature organisations.

Case study: Cyber Essentials stimulates resilience and growth

This report argues that stimulating demand will support the virtuous cycle of improving resilience of businesses, which will create confidence and growth for those businesses and in turn create growth for the cyber sector.

Based on the Cyber Essentials Impact Evaluation[63], there is evidence that Cyber Essentials improves the security posture and resilience of the businesses that adopt the scheme. There is also evidence that Cyber Essentials users encourage other businesses to adopt Cyber Essentials, thus broadening the impact on resilience. Quoting from the report:

'There is evidence that Cyber Essentials is overcoming the information asymmetry around cyber security; furthermore, that the scheme is now making organisations able to consider cyber security as part of their purchasing decisions. For example, the majority of Cyber Essentials users (61%) say they are more likely to choose suppliers that are Cyber Essentials certified than those without certification, while three quarters (75%) say they have greater confidence working with certified suppliers.'

The scheme has a direct impact on growth of the cyber sector, which in turn feeds the virtuous cycle of wider capability and resilience.

'The Cyber Essentials scheme is encouraging strong growth in the cyber security sector, with increasing numbers of Certification Bodies and assessors. This means a stronger external support network for cyber security should organisations need it for information or advice.'

And there is belief amongst those using Cyber Essentials that it helped with market competitiveness.

'Finally, more than two thirds of Cyber Essentials users (69%) believe that Cyber Essentials has increased their market competitiveness. This includes certification being perceived as "achievable" which makes the cost-benefits clearer to see, gaining additional credibility since their organisation is taken more seriously, and experiencing increased commercial activity since becoming certified.'

And

'Cyber Essentials evidently yields further commercial benefits considering that a third (33%) of contracts that Cyber Essentials users entered into over the preceding 12 months required them to be certified through the scheme and more than two thirds (69%) believe the scheme has increased their market competitiveness.'

Thus there are good grounds for believing that expanding Cyber Essentials and other changes that improve cyber risk management and engagement will stimulate demand and the virtuous cycle in the same way.

Participants were in a broad agreement that more emphasis should be placed on offering support in the face of the continuous nature of cyber security maintenance such as multi-factor authentication (MFA)[64] or patching. They also identified the need to help under resourced organisations with digital transformation more broadly, rather than solely focusing on cyber security. This comes from the appreciation that organisations are receptive to guidance when seeking to configure or update their digital infrastructures. However, it is important to bear in mind that these changes are usually prompted by a business need e.g. for communications, transactions, accounting, or client management and implemented via system integrators, rather than bespoke cyber security solutions.

Embedding security into products from the outset reflects the idea of 'secure by design', that is shifting the responsibility to software vendors to develop secure products[65]. According to the NCSC[66], security by design should be achieved through the combination of regulated standards (see the UK Product Security regime introduced in 2024[67]) and market incentives such as liability frameworks, financial reward, transparency, and consensus on security baselines.

Several participants talked about the complexity of complying to different regulations. Some pointed out the value of mapping standards or having fewer interfaces to have to deal with. While the NCSC and DSIT have already developed valuable mappings: across Internet of Things (IoT) product security[68]; and the Cyber Governance Code to the Cyber Assessment Framework[69]; several gaps remain.

In particular, the alignment of the UK standards with the upcoming EU regulations and sector-specific mappings stand out as areas for improvement. Further to that, some participants pointed out that mapping could act as an intermediate step towards the wider international harmonisation of standards to reduce the burdens on organisations operating in both domestic and export markets.

Case study: Energy sector partnerships in supply chain cyber security

The adoption of The Security of Network and Information Systems Regulations (NIS Regulations)[70] was an early example of mandating cyber security improvements in the UK. For many critical infrastructure operators, it presented opportunity to build security teams, argue for investment in infrastructure upgrades and start a dialogue with regulatory bodies through the practitioner-led Communities of Interest[71]. Partnership work was deemed particularly helpful for supply chain security, which did explicitly not fall under NIS (2018).

One of the responses worth highlighting comes from the UK energy sector community who convened to develop the common cyber security procurement guidance and establish industry-wide dialogue with the supply chain[72]. This collaboration has improved standardisation in cyber security to the benefit of suppliers and operators alike.

Initially involving only operators and policymakers, the work expanded to include 'validation' discussions with key suppliers. These open conversations helped both sides understand procurement tensions and how cyber security requirements could be better delivered. Suppliers highlighted that some procurement processes inhibited honest cyber security discussions and stressed the need for shared responsibility. Operators emphasised that cyber security should be integral to proposals, not an optional extra.

[60] Woods and Seymour (2024) Evidence-based cybersecurity policy? A meta-review of security control effectiveness

[61] Badva et al (2024) Assessing Effectiveness of Cyber Essentials Technical Controls and Such et al. (2019) Basic Cyber Hygiene: Does It Work? Here, the report authors caveat that the studies ground their claims in hypothetical data (e.g., architectural reviews, configuration reviews, and interviews) rather than industry data from past attacks

[62] Topping et al (2021) Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks

[63] Pye Tait Consulting (2024) Cyber Essentials impact evaluation. Commissioned by DSIT

[64] An example of that are ongoing efforts to roll out mandated MFA by major cloud providers (Google Workspace, Microsoft 365 and Azure) by the end of this year

[65] Examples include avoiding default admin/login passwords, automatic updates, enforced permissions in apps, built-in phishing detection, end-to-end encryption for communications

[66] NCSC (2024) NCSC Annual Review 2024

[67] DSIT and Viscount Camrose (2024) he UK Product Security and Telecommunications Infrastructure (Product Security) regime

[68] DSIT and DCMS (2018) Mapping of IoT security recommendations, guidance and standards

[69] DSIT (2025) Mapping cyber governance code to NCSC Cyber Assessment Framework

[70] DCMS (2018) The NIS Regulations

The case study above shows the value of communities working together on adoption and best practices. Some participants highlighted other areas where guidance has been in development but not available and suggested it would help if 'work in progress' regulations and standards could be shared as early as possible to help communities to input and align with them.

Participants widely praised the introduction of the NCSC Boards Toolkit and 'My Cyber' SMEs Toolkit. However, the conversation about adopting 'baseline' cyber security improvement is still not sufficiently linked to businesses' understanding of risks of cyber-attacks (e.g., financial, reputational and trust-related impacts). This gap is made worse by a wider accountability crisis at the board level, where IT failures (e.g., the Post Office scandal) are often poorly understood, downplayed, or blamed on technical teams rather than recognised as governance responsibilities. Some participants highlighted the problem of identifying where accountability should lie when regulation fails, although there were no simple solutions here. Despite the fact that material cyber risks are already subject to disclosure obligations, participants questioned whether stronger expectations or guidance are needed, given the growing threat landscape. This is not about reporting cyber incidents, but about highlighting for investors or other stakeholders, where cyber may impact the business and the steps being taken to manage and mitigate those risks. The evidence[73] suggests many are highlighting cyber risk, but there is a prevalence of low-quality reporting that lacks detail. Clearer guidance and expectations are needed to raise the quality of corporate cyber reporting. Overall, recent research argues that the cyber security market can be characterised as a failure of a 'merit-good', that is a public good that is not consumed optimally if left solely in the hands of the market[74]. This analysis leads to the following recommendation to stimulate informed demand through guidance, regulation and assurance.

Recommendation 2 – Stimulate informed demand

Government should use guidance and regulations to stimulate growth by setting expectations for high quality reporting of cyber risks, consulting on mandating the use of Cyber Essentials, and encouraging usage of cyber insurance and principles-based assurance.

The goal is to encourage organisations across sectors to prioritise cyber security in alignment with their organisational risks, thereby reducing incidents, increasing resilience, supporting broader economic growth, and driving demand for more UK cyber services.

Implementing this recommendation will require understanding of the implications for stakeholders and a phased approach to change as outlined in the following suggestions.

Suggestion 10 – Mandate Cyber Essentials in selected supply chains

DSIT and CISOs representative of critical or otherwise relevant sectors should agree on key controls to mandate across supply chains, starting with Cyber Essentials. A phased approach should embed these requirements into procurement frameworks for government departments, critical infrastructure, and large businesses. Over time, alignment with standards like NIST SP 800-161 should be considered. As the scheme evolves, NCSC should lead on building the evidence base for its effectiveness, working with academic and insurance sector experts.

Suggestion 11 – Map standards and regulations to help navigate compliance

NCSC, DSIT and DBT to continue their mapping and harmonisation efforts, prioritising international alignment and communication to organisations with significant export markets.

Suggestion 12 – Share guidance early to reduce burden

NCSC to share emerging cyber guidance early to help communities anticipate and share best practices and deal with overlaps and gaps. This could be particularly valuable for critical infrastructure operators whose budgets are regulated through long-term funding cycles and currently lack alignment with the updates of the Cyber Assessment Framework .

Suggestion 13 – Improve guidance on the reporting of cyber risk

Government should seek evidence and develop proposals on the quality of corporate reporting on what cyber risks exist for a business and how they are managed. The evolving proposals should help businesses tighten the connections between cyber risks and the material risks they are obliged to report on.

3.2.2. Facilitating SMEs access to government procurement

Participants characterised difficulties in accessing government procurement frameworks as a long-standing barrier to UK-based cyber security SMEs with potential innovations and solutions. In particular, the following challenges persist:

- the procurement process is too slow to work with the 'time to market' pressures faced by SMEs;
- procurement teams are mainly motivated by price and compliance at the expense of product fit. If 'product fit' is ever considered, it is usually limited to short-term requirements;
- buyers in government can lack domain expertise to select the best quality products;
- buyers rarely ask for product roadmaps or look at longer term solution fit;
- among buyers, there is insufficient knowledge sharing with regards to the solution efficacy.

A widely shared view among participants is that the UK Government, as a cyber security buyer, could do more to engage and support the domestic cyber security sector. Current procurement practices often favour large systems integrators, creating structural barriers that disadvantage smaller specialist cyber security businesses. A few examples of good practice in pre-procurement activities should be highlighted, e.g. the industry days[75] held by the Ministry of Defence. However, the existing procurement environment diminishes incentives for entrepreneurial innovation and risks entrenching incumbents, potentially undermining both market dynamism and national cyber resilience.

While policy efforts exist to broaden SMEs participation[76], practical challenges in procurement processes and risk management continue to limit meaningful access for newer entrants. Likewise, recent research argues that government buyers, especially in under resourced organisations, such as local authorities, should receive structured support to be able to confidently buy digital technologies in the public interest[77].

One opportunity for improvement highlighted by participants was adding meaningful weight to factors related to cyber security in the procurement decision frameworks, a suggestion inspired by the recent Industrial Strategy which states the intent of 'using government's procurement power to create good quality local jobs and boost skills by streamlining and strengthening criteria for suppliers to contribute to these objectives in their bids'[78]. While the reform introduced in the Procurement Act (2023) is a step in the right direction, some participants expressed an appetite for more radical and experimental solutions. For example, the government of Canada runs 'Innovative Solutions' programme providing both early-stage funding and linked-up procurement opportunities[79].

The above analysis leads to the following implementation suggestions in support of **Recommendation 2 – Stimulate informed demand**

Suggestion 14 – Support pre-procurement engagement for SMEs

The UK Government (Crown Commercial Services) and innovation incubators (for example but not limited to programmes such as Cyber Runway) should implement formal pre-engagement mechanisms to help SMEs showcase their cyber security solutions and educate procurement teams ahead of tender processes. This could include regular market engagement days, innovation showcases, and technical briefings specifically aimed at introducing SME capabilities to public sector buyers.

[71] Michalec et al. (2021) Reconfiguring governance: How cyber security regulations are reconfiguring water governance
[72] Wallis and Dorey (2023) Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience
[73] DSIT and Clark (2025) Research on the prevalence and quality of cyber disclosures
[74] Arroyabe et al. (2024) Exploring the economic role of cybersecurity in SMEs: A case study of the UK
[75] Ministry of Defence (2025) Preliminary Market Engagement Rapstone Industry Day
[76] Crown Commercial Service (2024) SME Action Plan
[77] Sanchez-Graells, A. (2023) Guaranteeing public sector adoption of trustworthy AI - a task that should not be left to procurement.
[78] P. 69 of the UK's Modern Industrial Strategy (2025)
[79] Government of Canada (2023) Innovative Solutions Canada: Annual Report 2022–23

3.3. Assuring supply with transparency and quality

A review of evidence as well as participant input identifies regulations (e.g. NIS Regulations[80]) and perceptions of crisis, for example attacks on retailers in early 2025[81], as two main factors stimulating demand[82,83]. However, the rise in demand for cyber security solutions doesn't automatically translate into a boost in cyber resilience. This is because both cases can create a poor information environment for adequate judgement of product quality and relevant risks. Buyers of cyber security are rarely driven by independent analysis, instead, the cyber security market is primarily based on interpersonal relationships as well as 'Fear, Uncertainty and Doubts' sales tactics[84]. Put simply, growing the cyber security industry without ensuring product quality would be a risky strategy for the country.

Researchers and participants characterise the problem as a market failure of information asymmetry between vendors and buyers[85]. This 'market failure' is characterised by poor information availability among the potential buyers of cyber, driving down the overall product quality on the market. As a result, cyber security products may lack efficacy, including the capability to deliver the security mission (fit-for-purpose), practicality in operations (fit-for-use), quality of security build and architecture, and provenance of the vendor and supply chain[86].

Case study: Principles Based Assurance

A growing consensus among the cyber practitioners is the need improve demand side literacy: 'We require informed demand'. Product assurance is an emerging solution for this problem and is receiving growing adoption within the cyber security sector.

One development worth highlighting is the NCSC's Principles Based Assurance (PBA)[87]. This emerging approach assesses security against high level, outcome focused principles rather than rigid technical checklists. To deliver this methodology the NCSC is setting up Cyber Resilience Test Facilities (CRTFs)[88] aligned with the Software Security Code of Practice[89], ensuring products are secure by design.

PBA encourages organisations to adopt proportionate, flexible and context driven security measures aligned with their specific risks and operational environments. Instead of prescribing exact solutions, the model supports innovation, scalability and adaptability.

This approach is a tool for risk owners to gain confidence in the products they are deploying. It could give a vendor a badge of 'cyber quality' which could help them sell. But there needs to be demand from the buyers.

Recent exploratory research recommended that the NCSC develop sociotechnical expertise in assurance communication to better align the perspectives of buyers and vendors[90]. If implemented effectively, PBA could help overcome checklist and audit fatigue by encouraging security buyers to continuously improve and reflect on the state of their digital infrastructures.

This analysis and input led to the following implementation suggestion for **Recommendation 2 – Stimulate informed demand**

Suggestion 15 – Accelerate the development of Principles Based Assurance

Accelerate adoption of the Principles Based Assurance in codes of practice and development of appropriate assessment facilities. This action will need pre-engagement activities and incentives between vendors and buyers, to make it real, and so should involve DSIT and the NCSC, and be supported by evidence from the academic leaders (e.g. Research Institute for Sociotechnical Cyber Security).

[80] Michalec (2023) What's next for the NIS Regulations? Findings from RITICS Fellowship
[81] Marks and Spencer (2025) Cyber incident update
[82] Dkaidek (2025) Contextual Dynamics in Cybersecurity Investment Decision-Making. Paper available upon request
[83] Michalec et al. (2020) Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures
[84] Dkaidek (2025) Contextual Dynamics in Cybersecurity Investment Decision-Making. Paper available upon request
[85] This is known as a 'market for lemons' problem in Anderson and Moore (2009) Information security: where computer science, economics and psychology meet; Debate Security (2020) Cybersecurity Technology Efficacy: Is cybersecurity the new market for lemons?; Woods (2023) Lemons and Liability: Cyber Warranties as an Experiment in Software Regulation
[86] Debate Security (2020) Cybersecurity Technology Efficacy: Is cybersecurity the new market for lemons?
[87] The NCSC (2025) Principles Based Assurance
[88] Cyber Resilience Testing - NCSC.GOV.UK
[89] Software Security Code of Practice - GOV.UK
[90] Spencer (2025) ASSURANCE BY PRINCIPLE: Preparing for the next generation of product security assurance. RISCS report

4. Places

Many participants suggested that organising the sector around places would facilitate cyber growth and, as explained below, foster teams that may be able to respond to future crises in a more agile way. The UK already has 18 cyber clusters who collaborate through the UK Cyber Cluster Collaboration (UKC3)[91]. The cyber clusters are regionally based and focus mainly on the supply side. A different approach is required and should be based on a smaller number of places that combine multiple regions and unite the supply and demand sides. Strong leadership is a prerequisite for such places to succeed and is addressed below.

In this section, the evidence collected from participants supports the argument for a small number of strategic places that support futures thinking, nurture chosen technical areas and provide safe environments for experimentation and the development of novel solutions. The NCSC has a role to play in supporting this activity.

Many participants supported the selection of a small number of places to focus on developing a new generation of innovative cyber technologies, whilst recognising that this might exclude a large part of the cyber security talent. To mitigate this risk, it is important that such places work in a super-regional way: if a place is selected in the South West of England, it must also incorporate South Wales and, similarly, a place in the North West of England must incorporate the North East too. Moreover, participants highlighted the need for national coordination between places. Such coordination could be provided by the UK Cyber Growth Leader role (suggested by several participants) or possibly through an organisation such as the Digital Catapult. This input is behind **Recommendation 5 – Appoint growth leaders in places of cyber strength.**

Whilst non-UK investors may see the UK as a single entity, local groups of angel investors tend to concentrate on a place. Places are also essential for shaping research and development, and building the relationships that a people-centric business like cyber depends upon.

Participants confirmed that the UK is widely recognised as having world-leading strengths in areas such as secure-by-design, high-grade cryptography and software assurance and verification. The UK also has diverse strengths spanning capability in government and university research, to regional clusters and ecosystems around research centres, major tech companies and industries.

Different regions in the UK have different mixes of skills, infrastructure, university, government and commercially-driven innovation. Analysis of participants' input suggests that the assets and organisations in a region are important, and that connectivity is essential for 'getting innovations out there and used'. Many startups and spinouts, which can be good vehicles for rapid technology scaling, find their first customers within their local region. At the same time, the investment ecosystems in different regions are at very different levels of maturity.

Where regional markets are underdeveloped or fragmented, or where international markets offer greater scale, profitability, or access to specialised customer bases, businesses may choose to adopt an 'export-first' strategy, prioritising national or international markets early in their growth cycle, rather than relying solely on local demand.

Participants told us that this approach is already being taken by businesses in Northern Ireland, where a significant proportion of external sales were directed to Great Britain (GB), the Republic of Ireland (ROI), and the United States (US) due to limited local opportunities to support scaling. This highlighted the importance of external markets in sustaining growth for businesses operating in specialised niches that are too small to scale effectively within the region alone. In this context, participants noted that regional and devolved administrations infrastructure and expertise is still essential, in supporting export ambitions. Access to commercial skills, especially the ability to sell into international markets was also a key factor in their success.

The UK academic centres of excellence in cyber security research and the four cyber research institutes[92,93,94,95] were competitively awarded and have been an effective community of academic experts for a long time, although by focusing on institutions there is a risk that some experts are excluded. Between this research community and initiatives to support, train, promote and mentor cyber startups (CyberASAP, Cyber Runway, the NCSC Cyber Accelerators programme and more) there is strong connective tissue that has helped ensure a healthy supply of cyber startups. The new UKRI Network+, CRANE[96], will address the exclusivity of some of the earlier academic schemes by including a greater proportion of the UK's academic expertise.

[91] UK Cyber Cluster Collaboration (2025) Home
[92] VeTSS – The Research Institute on Verified Trustworthy Software Systems (n.d.) Home
[93] RITICS – Research Institute in Trustworthy Industrial Control Systems (2025) Home
[94] RISE UK Research Institute in Secure Hardware and Embedded Systems (n.d.) Home
[95] Research Institute for Sociotechnical Cyber Security (2025) Home
[96] CRANE - Cyber Security Research Network (2025) Home

The DSIT 2025 cyber sector survey[97] organised businesses into twelve geographies, with 38% in London, 17% in the South East, 8% in both the North West and the South West, 7% in the East of England, and 6% in Scotland. These place-based strengths likely relate to government and industry locations and capability, with a lot of detail hidden behind the numbers. The question is whether and how to do more to stimulate activity in these places through shared spaces to support the co-creation of solutions – a characteristic of work in this sector. Ideally, such co-location spaces should convene a 6-helix of large enterprises, SMEs, academia, investors, government and civil society. The latter constituent could be represented by local government and schools/colleges or third sector organisations.

Proximity to talent is critical and in the security sector this tends to be located around government bases of activity. There is a need to have a porous capability between government, businesses and academia to ensure that real-world problems and appropriate skills are translated across. Subject to appropriate clearances and agreements, there should be fewer obstacles for individuals to move between organisations in the 6-helix. Co-working spaces have always been critical to enable fruitful collaboration[98] and could also support porous interaction between local government, stakeholders, and potential solution providers. To make progress here the suggestion is that the UK would be best served by choosing a small number of places that already have a healthy cyber ecosystem in which to develop Cyber Growth Centres (CGCs) with regional leaders to grow the cyber sector.

Each place based CGC leader would have responsibilities which include local leadership and obligations to deliver on the recommendations listed below. They would also have the responsibility to coordinate with fellow CGC leaders and support the UK Cyber Growth Leader role. The NCSC Industry 100 (i100) scheme has developed a cohort of senior figures who have suitable experience to assume these leadership roles. We recommend that CGC leaders have senior industrial experience and are appointed through an organisation such as the Digital Catapult. Whilst several participants argued for the appointment of a National 'Cyber Ambassador', it was suggested that this role need not necessarily be a government appointment but should have an expanded brief which could include:

- Promoting UK cyber capability internationally with a focus on supporting startups and smaller companies to reach export markets.
- Working with international organisations to harmonise cyber regulation; and to help companies navigate the international regulatory landscape.
- Liaising with place-based leaders, to coordinate their activities and support growth journeys.

Leadership will be essential to convene stakeholders, align strengths with national priorities and drive sustained action in the CGCs. It will ensure that this report's place-based recommendations to develop future-oriented communities, nurture distinct tech areas and provide safe environments achieve the intended growth impact.

Recommendation 4 – Appoint a UK cyber growth leader

Government should appoint a leader to provide expertise and drive coordinated action across the cyber security industry and within Whitehall. This role would encompass some of the previous Cyber Ambassador's responsibilities in advancing export growth and supporting national security objectives. It would also include responsibility for driving this growth plan forward.

The goal is to ensure cyber growth is prioritised and integrated across several policy areas.

Recommendation 5 – Appoint growth leaders in places of cyber strength

Appoint place-based leaders to be responsible for convening and driving cyber growth initiatives and outcomes. These leaders should have industry experience, support the UK cyber growth leader and be independent from central and regional government.

The goal is to ensure places use their strengths to grow, create, and attract more cyber businesses.

[97] Ipsos and Perspective Economics (2025) UK Cyber Security Sectoral Analysis

[98] Examples include business and academic-led centres such as the cyberQuarter in Abertay, the Centre for Secure Information Technologies (CSIT) in Belfast, the Digital Security Hub (DISH) in Manchester, Hub[8] in Cheltenham and Plexal in London.

[99] Chuenjitwongsa (2017) How to conduct a Delphi study

[100] Liveley et al (2021) Futures literacy through narrative

Suggestion 16 – Choose a few places for Cyber Growth Centres

Government should work with place-based stakeholders to identify areas of strength and establish Cyber Growth Centres. These Centres should be coordinated at the national level and have an obligation to engage with adjacent regions not directly served by a co-location centre.

Suggestion 17 – Support growth leaders with funding and structure

No current place has everything it needs to be a Cyber Growth Centre. To enable leaders to drive growth, they will need both support, for example through being employed within a common organisational structure such as the Digital Catapult, and access to funds, whether through local, regional, or national mechanisms.

4.1. Develop Futures

Many organisations are too busy fire-fighting today's threats to be able to focus on longer term futures. However, the threat landscape is rapidly evolving, and it is highly likely that disruptive technologies will severely impact the UK within the next few years. Successful anticipation of these disruptors can provide significant growth opportunities through UK companies being first to market with tools and mitigations.

One role for CGCs would be to convene stakeholders to conduct exploratory technology foresight work using a suitable futures methodology (for example a Delphi exercise[99] or the use of performative narrative creation[100]). This might be academia-led but should involve all of the different stakeholders in a given place. Some of the futures exercises may be place-focused (for example the impact and security implications of Industry n.0 on a region that is strong in manufacturing), others will be nationally important. The different futures should be aggregated at the national level to embed futures thinking in the cyber ecosystem.

Larger businesses could also socialise their mid to long term challenges and work with SME/startups and academia in the community to co-create potential solutions. In many cases, the solutions to one organisation's mid to long term challenges will have much wider applicability and would be suitable for new startup activity. The local investor community should be engaged here but the place-based cyber growth leader should also be resourced so that there is grant-based support for such futures focused initiatives. Whilst this recommendation is primarily a responsibility for the Cyber Growth Centre leader and local leadership, academia has an important role to play in facilitating the futures exercises and co-creation of solutions. A DSIT cyber growth fund would provide the CGC leader with the resource to co-fund potential winners.

Recommendation 7 – Develop futures-oriented communities

Place-based leaders should use their convening role to look forward and shape future markets. To do this, they should bring together CISOs, academia, small and large industry, government, and other stakeholders to share perspectives on, and pursue solutions to emerging cyber challenges.

The goal is to drive initiation, co-creation and delivery of innovative projects into the market, and to build a culture of anticipation.

The following suggestion provides an implementation approach for the development of these futures-oriented communities through the CGCs.

Suggestion 18 – Use places used to convene stakeholders on futures

Cyber Growth Centres should act in a convening role to bring together stakeholders to engage in futures planning and ensure that the place and the country innovate to remain resilient in the face of future technologies and threats.

4.2. Nurture chosen cyber security topics

Cyber Growth Centres should not be set up to compete with one another. The UK cyber ecosystem should operate as a single team with each place playing to its strengths in support of a common quest for growth. The selected CGCs should be able to demonstrate a pipeline of place-based talent that is equally strong across all elements of the 6-helix: large businesses supporting a fertile regional ecosystem of startups, a strong investment community and support from central government and local community groups. CGCs should also be able to demonstrate that this place-based talent can contribute to national excellence and leadership in a strategic cyber security topic or theme. For illustrative purpose only, the former might lead to CGCs such as:

1. West England and South Wales: defence and intelligence
2. North England: offence and advanced manufacturing
3. South England: finance and enterprise IT
4. Northern Ireland: outsourcing of services
5. Scotland: energy and security at the edge

Alternatively:

1. West England and South Wales: IT security
2. North England: cyber-physical security
3. South England: verification and assurance
4. Northern Ireland: hardware security
5. Scotland: verification and formal methods

Nurturing a cyber security topic will entail the CGC convening discussions about different futures for that topic, providing safe havens and data sharing to support growth and allowing startups to benefit from the experience of later stage founders in the region. Such founders could also benefit from being brought together as a community to share each other's networks, cross sell and collaborate, and to be a supportive peer group.

The place based cyber growth leaders should liaise with the UK Cyber Growth Leader to ensure that the work in any one place does not become siloed and that the places work effectively together as a network.

Recommendation 8 – Places to nurture distinct tech areas

Places should be strategic in prioritising technologies and application areas based on their cyber strengths and sector connections in alignment with the Industrial Strategy and the UK Government Resilience Action Plan. Cyber innovation in AI, cyber-physical systems, and tooling for fundamentals should be considered as initial priority areas.

The goal is for the UK to have place-based cyber strengths that are more than the sum of its parts, each contributing to UK cyber growth.

It will be important to work with regional stakeholders to identify what tech areas are best nurtured by which places. A consultation with regional leaders is suggested to inform decisions.

Suggestion 19 – Engage with places to identify strengths to focus on

The choice of location and themes for Cyber Growth Centres requires further exploration, namely a rapid study to engage with regional leaders to make informed choices on both. From the current review (see section 5.2) this report suggests that AI, cyber physical systems, quantum, tooling for fundamentals and digital secure by design should each be considered as key themes for growth.

4.3. Safe environments

Creating safe environments would ideally be a natural follow-on step from the futures discussions proposed above and would cover all topic areas of cyber. A key difference between these recommended 'safe environments' and existing national security co-creation environments, would include the ambition to try and do this without all stakeholders needing to hold clearances. A 'gold standard' version would be to include (suitably anonymised) real-time feeds from various Security Operations Centres and testbed facilities to provide a basis for many of the exercises and discussions. The Jill Dando Institute Research Laboratory[101] provides an example of an environment which supports access to sensitive data sets and the Innovation Hub in Cheltenham[102] is another example. However, neither environment currently provides the full range of facilities and ease of access that we propose is needed to drive cyber growth. New 'safe environment' facilities would support growth by enabling companies to demonstrate the scalability of their solutions and their applicability to real world systems at national level through the practice of challenge-led exercises.

Where appropriate, these exercises could be used to create demonstrators and training material for businesses, Further and Higher Education providers, consultancies, service providers, or schools – thereby helping to amplify the outcomes.

Such exercises, if challenge-led rather than problem-led[103], would build local and regional capability in working together and could enable groups to form the basis for place-based responses to large scale cyber events, something that the real-time feeds could also support.

Curation of which strategic challenges to tackle should be determined by CGC leadership, considering both growth opportunities as well as national security outcomes.

[101] The Jill Dando Institute Research Laboratory (n.d.) About us
[102] https://cynam.org/
[103] A challenge-led exercise would start with an organisational or societal challenge which admits of a broad range of possible solutions and exploratory research whereas a problem-led exercise would be more focused and have a more constrained set of solutions.

Recommendation 9 – Places to provide safe environments

Create safe havens with infrastructure and data for multiple groups of stakeholders (not just those with security clearances) to explore, 'role-play', co-create and share how to assemble and test solutions to current and emerging challenges.

The goal is to build broader cyber resilience capability, which will both serve in moments of crisis and be a pool of talent for cyber growth.

Organising the sector around places and providing safe environments for collaboration will drive innovation and build resilience. These approaches will better prepare teams to respond with agility in future crises. The CGCs should play a central role in hosting and facilitating these collaborations, as suggested below.

Suggestion 20 – Target a few places to create safe environments

Cyber Growth Centres should provide the means for multiple groups of stakeholders to come together to explore, exercise, co-create, and share how to assemble and test solutions to both current and emerging challenges. This includes the Cyber Growth Centres providing safe havens where real data from Security Operations Centres can be made available for exercises.

4.4. NCSC's role in places

NCSC's primary responsibility to date, as the National Technical Authority for cyber security, has been focused on improving the resilience of the UK. NCSC also has an important role to play in supporting businesses through the initial stages of their growth journey. Discussions identified the need for the NCSC to support CGCs across all their growth initiatives, and particularly in supporting them to help with assessing startups. The Cyber Resilience Test Facilities[104] provide a national ecosystem of assured test facilities that provide evaluations using PBA for a broader set of products. They will most likely be funded and used by well-resourced vendors or buyers, but the ambition for CGC leaders with their resources, should be to work with NCSC to find ways for these assured test facilities to support startups.

Recommendation 6 – Expand the NCSC role

The Government should expand and appropriately resource the NCSC to help drive cyber growth. The NCSC is a 'crown jewel' for cyber resilience, which is their primary mission. They also have the capability to guide and steer for growth outcomes. Given the importance of resilience, growth should be added without diverting attention from their existing priorities.

The goal is to use the deep expertise of NCSC in support of cyber growth, e.g. guiding and validating cyber businesses, research, futures, and technologies.

The following suggestions outline how the recommendation to expand the NCSC role on growth can be applied. They offer practical ways to embed national leadership in place-based innovation and collaboration.

Suggestion 21 – NCSC to support place based cyber growth leaders

Expand the role of NCSC to support the place based cyber growth leaders. This should include supporting selected startups through each of recommendations 7, 8 and 9.

Suggestion 22 – NCSC to work with place based cyber growth leaders assessing startups

Recognising that assessing businesses for admission into schemes such as the Cyber Resilience Test Facilities is resource intensive, both in terms of people and testing facilities, the Cyber Growth leaders should work with NCSC and test facility leadership to support startups.

[104] https://www.ncsc.gov.uk/schemes/cyber-resilience-test-facilities/introduction

5. Futures

Emerging technologies can rapidly disrupt the status quo. Technological innovations bring new opportunities for greater efficiency and can develop entire new markets, but they are also a source of new short- and long-term vulnerabilities. Malicious actors are able to exploit these new vulnerabilities quickly, forcing businesses on to the back foot, needing to adapt while remaining on top of the day-to-day challenges that already occupy most of their resources. New threats from emerging technology are likely to arise within the next five years, and not the distant future. For greater economic resilience the UK needs to be better prepared for the challenges ahead.

This section explores how to work towards that preparedness by creating a mindset across the UK cyber community that can anticipate changes and be agile in its response, supporting both growth and resilience hand in hand.

The 'Anticipate not adapt' subsection focuses on the benefits of, and ways in which, the cyber community might come together to collaboratively explore possible trajectories of emerging technology through futures thinking.

The 'Disruptive technologies' subsection highlights some of the most prominent technologies that participants raised as future disruptors for UK businesses to grow into: AI, quantum, tooling for Cyber Essentials and cyber-physical. Case studies are presented within these topics that showcase where current communities have been brought together and where future community building could enhance outcomes.

'Exploring future business innovation' addresses innovative thinking around cyber insurance as a means of improving cyber resilience, and touches on the intangible economy highlighting the importance of extending futures thinking beyond technical developments.

5.1. Anticipate not adapt

Part of exploring the future is understanding the impacts of technology both beyond and because of their 'hype'. AI and quantum technologies have both fallen into this category. From a cyber perspective this can pose a significant challenge as technologies with the greatest publicity can siphon away resources and attention from other areas, including the need for underpinning cyber considerations. Cyber needs to be positioned as a partner in the development of these technologies, leveraging the high levels of public awareness while keeping security considerations at the forefront of developments.
The UK is a consistent research leader across a broad list of technology domains, and internationally trusted when it comes to cyber technologies[105]. This global recognition is an opportunity for the UK to help shape the future of the cyber sector. One approach is to make use of futures thinking tools[106] and methodologies to bring together stakeholders throughout the sector to anticipate and prepare for future developments.

The Delphi method is one such tool where structured questioning can refine stakeholder futures insights into those most important to that community. Stakeholders should include those from across large enterprises, SMEs, academia, investors, government and civil society to provide diverse input and to identify specific place-based considerations. A further useful tool for these conversations is the Three Horizon method[107], distinct from but not unrelated to horizon scanning, which can provide a structured framework for discussing both current and emerging challenges and opportunities through different horizons. Participants told us that many organisations prioritise the day-to-day challenges or progressing incremental gains. Less time is available for adapting to the latest technology or to those that may disrupt the landscape of entire sectors, as AI is doing. Whether it is AI, cyber-physical, quantum, tooling for fundamentals or business innovations, this report proposes that support to help the community explore emerging disruptive technologies while minimising the impact on the day-to-day challenges will go a long way towards greater resilience and growth.

In line with the place-based strategy laid out in the previous section, the regional cyber growth leaders will play a vital role in supporting a change in mindset to identify and address future challenges that are complimentary to local ecosystems.

5.2. Disruptive Technologies

5.2.1. AI is already changing cyber

The recent rise of AI, the pace of change over the last 5 years, and the level of attention it attracts offers a perfect example of why the UK needs to be better prepared for the challenges and opportunities it will bring. Often found at the top of the priority list for both government and across industry, many are trying to capitalise on AI technology's advantages. Rapid adoption brings with it a broad range of threats. From swathes of vulnerabilities introduced through 'vibe-coding' to privacy concerns on personal data upload, applications are likely to expand faster than they can be assessed. As with many other cyber threats, these vulnerabilities arise not just from technical sources but from the behaviour and understanding, or lack thereof, from those looking to benefit from the adoption of new AI tools.

The current vulnerability of AI to unforeseen risks emphasises the importance for cyber to be baked into the thinking around emerging technologies, and for all sectors of the cyber ecosystem to be able to pre-emptively identify the areas likely to be disrupted. Linking cyber and AI should be considered from both perspectives: AI for cyber, to identify new opportunities that enhance cyber products and services; and cyber for AI, to ensure the new applications don't open the door to those poised to exploit new vulnerabilities.

The UK is already doing much to investigate the security implications of AI through entities such as The Laboratory for AI Security Research[108] and The AI Security Institute[109] alongside the expertise embedded across academia and industry. There are also several businesses competing in this intersection of cyber and AI[110].From a growth perspective, the UK needs more businesses developing and operating AI for cyber and cyber for AI products.

Innovation around AI is likely to continue and lead to an expansion of opportunities and threats. Futures thinking led by the place based CGC leaders would complement existing work and ensure that cyber remains intertwined with future technologies and supports growth.

Recommendation 7 – Develop futures-oriented communities

Place-based leaders should use their convening role to look forward and shape future markets. To do this, they should bring together CISOs, academia, small and large industry, government, and other stakeholders to share perspectives on, and pursue solutions to emerging cyber challenges.

The goal is to drive initiation, co-creation and delivery of innovative projects into the market, and to build a culture of anticipation.

As discussed above, AI presents a significant opportunity for collaboration with the cyber sector to develop future products and services in an emerging sector

Suggestion 23 – Identify commercialisation opportunities for cyber safe AI

Work with the 'AI Opportunities Action Plan 2025' to ensure cyber programmes and commercialisation opportunities are developed. Place based Cyber Growth Centre leaders should convene futures sessions between researchers and businesses in AI and cyber and the demand side to identify and co-create new products and services.

[105]DBT (2025) Cyber security
[106]Government Office for Science (2024) The Futures Toolkit
[107]Government Office for Science (2024) Three Horizons: facilitation worksheet
[108]LASR | Mitigating AI Security Risks for UK Prosperity & National Resilience
[109]The AI Security Institute (AISI)
[110]Perspective Economics and DSIT (2025) AI and software cyber security market analysis

5.2.2. Further disruptions

Participants highlighted securing cyber-physical systems as an area that will soon need more attention. Much of the UK's critical national infrastructure, from energy systems to transportation, run on cyber physical operational technology. As such, cyber resilience for operational technology systems will only grow as a challenge. These systems have very different characteristics than IT systems and securing them requires different domain knowledge. This is an area of strength for the UK, with the Industrial Control Systems Community of Interest[111] providing a forum for knowledge sharing and innovation.

Quantum is another example of an emerging technology where the UK has deep expertise. The threat to public key cryptography is well understood[114] and the UK has growth businesses doing a good job anticipating and helping organisations to migrate classical algorithms. More broadly, quantum technologies look set to change many rules for security, but few people have deep expertise in both cyber and quantum, making this a challenge and opportunity for anticipating the future.

Case study: Research Institute in Trustworthy Industrial Control Systems (RITICS) and the Industrial Control System Community of Interest

Soon after the founding of RITICS[112] in 2014, the NCSC together with RITICS and leaders of the CNI Information Exchanges created the Industrial Control Systems Community of Interest. The Community of Interest[113] brings together government, regulators, vendors, operators, consultancies and academia to share knowledge, experience and threat intelligence. Current work within the Community of Interest includes The Workbook, a 'living document' that identifies common cyber security issues across the Industrial Control Systems community. There are currently twelve workstreams within The Workbook, which cover key issues including insider threat, supply chain, global positioning, and cryptography/ secure communication. The Community of Interest arranges monthly Lunch and Learn sessions on specific topics and holds a quarterly meeting. It also supports six expert groups which produce technical guidance published on their website.

Case Study: Quantum key distribution and post-quantum cryptography

Quantum is a useful illustration that what makes people feel safe can be quite different depending on the kind of technical discipline in which they have been trained. Quantum Key Distribution (QKD) is an alternative to public-key cryptography to establish secure communications based on the fundamentals of quantum mechanics. It is a hardware technology that measures the properties of single photons and uses those measurements to establish a secure key between sender and receiver.

At the same time as quantum key distribution is being trialled, the cryptography community has been developing new algorithms, post-quantum cryptography (PQC), that are not based on factoring large numbers, and not vulnerable to the class of quantum algorithms that will break today's public-key cryptography.

The two communities have different perspectives on the merits of their approaches, with advocates of quantum key distribution seeing it as being better because it is based on 'the laws of physics', whilst the cryptography community see post-quantum cryptography as being better because it is based on many decades of understanding what makes breaking an algorithm 'a mathematically hard problem'.

Deciding between the approaches depends on understanding how they can be embedded into and integrated with other hardware and software, and the energy costs of deploying the technology. NCSC's guidance is for organisations to complete their migration to post-quantum cryptography by 2035. Such guidance, whilst important to protect organisations and support PQC businesses, has consequences for the growth opportunities and strategies of quantum key distribution businesses. Facing and debating these types of challenging choices is a perfect example of work that CGCs can help to facilitate.

[111] Industrial Control Systems Community of Interest (2025) Home
[112] RITICS – Research Institute in Trustworthy Industrial Control Systems (2025) Home
[113] Industrial Control Systems Community of Interest (2025) Home
[114] NCSC (2025) Timeline for PQC migration revealed

5.2.3. Building better foundations

Participants expressed that a challenge for many businesses was putting in place the controls of Cyber Essentials. They pointed out that as well as skills, controls for Cyber Essentials really needs tooling. Some of this will be dealt with by Big Tech (Amazon, Microsoft, Apple, Meta, and Alphabet) but these will not cover every situation, especially in operational technology.

The level of influence and access that Big Tech has over major components of the technology landscape that allow for deployment of specific tooling on a global scale cannot be understated. They are also subject to having to bake solutions into products that cover entire markets and are subject to their demands and requirements. Cyber Essentials is a predominantly UK standard, not a universal approach, and therefore currently has a set of requirements that could be best met by UK developed technologies. Given their dominance it makes sense to try to include Big Tech in the futures thinking communities, to accelerate adoption and create new opportunities for UK businesses through partnerships and collaboration.

As well as tooling, several participants pointed to the need for better foundations. The Digital Security by Design programme[115] has made major progress in changing hardware foundations to remove classes of vulnerabilities (memory safety issues). There is still urgent need and an opportunity to use the UKs strengths in chip design and low-level software[116].

Case study: Digital security by design

Launched in 2019 through the UK Government's Industrial Strategy Challenge Fund, UKRI's Digital Security by Design programme aimed to identify ways to address the persistent cost and complexity of identifying and patching newly discovered vulnerabilities. In particular, the programme looked to address the vulnerabilities caused by memory safety issues, a known vulnerability since the 1970s and estimated to make up 70% of ongoing vulnerabilities[117], causing a move away from memory-unsafe languages[118]. By pulling together underlying academic research through CHERI with ARM's technical expertise, and cross-sector ecosystem engagement, the programme created a prototype platform and tools in demonstrator projects relevant to different sectors.

The Digital Security by Design programme embodied futures thinking. By exploring the widespread industry problem of patching vulnerabilities it worked towards identifying how to address the future of the technology through a combination of fundamental research and industry translation.

Discribe, an initiative within the Digital Security by Design programme that takes a social science-led approach, provides further evidence for the need to understand the various considerations towards adoption[119]. Adoption of this type of technology is unlikely to be driven by customer demand alone and will require interventions to overcome skills barriers.

The 2025 Industrial Strategy looks to continue support for the development of secure chips, but understanding and addressing barriers to adoption and encouraging uptake will be required to ensure a return on this investment.

Design choices being made today, for example on architectural decisions, are a near-term consideration that may rhyme with past missed opportunities to provide a secure by design solution and building of the associate companies that can grow to fill that need.

[115] UKRI (2025) Digital Security by Design (DSbD) programme outcomes
[116] RISE UK Research Institute in Secure Hardware and Embedded Systems
[117] UKRI (2025) Digital Security by Design (DSbD) programme outcomes
[118] CISA (2025) Product Security Bad Practices
[119] Discribe Hub (2025) Digital security by design: opportunities, adoption, developer readiness, regulation and attitudes

5.3. Exploring future business innovation

5.3.1. Cyber insurance

Participants identified cyber insurance as an important yet underutilised tool for improving cyber security resilience. Unlike some traditional insurance models, which cover harms to third parties (e.g., automotive), cyber risk insurance cover is largely internal to organisations. This structural difference limits the ability of insurers to drive better security practices, particularly as market dynamics incentivise minimal standards to remain competitive. While some insurers do push for stronger controls, such as multi-factor authentication and incident response readiness, these efforts are inconsistent and the market lacks clear, enforceable guidance[120,121]. The result is that many businesses, especially SMEs, either absorb higher premiums without improving their security posture or opt out of coverage entirely.

Policy proposals such as banning ransom payments raise further complexities. An outright ban on ransomware payments in particular sectors risks driving attackers toward domains which wouldn't be covered by the ban. Without concurrent investment in cyber security across all sectors, such a policy could also have perverse effects, making organisations more vulnerable to cyber extortion. In terms of market challenges, participants pointed out that the cyber insurance sector missed a key opportunity during the 2018–2021 ransomware surge[122]: while insurers raised premiums and tightened policies, they largely failed to provide clear, actionable guidance on how businesses could improve security to reduce costs[123]. This undermined the insurance market's potential as a driver of widespread good practice in cyber security. Without clearer guidance, there is a risk of returning to lax underwriting standards as market competition increases – an issue already evident in the post-2023 'market softening', where falling premiums have reduced incentives for businesses to maintain robust controls[124].

The following suggestion aims to progress innovation in cyber insurance to support good practice in businesses, stimulating informed demand.

Suggestion 24 – Convene innovation work on cyber insurance

DSIT and regional cyber growth leaders should convene further work with the insurance industry and SMEs to explore the future of business innovations within the cyber insurance industry.

In particular, the following points should be deliberated:

- The UK Government mandating cyber insurance to business under the following scenarios: a) all businesses; b) based on turnover threshold; c) based on most relevant sectors; d) based on the impact across supply chains.
- Incentivising the uptake of cyber insurance across SMEs, especially under a 'mandated insurance scenario' e.g. free consultancy services for SMEs going through the underwriting process on cyber insurance for the first time[125].
- Providing clearer, standardised guidance on how specific security improvements can reduce premiums or improve insurability.

5.3.2. Experimenting with cyber in the intangible economy

Some participants highlighted opportunities to experiment with new business models. They contrasted the traditional emphasis on Intellectual Property, such as patents and proprietary technologies, with the growing open-source approaches to cyber security[126]. This discussion connects to broader ideas about the intangible economy, where value is increasingly driven by non-physical assets such as knowledge, data, relationships, and reputation. Cyber security is not only a key part of this economy, it also plays a critical role in protecting these intangible assets, making it foundational to the UK's future prosperity and resilience[127].

[120]Woods and Moore (2020) Does Insurance Have a Future in Governing Cybersecurity?
[121]Reinsurance news (2024) Coalition reveals new integrations with Microsoft365, Google workspace, Amazon Web Services
[122]The NCSC (2021) Annual Review 2021
[123]Mott et al (2023) Between a rock and a hard(ening) place: Cyber insurance in the ransomware era
[124]Farley (2025) 2025 Cyber Insurance Market Conditions Outlook
[125]Lemnitzer (2021) Why cybersecurity insurance should be regulated and compulsory

[126]Red Hat is an American company developing open source software (meaning anyone can download, use, and modify it). Their business model relies on 1) subscriptions for support, maintenance, updates, and security patches; 2) Consulting and training services; 3) Certified hardware and software ecosystem compatibility. In practice, this effectively 'open core' model means the source code is freely available, but paying customers get access to tested, stable, and secure versions plus expert support. Red Hat actively contributes to upstream open-source projects, fostering a collaborative ecosystem and driving innovation. Source: Wiki
[127]Haskel and Westlake (2018) Capitalism without Capital: The Rise of the Intangible Economy

6. Strategy alignment

This section builds on the preceding analysis by focusing on the alignment of the Cyber Growth Action Plan with the existing and forthcoming strategic frameworks. As cyber security is increasingly recognised as a 'frontier technology'[128], it holds significant potential for growth across regions and sectors. It is apparent there is a lot to align to, and it is important that the emphasis on cyber growth and resilience is not diluted across these multiple concerns. One participant noted, 'cyber is one of the preeminent sources of risk to the economic security of the country – it deserves to receive far more attention and funding'.

Three cross-cutting challenges to achieving strategic coherence are discussed. First, there is a need for greater compatibility between standards, recognising the audit fatigue organisations experience when navigating a fragmented regulatory landscape. The participants described the craft of good cyber policy design as being risk-based (rather than a 'tick box exercise'), consolidating numerous directives, including sufficiently high penalties, and being easily enforced in practice.

The second challenge lies in managing the tension between global collaboration and national sovereignty. Shifting geopolitical uncertainties have sharpened this dilemma[129]. The UK Government's National Security Strategy recognises increased exposure to economic shocks and rapid technological change, calling for 'the whole of society; to adopt stronger cyber practices in the name of national resilience'[130]. Yet several participants reported uncertainty around how the UK should position itself internationally, particularly regarding trade partnerships and political alliances. While new priorities around sovereignty are emerging, their implementation requires coordinated engagement with internationally oriented departments and sectors to ensure export markets and scaleup potential are not compromised.

The third challenge underscores the role of the NCSC in supporting both cyber resilience and growth. The NCSC has delivered a range of high-impact outputs, including the Cyber Assessment Framework[131], market incentives analysis[132], and post-quantum cryptography migration guidance[133], among many others. These contributions form the foundation of the UK's cyber capability and should be more fully resourced and recognised. As highlighted throughout this report, growth in the cyber sector should be explicitly linked to the UK's wider resilience goals and aligns with the recommendation to expand the NCSC's mandate and capacity.

The remainder of the section will identify opportunities for alignment between this report and several key policy developments.

[128]DBT (2025) The UK's Modern Industrial Strategy and Cabinet Office (2025) UK Government Resilience Action Plan
[129]Ministry of Defence (2025) Strategic Defence Review
[130]Cabinet Office (2025) National Security Strategy 2025: Security for theBritish People in a Dangerous World
[131]NCSC (2024) Cyber Assessment Framework
[132]NCSC (2024) NCSC Annual Review 2024
[133]NCSC (2025) Timelines for migration to post-quantum cryptography

6.1. Relevant policy areas

The summary of the section can be found in the table below.

Strategy / Policy Document	Opportunities for Alignment
Industrial Strategy (2025)	**Supply and demand:** Cyber is called out as a priority area for growth; Use of procurement to strengthen domestic security market; Expansion of Cyber Essentials **Places:** Policies for local growth plans and use of British Business Bank and Local Innovation Partnerships Fund as champions of regional growth
AI Opportunities Action Plan – Government Response (2025)	**Supply and demand:** Stimulating the growth of domestic and secure AI industry **Futures:** Prioritising security challenges in AI research utilising supercomputer facilities
Networks and Information Systems Security Regulations (2018)	**Supply and demand:** Balancing between mandating prescribed standards and outcomes-oriented frameworks; regular communications of Cyber Assessment Framework updates to operators
Cyber Security and Resilience Bill (forthcoming)	**Supply and demand:** Strengthening the security of supply chains in critical sectors
Data Use and Access Bill (2025)	**Culture:** Engaging civil society on the role cyber plays for the UK so that their needs are factored in the development of secure data sharing environments
Online Safety Act (2023)	**Culture:** Shifting the narrative about cyber security as civic infrastructure, empowering 'the whole of society' to contribute to resilience and growth
Strategic Defence Review (2025)	**Futures:** Integrating cyber and electromagnetic domain in defence to better anticipate future threats **Supply and demand:** Innovating procurement to engage a wider set of prospective vendors **Places:** Treating data as crucial assets with assured flows and information sharing between trusted stakeholders
The Computer Misuse Act (1990)	**Culture:** Encouraging the cyber community to define permissible offensive security practices under the Pall Mall Needs process and future CMA update
Product Security and Telecommunications Infrastructure Act (2024)	**Supply and demand:** Raising standards of 'security by design' among product vendors to harmonise with the EU and facilitate export markets

6.1.1. Modern Industrial Strategy 2025

The recommendations of this report should be anchored in the Industrial Strategy through several means:

- The recommendation on stimulating informed demand and the specific suggestion on Cyber Essentials will fit into the Industrial Strategy mandate of 'expanding our Cyber Essentials accreditation scheme across the UK'[134].
- The suggestions on improving pre-procurement and procurement for cyber align well with the ambition of 'leveraging the government's purchasing power through public procurement to bolster domestic competitiveness, making the economy stronger and more resilient, and providing a solid foundation of security for UK businesses'[135]
- The recommendation to support growth journeys aligns with the announcement of the revamped Office for Investment which 'now has greater backing to ensure that the most strategically important investors in the IS-8[136] receive the strongest possible support'[137]
- Finally, the message in recommendations and suggestions on using places could be delivered building on the announcement of 'The British Business Bank introducing a new Cluster Champions programme in 10 places'[138] as well as 'Local Innovation Partnerships Fund growing high-potential innovation ecosystems'[139].

6.1.2. Government response to the AI Opportunities Action Plan 2025

In recognition of both AI and cyber being classed as 'frontier technologies' by the UK Government[140], the suggestion on cyber safe AI highlights the need to find areas of overlap rather than competition between these technologies. This pertains to skills, infrastructure investment and broader 'attention economy'[141] related to technological innovations. Two interconnected opportunities emerge: first, for AI innovators to create use cases that address security needs; second, for security and privacy researchers to enhance the trust and assurance of AI models. The ongoing work on implementing AI Opportunities Action Plan is relevant to cyber security in the following ways:

- The statement from the AI report that 'we will responsibly, securely and ethically unlock the value of public sector data assets to support AI research and innovation through the creation of the National Data Library and the government's wider data access policy'[142] ought to include the wider civil society as a critical stakeholder in negotiating the trade-offs between privacy, resilience, and harms as per the recommendation on fostering public participation in cyber skills and growth.
- The AI report's recommendation to 'mitigate the sustainability and security risks of AI infrastructure, while positioning the UK to take advantage of opportunities to provide solutions'[143] could be concentrated in specific regions with existing expertise in the security of AI systems as per the place-based recommendations. Likewise, researchers developing AI tools for security use cases could be considered for enhanced access to supercomputing facilities.

6.1.3. Networks and Information Systems Security Regulations (2018)

Across several interviews, participants agreed that the NIS regulations had a significant impact in driving increased investment into cyber security of critical infrastructures. However, many operators highlighted an ongoing challenge. While the main reporting document, the 'Cyber Assessment Framework' was intended as an outcomes-based assessment, on occasions, it has been used as a checklist due to limited in-house expertise. This reflects wider findings: although checklists are often criticised for driving down the quality of cyber assessments, outcomes-based regulations cannot be fully realised until the whole sector has access to appropriate expertise to assess more sophisticated frameworks[144].

NIS Regulations have brought attention to the risks associated with legacy systems and migration to newer infrastructures. Several participants shared security dilemmas relevant to cloud migration. While this shift can enable modern practices such as Zero Trust Architecture, it also increases the attack surface and shifts critical expertise away from local operators. Further questions arose regarding the UK's reliance on the international cloud providers in terms of critical infrastructures resilience and possible vendor lock in[145].

Looking ahead, participants saw an opportunity to reduce audit fatigue and engage operators in a timely manner as new versions of the Cyber Assessment Framework are being developed. This will enable security teams to better anticipate their budgets and strengthen their case for strategic investment at board level.

6.1.4. Cyber Security and Resilience Bill (forthcoming)

The forthcoming Cyber Security and Resilience Bill will build on the NIS Regulations, by bringing new sectors into the scope of mandated cyber security improvements. In particular, Managed Service Providers and so-called 'Critical Suppliers' to the current NIS-compliant infrastructure operators will be expected to raise the baseline of their current security standards. While the exact designation of 'Critical Suppliers' and the legal duties will be a subject to consultation, the Bill is expected to bring the UK into closer alignment with the EU NIS2 Directive, streamlining exports of UK businesses to the EU markets[146]. There is an opportunity to anchor the suggestions on Cyber Essentials and supply chain security standards into the upcoming consultation on the Bill.

[134] p. 45 of the Modern Industrial Strategy 2025
[135] p. 69 of the Modern Industrial Strategy 2025
[136] Growth driving sectors according to the 2025 Industrial Strategy. These are: Advanced Manufacturing, Clean Energy Industries, Creative Industries, Defence, Digital and Technologies, Financial Services, Life Sciences, Professional and Business Services DBT (2025) Industrial Strategy Sector Definitions List
[137] p. 153 of the Modern Industrial Strategy 2025
[138] p. 98 of the Modern Industrial Strategy 2025
[139] p. 100 of the Modern Industrial Strategy 2025
[140] UK Government (2025) Digital and technologies sector plan
[141] Pedersen et al (2021) The Political Economy of Attention
[142] p.6 of DSIT (2025) AI Opportunities Action Plan Government Response
[143] recommendation 5; DSIT (2025) AI Opportunities Action Plan Government Response
[144] Michalec (2023) What's next for the NIS Regulations? Findings from the RITICS Fellowship
[145] Michels et al (2025) Storm Clouds are Building: Surveillance, Sovereignty, and State Interests

6.1.5. Data Use and Access Act (2025)

The Data Use and Access Act (2025) will introduce further provisions for the National Data Library, which aims to improve the availability of 'high value public data sets' through the provision of secure data sharing environments[147]. While its architecture is still under discussion, the new data sharing regime is expected to account for a variety of end-users (e.g. consumers, researchers, commercial, civil servants), include security and privacy provisions and offer a varied market incentive structure to respond to the needs of different users[148].

Data sharing and interoperability are complex challenges. They require coordination of stakeholder interests, ongoing trust building and sustainable investment. If the work on the Data Use and Access Act is framed as predominantly technical, there is a risk that decisions about privacy, security, and access are locked in before the public has a chance to debate the trade-offs. As the UK Government already recognises that 'there is low engagement and a lack of trust amongst consumers to utilise their own data in many sectors'[149]. The Act presents an opportunity to leverage **Recommendation 3** to foster public participation in cyber skills and growth. Ultimately, the members of the public are critical consumers and users of IT and their diverse needs ought to be properly accounted for when growing the cyber security industry.

6.1.6. Online Safety Act (2023)

The Online Safety Act is a recent law placing duties on tech businesses to reduce illegal and harmful content. The Act is broad in scope, including provisions for age assurance, online marketplace fraud and misinformation, among other measures. Similarly to the Data Use and Access Act, the Online Safety Act sparked a debate on the tensions between security, privacy and civil liberties[150]. Participants noted that the core issues went beyond privacy and free expression – they also posed a strategic challenge for cyber growth, identifying two issues: 1) weakening encryption may harm the competitiveness of UK-based tech businesses that rely on privacy-preserving design; 2) a lack of public trust in digital technologies could undermine adoption and innovation.

Looking ahead, future digital policy must move beyond polarising debates framed as a choice between absolute security and absolute privacy. A report from The Royal United Services Institute argues that 'a more nuanced debate must continue which actively moves away from zero-sum views of absolute privacy versus absolute security and focuses more on how the risks to public safety can be reduced in proportion with the need to protect citizens' rights and freedoms'[151]. One way to advance that debate, according to one of the participants, is 'building relationships between tech industry, civil service and civil society early on policy development. If consultations come too late, they lead to confrontations rather than collaboration'. This more constructive approach recognises cyber security as a form of civic infrastructure. Achieving this vision will require building a public culture of cyber security, where resilience and growth are co-produced across society. There is growing evidence that the UK public supports the growth agenda[152]. But for this support to be sustained, cyber security must be presented as a public good: delivering secure digital services, good jobs, and improved confidence in the UK's digital future.

6.1.7. Strategic Defence Review (2025)

Across the interviews and evidence review, there was acknowledgement of the changing nature of cyber conflicts, with an intensification of serious threats[153] and an increasingly hybrid nature of military activities. The domains of cyber security and electromagnetic spectrum are converging (e.g. drones can operate on radio frequencies as well as Wi-Fi). However, the operations and funding have historically been siloed. Going forward, there are several tensions regarding future governance and business models of defence cyber contractors and civilian-oriented businesses. While defence organisations utilise enhanced clearances, bespoke tools and offensive cyber capabilities, civilian organisations typically rely on commercial threat intelligence feeds and standardised security products. When increasing public spending on military technologies, it is important that cyber growth does not overlook civilian innovation.

The Strategic Defence Review (SDR) recommended several interventions relevant to the military side of the cyber security sector:

- Participants' input aligns with the SDR's recommendation to create an 'integrated CyberEM Command'[154], unifying the UK's cyber, electromagnetic and information operations under a single structure;
- The recommendations in this report on procurement is supported by the SDR's commitment to 'maximise internal and industrial expertise, accelerate acquisition processes, manage risk and cost, and engage a wider set of suppliers'[155] but it should be noted that procurement reform for cyber should not be limited to the defence sector.
- The point on 'treating data as a strategic asset, with protected computing and data infrastructure, and assured data flows from allies and the UK Intelligence Community'[156] aligns with this report's recommendations to create safe environments where trusted stakeholders can explore and test solutions to critical cyber security challenges.

6.1.8. The Computer Misuse Act (1990)

The Computer Misuse Act is a legal framework criminalising unauthorised access to computer systems, hacking, and related cyber offenses. The wording of the CMA is broad, and civilian cyber security businesses must comply with the CMA, limiting their ability to engage in activities like penetration testing without explicit consent. Several participants[157] expressed that they were keenly awaiting a reform of the legislation, and highlighted that future updates should treat the CMA as a lever for growth. There is an opportunity for the cyber industry to help define ethical cyber security practices and align these with ongoing developments such as the Pall Mall process[158]. Participants called for clear legal pathways and safe learning environments for offensive security talent in order to modernise the sector and support responsible innovation. These insights align with the recommendations and suggestion regarding the role of language in cyber security practice, and the need to create place-based 'safe havens' for research and innovation.

6.1.9. Product Security and Telecommunications Infrastructure Act (2024)

The Product Security and Telecommunications Infrastructure Act (PSTI) is a new product security regime placing responsibility on vendors of IoT devices (e.g., smart TVs, smart doorbells etc) to meet baseline security requirements. This includes banning universal default and easily guessable passwords, publishing information on how to report security issues and publishing information on minimum security update periods. The PSTI Act is an example of 'security by design' and it draws from the European IoT security standard ETSI EN 303 645[159]. With that in mind, there are further opportunities to harmonise the UK legislation with the evolving EU Cyber Resilience Act[160]. This will ensure that the UK businesses exporting to the EU market are not overburdened with conflicting or unclear expectations, as per this report's suggestions on harmonising compliance requirements.

6.2. Summarising the policy landscape

This overview of key policy areas highlights the complexity of ensuring cyber security is addressed across the full range of UK interests. Given this landscape, it's unsurprising that many UK cyber businesses struggle to navigate the multitude of initiatives and opportunities. This underscores the importance of targeted support for their growth journeys as a central policy recommendation.

[146] Slaughter and May (2025) What will the Cyber Security and Resilience Bill mean for your organisation?
[147] The National Data Library (2025) Home
[148] Worth et al (2025) Developing the UK National Data Library for public benefit: 10 key reflections
[149] DSIT (2024) Data (Use and Access) Bill factsheet: growing the economy
[150] Here, the context is the UK Government's proposal to apply 'client-side scanning' as a tool helping with the identification of child sexual abuse materials on encrypted messaging services (e.g. Signal, WhatsApp). Client-side scanning refers to the practice of scanning data, like text, images, or videos, on a user's device (the 'client') before it's encrypted or after it's decrypted. Consequently, client-side scanning would undermine the confidentiality of the end-to-end encryption. An independent technical review commissioned by the Government concluded that none of the reviewed client-side scanning tools were suitable to be deployed on end-to-end encrypted communications (Peersman et al. 2025). Additional reporting raised concerns about the broader cyber security risks of embedding surveillance functions at the device level, potentially exposing users to criminal exploitation (Abelson et al, 2021). In response to mounting concerns, over 70 civil society organisations and security researchers issued an open letter criticising the OSA's impact on digital rights and calling for the protection of strong encryption. At the same time, online safety advocates and child protection organisations argued that stronger safeguards were urgently needed to address the growing prevalence of child sexual abuse materials. In the final version of the legislation, the Government added a clause requiring that proposed surveillance measures must be technically feasible
[151] Herath and Dawda (2022) Balancing End-to-End Encryption and Public Safety
[152] Ipsos (2025) New Ipsos survey shows divides between MPs and the public on priorities for economic growth
[153] National Audit Office (2025) Cyber threat to UK government is severe and advancing quickly, spending watchdog finds
[154] p. 123 of the Strategic Defence Review, 2025
[155] p. 62 of the Strategic Defence Review, 2025
[156] p. 47 of Strategic Defence Review 2025
[157] CyberUp Campaign (2025) Home
[158] FCO (2025) The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities The Pall Mall Process is an international initiative launched by the UK and France to address the proliferation and irresponsible use of commercial cyber intrusion tools and services
[159] ETSI (2020) Cyber Security for Consumer Internet of Things: Baseline Requirements
[160] Osborne Clarke (2024) UK and EU take steps to bolster product security regimes

7. Conclusion and next steps

This review has involved consultation across the UK cyber sector. It is based on perspectives from startup founders, security technologists, security service providers, security product vendors, CISOs from multiple sectors, large technology vendors, cyber research scientists and engineers, trade, accreditation and membership associations, investors, regional leaders, and various parts of government.

The conversations were focused on cyber growth which is needed to improve cyber resilience across all sectors. This will give the freedom for organisations in those sectors to take risks and advantage of data and digitalisation, which in turn will help them to grow too.

It has been a rapid review, meaning it is not comprehensive. No doubt there are more voices and ideas than there was time to accommodate, and some ideas need to be developed further. That said, there was a lot of consistency in the identification of the challenges and opportunities.

The message is clear – the cyber sector is growing and can grow much more. The report highlights that to achieve this, the stakeholders in industry and government need to:

i. push the virtuous cycle of resilience and growth by stimulating informed demand and support businesses at all stages of their growth journeys in meeting that demand;
ii. make strategic choices about where to focus on technologies and sectors; and
iii. simplify and clarify the roles of government (including the National Cyber Security Centre (NCSC)) in relation to cyber resilience and growth.

The growth plan described here includes 9 recommendations and 24 associated suggestions which outline actions for all parts of the UK cyber ecosystem including government and industry. In summary they call for:

- Curating the UK's cyber culture to drive growth and public participation in cyber skills and innovation.
- Putting leadership in the right places with industry-led national and place-based cyber growth roles.
- Building on the UK's places of cyber strength to collaborate on sensitive topics, chosen technology areas and make time to create and anticipate cyber futures.

The cyber world is moving quickly, and the UK really needs an agile but stable plan for cyber growth. This implies a mix of experimental approaches where there is a need to get started and iterate, and structural changes to set the UK up for success.

Although the UK cyber community is willing, it is fragmented with no single group able to represent the aggregated interests of cyber suppliers, different sectors, cyber professionals, government, research, and civil society. This is why this report emphasises place-based leadership and an approach underpinned by the principles to act as one team and recognise the connections between cyber growth and resilience. When integrating these principles into recommendations, the UK can be confident about delivering value for money across places and stakeholders, including large and small vendors, customers, investors, government, and civil society.

In the development of this report, it was apparent that there is a lot of goodwill. The UK cyber community is leaning in and figuring out how to do better. The timing is ripe, with the Industrial Strategy and the refresh of the National Cyber Strategy, there is a huge opportunity to help this community be even more effective.

7.1. Table of Suggestions

Suggestion 1 – Pilot programmes that allow NCSC and DSIT to qualify and connect cyber startups with government departments

Suggestion 2 – Expand the co-creation and government investment models for wider commercial participation

Suggestion 3 – Include marginalised demographics in product development

Suggestion 4 – Convene 'cyber in the public interest' events

Suggestion 5 – Use immersive methods to engage civil society

Suggestion 6 – Focus on the way cyber language is used with the public

Suggestion 7 – Incentivise organisations to create cyber career entry roles

Suggestion 8 – Double down on skills

Suggestion 9 – Review the Computer Misuse Act

Suggestion 10 – Mandate Cyber Essentials in selected supply chains

Suggestion 11 – Map standards and regulation to help navigate compliance

Suggestion 12 – Share guidance early to reduce burden

Suggestion 13 – Improve guidance on the reporting of cyber risk

Suggestion 14 – Support pre-procurement engagement for SMEs

Suggestion 15 – Accelerate the development of Principles Based Assurance

Suggestion 16 – Choose a few places for Cyber Growth Centres

Suggestion 17 – Support growth leaders with funding and structure

Suggestion 18 – Use places used to convene stakeholders on futures

Suggestion 19 – Engage with places to identify strengths to focus on

Suggestion 20 – Target a few places to create safe environments

Suggestion 21 – NCSC to support place based cyber growth leaders

Suggestion 22 – NCSC to work with place based cyber growth leaders assessing startups

Suggestion 23 – Identify commercialisation opportunities for cyber safe AI

Suggestion 24 – Convene innovation work on cyber insurance

8. Technical annex

8.1. Methodology

The research team took an agile and collaborative approach to deliver a high-quality review supporting the need for ambitious and feasible recommendations. The approach consisted of five overlapping phases, which took place between May and July 2025:

- A rapid review of available evidence supporting the growth of cyber security industry across the existing grey and academic literature (listed in Section 8.3 'References');
- Informal consultations with cyber security experts across the private sector, communities and academia to facilitate project scoping;
- Formal interviews with cyber security experts ranging from CISOs, startup founders, consultants, senior researchers, critical infrastructure operators, civil society organisations, community interest companies, cyber security investors.
- Structured and open roundtables where cyber security stakeholders were invited to comment on draft recommendations. These were held across several regions including Bristol, Manchester, Belfast and London[161], and with stakeholder groups such as Tech UK[162].
- Regular engagement with DSIT and NCSC stakeholders to better understand the needs for evidence and implementation gaps.

The research team opted for a mix of convenience and snowball sampling, recruiting participants through the existing professional networks, while remaining considerate of the need for a balance in expertise and viewpoints offered. Attendance was not tracked at all of the roundtables, so it is an estimate that the total consulted exceeded a hundred participants. 93 participants provided detailed input, many play multiple roles but for illustrative purposes each has been put into one of the categories of demand (leading or in a team responsible for security of an organisation), supply (startup, medium or large cyber vendor), support (accreditation, training, trade, civil society or membership organisations), research (academic or industrial researcher), Investor (angel investor or venture capital) and Government (cyber domain experts). The breakdown is shown in the pie chart below.

The report highlighted the low numbers of women in cyber. This was somewhat reflected in our demographics. Of the 93 participants, 20 were female, (22%).

Figure 1 - Categories of participants

The research received ethics approval from the University of Bristol. The recommendations were developed independently by the authors. While the research involved engagement with diverse stakeholders across government and industry, no external party had editorial control over the findings or conclusions. Diverging views were considered but did not determine the analysis.

All participants were given the option to either remain anonymous or to be listed as report contributors. The list of contributors can be found in the 'Acknowledgements' section of the Technical Annex.

To facilitate an open discussion, interviews were semi-structured, leaving space for reflections led by participants. Conversations covered a range of topics such as R&D, supply and demand, language, skills, societal resilience, policy, future technologies, future jobs and regional clusters.

While the research team took efforts to ensure the diversity of contributions, the report has been designed as a rapid overview of the sector, highlighting opportunities for change, existing good practice and challenges to growth. As such, the review presented is illustrative rather than comprehensive. Future studies and policy consultation activities ought to prioritise engagement with groups who are often neither buyers nor vendors of cyber security yet are critical to the goal of nation-wide cyber resilience (e.g., under resourced Local Authorities across the regions, SMEs or charities).

[161]A further roundtable was held with Scotland IS in the first week of August 2025
[162]A further session was held with the Government Cyber Advisory Board (GCAB) in the first week of August 2025

[163]DSIT (2025) Cyber Security Sectoral Analysis
[164]DSIT and Home Office (2025) Cyber security breaches survey 2025
[165]DSIT (2024) Cyber Security Skills in The UK Labour Market

8.2. Tracking cyber growth

This annex sets out a practical, pluralistic approach for tracking cyber growth in the UK, aimed at researchers in government, academia, and industry. It proposes core indicators, discusses measurement challenges, and outlines priority research directions, with clear links to the report's recommendations.

8.2.1. Selected existing datasets and indicators

The UK already monitors the following growth indicators through the publicly available data and regularly commissioned reports, such as:

- **Gross Value Added** (GVA) is a measure of the increase in the value of the economy due to the production of goods and services. It can be treated as the estimated direct contribution of the cyber security sector to the UK economy. The GVA of the UK cyber sector can be modelled through the combination of the publicly available data and modelling, like in the case of the DSIT Cyber security sectoral analysis 2025 by Perspective Economics and Ipsos[163]. The most recent estimate quotes the figure of £7.8 bn as the total GVA of the sector, a 21% increase from the previous year. This report's **Recommendation 1** (Support growth journeys) could be linked to this indicator.
- **Negative outcomes of cyber breaches and attacks** are presented as official statistics by the Department for Science, Innovation and Technology and Home Office, with the most recent report released in 2025[164]. The data is collected through surveys and interviews, and it shows that 43% of businesses and 30% of charities reported having experienced any kind of cyber security breach or attack in the last 12 months (with 85% reporting phishing as the most prevalent type). In that pool, 16% of businesses and charities experienced a negative outcome. The average self-reported cost of the most disruptive breach or attack among businesses in the last 12 months was £1,600 including those giving a £0 response (and £3,550 excluding £0 responses). For charities in the last 12 months, it was £3,240 including £0 responses (and £8,690 excluding £0 responses). As the data is self-reported and highly variable, it should be interpreted cautiously and triangulated with other indicators (e.g. trust, operational delays, reputation). This report's **Recommendation 2** (Stimulate informed demand) could be linked to the indicators above.
- **The number of students enrolled on cyber security courses** is a measure tracked by the DSIT Cyber security skills in the UK labour market report.[165] Data from the 2024 report quote 20,890 students enrolled in cyber security courses in Higher Education Institutions, a 14% increase from the previous year. Within that, 89% of undergraduate and 38% of postgraduate students are classed as domicile (UK-based). The figures do not cover vocational training or Continuous Professional Development. This report's **Recommendation 3** (Foster public participation in cyber skills and growth) could be linked to this indicator.
- **The number of employees within the cyber security sector** (full time equivalents) is a measure regularly tracked by the DSIT Cyber Security Sectoral analysis, amounting to 67,299 reported in 2025 (an increase of 11% from the previous year). Further detailed estimates are available for places, firm sizes, demographic diversity, seniority, expertise types through the DSIT Cyber security skills in the UK labour market report[166]. This figure doesn't take into account in-house cyber security professionals working in other firms (e.g., retail, manufacturing etc). This report's **Recommendation 3** (Foster public participation in cyber skills and growth) could be linked to this indicator.
- **Recruitment and staff retention** is a set of signals tracked by DSIT Cyber security skills in the UK labour market report published in 2025. Trends like the number of job postings, top job titles advertised, experience and education requirement are used to understand the demand for cyber security professionals as well as the sustainability of career pipelines in the sector. The main findings state that that despite 49% businesses estimated to have skills gaps in technical areas and an increase in cyber security graduates by 20%, the number of cyber job postings decreased by 33% between 2023 and 2024. This has been attributed to the wider challenging economic and political factors as well as job cuts in the technology sector. In the environment of competing narratives such as 'global shortage of cyber security professionals'[167] vs 'reluctance to hiring and providing in-house training'[168], it is vital to seek further evidence to be able to validate such claims. This report's **Recommendation 3** (Foster public participation in cyber skills and growth) could be linked to this indicator.

[166]DSIT (2024) Cyber Security Skills in The UK Labour Market
[167]World Economic Forum Centre for Cybersecurity (2025) Bridging the Cyber Skills Gap - Why is there a cybersecurity talent shortage?
[168]Chickowski (2024) Cybersecurity's Workforce Woes Are a Myth: 5 Ways to Rethink Recruiting

- **Cyber security exports** are presented as official statistics by the Department of Business and Trade and UK Defence and Security Exports[169], with the data covering the period from 2013-2023. Revenues from cyber and physical security are valued at £7.2 billion for 2023, an increase by 18% in nominal prices from 2022. Within that, the main destinations are Europe (£3.8 billion) and North America (£1.8 billion). This report's **Recommendation 4** (Appoint a UK cyber growth leader) could be linked to this figure.

- **The number of businesses in the UK supplying cyber products or services** is a measure regularly tracked by the DSIT Cyber Security Sectoral analysis. Due to the lack of a cyber-specific Standard Industrial Classification code, the figure is an estimate based on datasets from a mix of proprietary industry databases (e.g., Beauhurst) and public databases (e.g., Companies House). The most recent report published in 2025 estimates there are 2,165 firms active in the UK, with more granular data available for firm size, products/services provided and place-based distribution. This report's **Recommendation 4** (Appoint and UK Cyber growth leader) and **Recommendation 5** (Appoint growth leaders in places of cyber strength) could be linked to these metrics.

- **The size and scale of the market at the intersection of AI and cyber security** is a new area of analysis commissioned by DSIT in the AI and software cyber security market analysis 2025 report[170]. It explores the levels of investment, location, and types of products and services offered. This report's **Recommendation 8** (Places to nurture distinct tech areas) could be linked to these datasets.

8.2.2. Challenges to measurement

- **Lack of sectoral classification.** The UK cyber security businesses don't have their own Standard Industrial Classification code which would help to distinguish the sector's contribution from wider IT businesses. This creates uncertainty around the sector's true scale and trajectory.

- **Shifting sectoral boundaries.** What "counts" as cyber security is contested and evolving. While traditional definitions emphasise technical protections against breaches, many researchers and practitioners argue for including privacy, mis/disinformation, and even physical safety in the sector's remit[171,172,173]. These conceptual debates affect comparability across studies and over time.

- **Valuing avoided losses.** Much of the benefit of cyber capacity accrues in the form of risks averted - financial, reputational, or operational. Yet modelling avoided losses at national scale is inherently difficult: incidents are unevenly distributed, their severity fluctuates, and firms under-report sensitive impacts. This creates wide error margins in aggregate estimates[174].

- **Limits of growth metrics.** Traditional measures of economic growth such as Gross Domestic Product (GDP) or GVA capture commercial expansion but not whether cyber growth strengthens resilience, trust, or wellbeing. A cyber sector that expands in value but delivers poor-quality products or erodes public confidence could register as 'growth' in official data while undermining national capacity[175,176,177].

A pluralistic approach to measuring cyber growth acknowledges its complexity, while articulating the value of the sector across several parts of the government responsible for cyber policy (DSIT, Home Office, HMRC, NCSC, DBT etc). It will help the government with de-risking policy choices, identifying most promising areas of growth and improving public support and trust in public technology rollouts.

[169] DSIT and DBT (2023) UK Security Export Statistics
[170] DSIT (2025) AI and Software Cyber Security Market Analysis
[171] Caramancion et al (2022) The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats
[172] RITICS (2023) Resolving Anti-patterns in Industrial Control System / Operational Technology Environments
[173] REPHRAIN (2022) Response to DCMS Consultation: Security and Privacy in Apps and App Stores
[174] Shevchenko et al (2023) The Nature of Losses From Cyber-Related Events: Risk Categories and Business Sectors
[175] Bennett School of Public Policy (2022) Beyond GDP
[176] Office for National Statistics (2022) Inclusive measures of growth – How ONS is moving Beyond GDP

8.2.3. Future research directions

Further analysis ought to establish a robust evidence base linking the case for cyber growth with cyber resilience, while drawing on a mix of qualitative, quantitative and longitudinal data. In each case, further research requires attention to the sociotechnical context in which the cyber security market develops. In particular, the following areas require the development of enhanced frameworks for an improved understanding and monitoring of cyber growth:

- **Examining startup success over time** could involve identifying cyber-focused startups and monitoring their survival, scaling, and exit rates over time. Beyond quantitative metrics, qualitative analysis of startup growth narratives and developments of novel security design patterns can reveal common factors in success. To consistently select relevant startups, four categories could be used: cyber skills development initiatives, firms assisting with the adoption of standards like Cyber Essentials, products and services relevant to critical national infrastructure and innovative security-by-design technologies. It is important to note, however, that success is multi-dimensional; not all thriving startups appear in standard metrics, and qualitative case studies are essential to complement quantitative tracking. This approach aligns with **Recommendation 1** (Support growth journeys).

- **Cyber insurance data** could serve as a proxy for evaluating the effectiveness of cyber security standards. By tracking uptake of cyber insurance and analysing claims data, it is possible to assess whether schemes like Cyber Essentials reduce risk exposure and financial losses. This report's **Recommendation 2** (Stimulate informed demand) could be advanced with further exploratory work on the role of cyber insurance.

- **Product quality** could be monitored through a comprehensive evaluation of the Principles-Based Assurance (PBA). The programme could incorporate recommendations from earlier research on the PBA conducted by RISCS[178], such as maintaining proactive communication, conducting usability testing, or examining links to procurement decisions. In order to grasp the extent of change in quality over time, it is vital to conduct a study establishing the baseline, through quantitative and qualitative description of the current UK cyber security market, including a critical account of the 'market for lemons' problem[179] and the prevalence of 'snake oil' solutions[180]. It should be noted that quality assurance is a lagging indicator, and widespread adoption could take years. This report's **Recommendation 2** (Stimulate informed demand) could be advanced with this research.

- **Public engagement in cyber security** is a crucial dimension to monitor as it's linked to public spending on digital infrastructure rollouts (e.g. future consent solutions for sharing of patient or energy consumption data). Existing surveys typically track public acceptance of technologies, e.g. attitudes to age verification[181] or processing personal data for national security[182]. However, future metrics should aspire to go beyond the model of 'public deficit' and avoid assuming that a lack of public trust in technology and institutions is a matter of low awareness or irrationality[183]. Rather, it is important to frame public trust and engagement as relational and context-specific, shaped by past experiences, accountability and transparency. This aligns with **Recommendation 3** (Foster public participation in cyber skills and growth).

- **Place-based economic trajectories** could offer another lens for assessing cyber growth. Despite several indicators being already measured at place-based level, current datasets come with limitations due to administrative boundary issues which don't always reflect how cyber security communities see themselves. For that reason, a case study approach could better illuminate the dynamics of growth and innovation, informing **Recommendations 5, 7, and 9** (Appoint growth leaders in places of cyber strength, Develop futures-oriented communities, Places to provide safe environments).

- Finally, **the growth of other sectors enabled by cyber security improvements** is an important outcome to capture. Enhancements in operational efficiency, consumer trust, and uptake of digital services can signal positive spillover effects from cyber as an enabling sector. Measuring these effects requires triangulating several sources of data, e.g., firm-level surveys, sectoral productivity analyses, and macroeconomic indicators. Further research could develop an analytical framework focusing on a limited number of diverse indicators that are feasible to track over time. It is important to note that attribution of causality is challenging due to confounding factors such as regulatory changes or the broader political and economic landscape. This supports **Recommendation 6** (Expand the NCSC role) by demonstrating how cyber investments drive broader economic impact.

[177] Dutton et al (2019) Cybersecurity Capacity: Does It Matter?
[178] Spencer (2023) Assurance by Principle: Preparing for the Next Generation of Product Security Assurance
[179] Anderson and Moore (2006) The Economics of Information Security
[180] Schneier (1999) Crypto-Gram
[181] Ipsos (2025) Britons back Online Safety Act's age checks, but are sceptical of effectiveness and unwilling to share ID
[182] Powell et al (2025) UK Public Attitudes to National Security Data Processing: Assessing Human and Machine Intrusion
[183] Klimburg-Witjes and Wentland (2021) Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses

8.3. Acknowledgements

The authors of this report would like to express their gratitude to the research participants for sharing their invaluable expertise throughout the project, these included:

Eddie Alleyn, Simon Arnell, Debi Ashenden, Ian Bailey, James Baker, Boris Balacheff, Ian Barton, Nick Benson, Robin Bloomfield, Joyann Boyce, Paul Briault, Jill Broom, Fraser Buchan, Pete Burnap, Paul Ceely, Joseph Chambers, Tommy Charles, Deepinder Chhabra, Simon Cook, Pete Cooper, Campbell Cowie, Barney Craggs, Niall Cronin, Richard Crowther, David Crozier, John Cruise, Peter Davies, Martin Dehnel-Wild, Victor Djondo, Zaina Dkaidek, Sam Donaldson, David Edmunds, Tarquin Folliss, Nathalie Goodsir, Bruce Gregory, Ali El Kaafarani, Andrzej Kawalec, Mark Evans, Katie Gallagher, Matt Griffith, Rycharde Hawkes, Chad Heitzenrater, Simon Hodgkinson, Paul Hopkins, Saj Huq, Sian John, Verona Johnstone-Hulse, Rob Kearney, Paul Lee, Phil Legg, Phil Litherland, Genevieve Liveley, Ben Lyons, Lucy Mason, Ross McKerchar, Sanjana Mehta, Simon Minton, Stuart Murdoch, Maire O'Neill, Izak Oosthuizen, David Palmer, Neil Passingham, Alastair Paterson, Danielle Philips, Emma Philpott, Ian Pratt, Daniel Prince, Awais Rashid, Elspeth Robertson, Jenny Seaborne, Aurorah Smith, Steve Smith, Dagmar Steffens, Nick Sturge, Dafydd Stuttard, Nicola Taylor, Anthea Terry, Colin Topping, Martina Trucco, Alex Van Someren, Cevn Vibert, Stephen Wales, Tim Watson, Thomas Willson, Martin Whitworth, Daniel Woods, Richard Wright, Richard Yorke

The authors would also like to acknowledge the support from roundtable hosts from HP, NCC, Tech UK, Scotland IS, The Northern Ireland National Cyber Strategy Development Engagement Forum, and Plexal who provided their facilities and convened groups of expert stakeholders to discuss recommendations.

Many individuals from DSIT, the NCSC and other government departments gave significant time and guidance, made many introductions, and created a lot of visibility and opportunity for the project to have impact.

The helpful suggestions and support provided by Rupert Shute and Nigel Steward were greatly appreciated throughout the project.

The project has been generously supported by the Gatsby Foundation and the Centre for Economic Performance (Imperial College London).

8.4. References

1. Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Callas, J., Diffie, W., Landau, S., Neumann, P.G., Rivest, R.L. and Schiller, J.I. (2024) Bugs in our pockets: the risks of client-side scanning. Journal of Cybersecurity, 10(1), https://arxiv.org/abs/2110.07450

2. Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S. and Abeler, J., (2020) Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. JMIR mHealth and uHealth, 8(8) https://mhealth.jmir.org/2020/8/e19857

3. Anderson, R., & Moore, T. (2006). The economics of information security. science, 314(5799), 610-613. https://www.cl.cam.ac.uk/archive/rja14/Papers/sciecon2.pdf

4. Anderson, R. and Moore, T., (2009) Information security: where computer science, economics and psychology meet. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 367(1898), https://doi.org/10.1098/rsta.2009.0027

5. Arroyabe, M.F., Arranz, C.F., De Arroyabe, I.F. and de Arroyabe, J.C.F., (2024) Exploring the economic role of cybersecurity in SMEs: A case study of the UK. Technology in Society, 78, https://doi.org/10.1016/j.techsoc.2024.102670

6. Azets UK (2025) Research on the prevalence and quality of cyber disclosures. Report commissioned by DSIT and Clark, F. MP https://assets.publishing.service.gov.uk/media/67c8494bae2aa47d2f5ae2fe/Cyber_disclosures_report.pdf

7. Badva, P., Chowdhury, P.D., Ramokapane, K.M., Craggs, B. and Rashid, A., (2024) Assessing Effectiveness of Cyber Essentials Technical Controls. arXiv preprint https://arxiv.org/abs/2406.15210

8. The Behavioural Insights Team and Alanah& Madeline Foundation (2022) Digital Compass https://www.bi.team/wp-content/uploads/2022/02/Digital-Compass-Brochure_inc-trial-results-final.pdf

9. Bennett School of Public Policy (2022) Beyond GDP. Blog Post https://www.bennettschool.cam.ac.uk/blog/beyond-gdp-impact/

10. British Business Bank (2025) National Security Strategic Investment Fund https://www.british-business-bank.co.uk/finance-options/equity-finance/national-security-strategic-investment-fund

11. Burton, J., Janjeva, A, Mosley, S and Alice (2025) AI and Serious Online Crime, Center for Emerging Technology and Security Research Reports. Alan Turing Institute https://cetas.turing.ac.uk/publications/ai-and-serious-online-crime

12. Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats. Data, 7(4), 49. https://www.mdpi.com/2306-5729/7/4/49

13. Chickowski, E. (2024) Cybersecurity's Workforce Woes Are a Myth: 5 Ways to Rethink Recruiting. Reversing Labs. Blog post https://www.reversinglabs.com/blog/cybersecuritys-workforce-talent-gap-woes-myth-or-reality

14. Chuenjitwongsa, S. (2017) How to conduct a Delphi study. Cardiff University https://www.cardiff.ac.uk/__data/assets/pdf_file/0010/1164961/how_to_conduct_a_delphistudy.pdf

15. CISA – Cybersecurity and Infrastructure Security Agency (2025) Product Security Bad Practices Version 2. Joint Guide https://www.cisa.gov/resources-tools/resources/product-security-bad-practices#:~:text=Development%20in%20Memory%20Unsafe%20Languages

16. Cabinet Office (2025) National Security Strategy 2025: Security for the British People in a Dangerous World. Policy Paper https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html

17. Cabinet Office (2025) UK Government Resilience Action Plan. Policy paper. https://www.gov.uk/government/publications/uk-government-resilience-action-plan

18. Campbell-Jack, D., Bickley, H., Lillis, J. (2021) CyberFirst Evaluation. Report. Comission by SANS for DCMS (Department for Digital, Culture, Media and Sport) and NCSC (National Cyber Security Centre) https://assets.publishing.service.gov.uk/media/610c0380e90e0706cae5b81e/CyberFirst_report_ACCESSIBLE.pdf

19. Collier, B & Clayton, R 2025 'Not just BANAL: How branding shapes cybercrime ecosystems'. The 24th Workshop on the Economics of Information Security. https://www.pure.ed.ac.uk/ws/portalfiles/portal/518169227/WEIS2025_paper_21-2.pdf

20. CRANE - Cyber Security Research Network (2025) Home https://crane.ac.uk/

21. Crown Commercial Service (2024) SME and VCSE Action Plans. Policy paper https://www.gov.uk/government/publications/crown-commercial-service-sme-and-vcse-action-plans

22. Cyber and Fraud Centre Scotland (2022) Scottish Business Resilience Centre to extend 'Exercise in a Box' programme for third year https://cyberfraudcentre.com/sbrc-to-extend-exercise-in-a-box-programme-for-third-year

23. CyberUp Campaign (2025) Campaign responds to withdrawal of amendment to update Computer Misuse Act. News. https://www.cyberupcampaign.com/news/campaign-responds-to-withdrawal-of-amendment-to-update-computer-misuse-act

24. CyLon Ventures (2025) Home https://www.cylonventures.com/

25. DBT - Department for Business and Trade (2023) UK security export statistics 2023. https://www.gov.uk/government/statistics/uk-security-export-statistics-2023/uk-security-export-statistics-2023#estimated-rest-of-world-security-exports

26. DBT- Department for Business and Trade (2025) Cyber security https://www.business.gov.uk/invest-in-uk/investment/sectors/cyber-security/

27. DBT - Department for Business and Trade (2025) Industrial Strategy Sector Definitions List https://www.gov.uk/government/publications/industrial-strategy/industrial-strategy-sector-definitions-list

28. DBT - Department for Business and Trade (2025) The UK's Modern Industrial Strategy https://www.gov.uk/government/collections/the-uks-modern-industrial-strategy-2025

29. Debate Security (2020) Cybersecurity Technology Efficacy: Is cybersecurity the new market for lemons? Research Report https://www.debatesecurity.com/cybersecurity-technology-efficacy-is-cybersecurity-the-new-market-for-lemons/

30. Discribe Hub (2025) Digital security by design: opportunities, adoption, developer readiness, regulation and attitudes. Summary Report. https://static1.squarespace.com/static/5f8ebbc01b92bb238509b354/t/67e673b85d427f3ad23ee7a9/1743156154318/Summary_Report_Discribe.pdf

31. Dkaidek, Z. (2025) Contextual Dynamics in Cybersecurity Investment Decision-Making. PhD Project. Paper available upon request https://www.bristol.ac.uk/cdt/cyber-security/tipscdtstudents/stu-profiles/studentprofilezd/

32. DSIT – Department for Science, Innovation and Technology (2023) Evaluation of the Cyber Runway programme https://www.gov.uk/government/publications/evaluation-of-the-cyber-runway-programme/evaluation-of-the-cyber-runway-programme#conclusions-and-recommendations

33. DSIT - Department for Science, Innovation and Technology (2024) Data (Use and Access) Bill factsheet: growing the economy. Guidance https://www.gov.uk/government/publications/data-use-and-access-bill-factsheets/data-use-and-access-bill-factsheet-growing-the-economy

34. DSIT - Department for Science, Innovation and Technology (2025) AI Opportunities Action Plan Government Response. Policy paper https://www.gov.uk/government/publications/ai-opportunities-action-plan-government-response/ai-opportunities-action-plan-government-response

35. DSIT- Department for Science, Innovation and Technology (2025) Mapping cyber governance code to NCSC Cyber Assessment Framework https://www.gov.uk/government/publications/cyber-governance-mapping/mapping-cyber-governance-code-to-ncsc-cyber-assessment-framework

36. DSIT and DCMS (2018) Mapping of IoT security recommendations, guidance and standards https://www.gov.uk/government/publications/mapping-of-iot-security-recommendations-guidance-and-standards DSIT (Department for Science, Innovation and Technology) and DCMS (2018) Mapping of IoT security recommendations, guidance and standards https://www.gov.uk/government/publications/mapping-of-iot-security-recommendations-guidance-and-standards

37. DSIT (Department for Science, Innovation and Technology) and Camrose, V. (2024) The UK Product Security and Telecommunications Infrastructure (Product Security) regime. Policy Paper. https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

38. Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity capacity: does it matter?. Journal of Information Policy, 9, 280-306. https://doi.org/10.5325/jinfopoli.9.2019.0280

39. Dwyer, A. (2015) Academic Cyber Security Research: Best Practice for Commercialisation. Report https://ora.ox.ac.uk/objects/uuid:15a54083-77f3-4ceb-bbde-c48a49dedbb8

40. Education Policy Institute (2020) An international comparison of technical education funding systems: What can England learn from successful countries? Report https://epi.org.uk/wp-content/uploads/2020/03/EPI-Tech_ed_funding_2020.pdf

41. ETSI - European Telecommunications Standards Institute (2020) Cyber Security for Consumer Internet of Things: Baseline Requirements https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

42. Farley, J. (2025) 2025 Cyber Insurance Market Conditions Outlook. Gallagher report. https://www.ajg.com/-/media/files/gallagher/us/news-and-insights/2025/2025-cyber-insurance-market-conditions-outlook.pdf

43. FCO – Foreign, Commonwealth and Development Office (2025) The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

44. Federation of Small Businesses (2024) UK entrepreneurs should learn how to 'fail well' like their US counterparts, says Karen Mills, former Barack Obama Cabinet member. Press Release. https://www.fsb.org.uk/media-centre/press-release/uk-entrepreneurs-should-learn-how-to-fail-well-like-their-us-counterparts-says-k-MCGOEZGDUT3NFDLIPR6PWZIIB2JU#:~:text=Karen %20Mills%20says:%20%E2%80%9CThe%20American,start%2Dups%20in%20the%20UK.

45. Government of Canada (2023) Innovative Solutions Canada: Annual Report 2022–23 https://ised-isde.canada.ca/site/innovative-solutions-canada/en/innovative-solutions-canada-annual-report-2022-23

46. Government Office for Science (2024) The Futures Toolkit https://www.gov.uk/government/publications/futures-toolkit-for-policy-makers-and-analysts/the-futures-toolkit-html

47. Government Office for Science (2024) Three Horizons: facilitation worksheet https://www.gov.uk/government/publications/three-horizons-facilitation-worksheet/three-horizons-facilitation-worksheet

48. Haskel, J. and Westlake, S. (2018) Capitalism without Capital: The Rise of the Intangible Economy. Princeton University Press https://press.princeton.edu/books/hardcover/9780691175034/capitalism-without-capital?srsltid=AfmBOopju5YIlnd4SZdHOiSEGdMl12KQPBNRu68JBgDO3wso6zwhylK4

49. Herath C. and Dawda S. (2022) Balancing End-to-End Encryption and Public Safety. Royal United Services Institute for Defence and Security Studies. Occasional Paper https://static.rusi.org/325-OP-E2EE.pdf

50. HMGCC - His Majesty's Government Communications Centre (2025) Co-creation https://www.hmgcc.gov.uk/co-creation/

51. Home Office (2023) Review of the Computer Misuse Act 1990. Analysis of responses https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990/outcome/analysis-of-responses-accessible

52. ICS2 (2025) Survey: 30% of Cyber Pros Using AI Security Tools. https://www.isc2.org/Insights/2025/07/2025-isc2-ai-pulse-survey

53. IASME Consortium (2025) The benefits of Cyber Essentials certification. Webpage. https://iasme.co.uk/cyber-essentials/

54. Industrial Control Systems Community of Interest (2025) Home https://ritics.org/ics-coi/

55. Innovate UK (2025) CyberASAP. Website. https://iuk-business-connect.org.uk/programme/cyberasap/

56. Ipsos (2025) New Ipsos survey shows divides between MPs and the public on priorities for economic growth. News release. https://www.ipsos.com/en-uk/new-ipsos-survey-shows-divides-between-mps-and-public-priorities-economic-growth

57. Ipsos (2025) Britons back Online Safety Act's age checks, but are sceptical of effectiveness and unwilling to share ID https://www.ipsos.com/en-uk/britons-back-online-safety-acts-age-checks-are-sceptical-effectiveness-and-unwilling-share-id

58. Ipsos and Perspective Economics (2025) UK Cyber Security Sectoral Analysis Research report for the Department for Science, Innovation and Technology. https://assets.publishing.service.gov.uk/media/67cad8b18c1076c796a45c25/Cyber_Security_Sectoral_Analysis_Report_2025.pdf

59. Ipsos and Perspective Economics on behalf of DSIT - Department for Science, Innovation and Technology (2024) Cyber security skills in the UK labour market https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024

60. The Jill Dando Institute Research Laboratory (n.d.) About us https://www.ucl.ac.uk/engineering/jdi-research-laboratory

61. Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses. Science, Technology, & Human Values, 46(6), 1316-1339. https://doi.org/10.1177/0162243921992844

62. Lemnitzer, J.M., (2021) Why cybersecurity insurance should be regulated and compulsory. Journal of Cyber Policy, 6(2), pp.118-136. https://doi.org/10.1080/23738871.2021.1880609

63. Liebig, L., Jobin, A., Güttel, L. and Katzenbach, C., (2024) Situating AI policy: Controversies covered and the normalisation of AI. Big Data & Society, 11(4), https://doi.org/10.1177/20539517241299725

64. Liveley, G. (2022) Stories of Cyber Security Combined Report. Research Institute for Sociotechnical Cyber Security https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/3/939/files/2022/04/SOCS-Combined-Report-V4.-Final.pdf

65. Liveley, G., Slocombe, W. and Spiers, E., (2021) Futures literacy through narrative. Futures, 125, https://doi.org/10.1016/j.futures.2020.102663

66. Marks and Spencer (2025) Cyber incident update https://www.marksandspencer.com/help-and-support/cyber-incident-update

67. Michalec, O., Milyaeva, S. and Rashid, A., (2022) Reconfiguring governance: How cyber security regulations are reconfiguring water governance. Regulation & Governance, 16(4), pp.1325-1342. https://doi.org/10.1111/rego.12423

68. Michalec, O., Milyaeva, S. and Rashid, A. (2022) When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? Big Data and Society https://journals.sagepub.com/doi/full/10.1177/20539517221108369

69. Michalec, O. (2023) What's next for the NIS Regulations? Findings from RITICS Fellowship https://ritics.org/wp-content/uploads/2023/06/Whats-next-for-NIS-RITICS-report-final-310123.pdf

70. Michels, J.D., Walden, I. and Millard, C., (2025) Storm Clouds are Building: Surveillance, Sovereignty, and State Interests. Sovereignty, and State Interests (February 03, 2025). Preprint https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5159829

71. Microsoft (2020) Back to the future: What the Jericho Forum taught us about modern security https://www.microsoft.com/en-us/security/blog/2020/10/28/back-to-the-future-what-the-jericho-forum-taught-us-about-modern-security/

72. MOD - Ministry of Defence (2025) Preliminary Market Engagement Rapstone Industry Day. Planning notice https://www.find-tender.service.gov.uk/Notice/031070-2025

73. MOD- Ministry of Defence (2025) Strategic Defence Review. Review by Lord Robertson of Port Ellen KT GCMG, General Sir Richard Barrons KCB CBE and Dr Fiona Hill CMG https://assets.publishing.service.gov.uk/media/683d89f181deb72cce2680a5/The_Strategic_Defence_Review_2025_-_Making_Britain_Safer_-_secure_at_home__strong_abroad.pdf

74. Mott, G., Turner, S., Nurse, J.R., MacColl, J., Sullivan, J., Cartwright, A. and Cartwright, E., (2023) Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. Computers & Security, 128 https://doi.org/10.1016/j.cose.2023.103162

75. NAO - National Audit Office (2025) Cyber threat to UK government is severe and advancing quickly, spending watchdog finds. Press Release https://www.nao.org.uk/press-releases/cyber-threat-to-uk-government-is-severe-and-advancing-quickly-spending-watchdog-finds/

76. NCSC – National Cyber Security Centre (n.d.) CHECK penetration testing. Website https://www.ncsc.gov.uk/schemes/check/introduction

77. NCSC - National Cyber Security Centre (n.d.) Exercise in a Box. Website https://www.ncsc.gov.uk/section/exercise-in-a-box/overview

78. NCSC - National Cyber Security Centre (2021) Annual Review 202. Report https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf

79. NCSC - National Cyber Security Centre (2023) Accessibility as a cyber security priority. Blog post by Lee C. https://www.ncsc.gov.uk/blog-post/accessibility-as-a-cyber-security-priority

80. NCSC - National Cyber Security Centre and DSIT – Department for Science, Innovation and Technology (2024) 10 years of Cyber Essentials. Report https://www.ncsc.gov.uk/files/10-years-of-Cyber-Essentials.pdf

81. NCSC - National Cyber Security Centre (2024) Cyber Assessment Framework. Guidance https://www.ncsc.gov.uk/collection/cyber-assessment-framework

82. NCSC - National Cyber Security Centre (2024) NCSC Annual Review 2024. Report https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024/chapter-03/market-incentives

83. NCSC - National Cyber Security Centre and Plexal (2024) NCSC For Startups: Everything you need to know. Report https://www.ncsc.gov.uk/files/ncsc-for-startups-guidebook-alumni-may-24.pdf

84. NCSC - National Cyber Security Centre (2024) NCSC warns of widening gap between cyber threats and defence capabilities. News https://www.ncsc.gov.uk/news/ncsc-warns-widening-gap-between-cyber-threats-and-defence-capabilities

85. NCSC - National Cyber Security Centre (2024) The NCSC research problem book. Guidance https://www.ncsc.gov.uk/collection/problem-book

86. NCSC - National Cyber Security Centre (2025) CyberFirst overview. Website https://www.ncsc.gov.uk/cyberfirst/overview

87. NCSC - National Cyber Security Centre (2025) Cyber Security Toolkit for Boards. Guidance https://www.ncsc.gov.uk/collection/board-toolkit

88. NCSC - National Cyber Security Centre (2025) Principles Based Assurance. Information. https://www.ncsc.gov.uk/information/principles-based-assurance

89. NCSC - National Cyber Security Centre (2025) Cyber chiefs unveil new roadmap for post-quantum cryptography migration. News https://www.ncsc.gov.uk/news/pqc-migration-roadmap-unveiled

90. NDL - The National Data Library (2025) Home https://datalibrary.uk/

91. ONS - Office for National Statistics (2022) Inclusive measures of growth – How ONS is moving Beyond GDP, Blog post. https://blog.ons.gov.uk/2022/11/11/inclusive-measures-of-growth-how-ons-is-moving-beyond-gdp/

92. ONS - The Office for National Statistics (2025) Labour market overview, UK, July 2025 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/uklabourmarket/july2025

93. Osborne Clarke (2024) UK and EU take steps to bolster product security regimes https://www.osborneclarke.com/insights/uk-and-eu-take-steps-bolster-product-security-regimes

94. Pakes, A. and Pitts, H. (2023) Securonomics. The Foundation for European Progressive Studies https://ore.exeter.ac.uk/repository/bitstream/handle/10871/134208/Cybersecuronomics_Cybersecurity_and_Labo.pdf?sequence=1&isAllowed=y

95. Paterson, A. (2025) The UK Fly Wheel: Time to Win. Industry Insights https://www.harmonic.security/blog-posts/the-uk-fly-wheel-time-to-win

96. Pedersen, M.A., Albris, K. and Seaver, N., (2021) The political economy of attention. Annual Review of Anthropology, 50(1), pp.309-325. https://doi.org/10.1146/annurev-anthro-101819-110356

97. Peersman, C., May-Chahal, C., Das Chowdhury, P. (2025) Client-side scanning in private communication: security and privacy risks. REPHRAIN. Policy briefing. https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2025/01/REPHRAIN-CSS-Policy-Brief-January-2025.pdf

98. Perspective Economics and DSIT (2025) AI and software cyber security market analysis. Research and Analysis. https://www.gov.uk/government/publications/ai-and-software-cyber-security-market-analysis/ai-and-software-cyber-security-market-analysis

99. Plexal (2025) LORCA: The London Office for Rapid Cyber Security Advancement. Website. https://www.plexal.com/our-work/lorca/

100. Powell, R., Oswald, M., Janjeva, A. (2025) UK Public Attitudes to National Security Data Processing: Assessing Human and Machine Intrusion. Centre for Emerging Technology and Security https://cetas.turing.ac.uk/publications/uk-public-attitudes-national-security-data-processing-assessing-human-and-machine

101. Primer Minister's Office (2025) PM launches national skills drive to unlock opportunities for young people in tech. Press release https://www.gov.uk/government/news/pm-launches-national-skills-drive-to-unlock-opportunities-for-young-people-in-tech

102. Queen's University Belfast (n.d.) Centre for Secure Information Technologies. Website. https://www.qub.ac.uk/research-centres/csit/about/

103. Reinsurance News (2024) Coalition reveals new integrations with Microsoft365, Google Workspace, Amazon Web Services https://www.reinsurancene.ws/coalition-reveals-new-integrations-with-microsoft-365-google-workspace-amazon-web-services/

104. Renaud, K. and Coles-Kemp, L., (2022) Accessible and inclusive cyber security: a nuanced and complex challenge. SN Computer Science, 3(5) https://link.springer.com/article/10.1007/s42979-022-01239-1

105. REPHRAIN (2022) Response to DCMS Consultation: Security and Privacy in Apps and App Stores https://www.rephrain.ac.uk/wp-content/uploads/DCMS-Consultation-Security-and-Privacy-in-Apps-REPHRAIN-response.pdf

106. RISE UK Research Institute in Secure Hardware and Embedded Systems (n.d.) Home https://www.ukrise.org/about/

107. RITICS (2023) Resolving Anti-patterns in Industrial Control System / Operational Technology Environments. Industrial Control Systems Community of Interest https://ritics.org/wp-content/uploads/2023/10/ICS-COI-Resolving-Anti-Patterns.pdf

108. RITICS – Research Institute in Trustworthy Industrial Control Systems (2025) Home https://ritics.org/

109. Sanchez-Graells, A. (2023) Guaranteeing public sector adoption of trustworthy AI - a task that should not be left to procurement. Policy Briefing https://www.bristol.ac.uk/policybristol/policy-briefings/public-sector-ai/

110. Sampson, D., Kampylis, P., Moreno-León, J. and Bocconi, S., (2025) Towards high-quality informatics K-12 education in Europe: key insights from the literature. Smart Learning Environments, 12(1), https://link.springer.com/article/10.1186/s40561-025-00366-5

111. Schneier (1999) Crypto-Gram https://www.schneier.com/crypto-gram/archives/1999/0215.html

112. Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2023). The nature of losses from cyber-related events: risk categories and business sectors. Journal of Cybersecurity, 9(1) https://academic.oup.com/cybersecurity/article/9/1/tyac016/7000422

113. Slaughter and May (2025) What will the Cyber Security and Resilience Bill mean for your organisation? https://www.slaughterandmay.com/insights/new-insights/what-will-the-cyber-security-and-resilience-bill-mean-for-your-organisation/

114. Slupska, J. and Tanczer, L.M., (2021) Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things. In The Emerald international handbook of technology-facilitated violence and abuse (pp. 663-688). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211049

115. Spencer, M. and Pizio, D. (2023) The de-perimeterisation of information security: The Jericho Forum, zero trust, and narrativity. Social Studies of Science https://journals.sagepub.com/doi/full/10.1177/03063127231221107

116. Spencer, M. (2025) ASSURANCE BY PRINCIPLE: Preparing for the next generation of product security assurance. RISCS report. https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/3/939/files/2024/03/RISCS_ASSURANCE-BY-PRINCIPLE-REPORT_AW-4f8c70e9feb14517.pdf

117. Such, J.M., Ciholas, P., Rashid, A., Vidler, J. and Seabrook, T., (2019) Basic cyber hygiene: Does it work?. Computer, 52(4), pp.21-31. https://core.ac.uk/reader/224767750

118. Topping, C., Dwyer, A., Michalec, O., Craggs, B. and Rashid, A., (2021) Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security, 108, https://doi.org/10.1016/j.cose.2021.102324

119. UK Cyber Cluster Collaboration (2025) Home https://ukc3.co.uk/

120. UK Government (2025) Digital and technologies sector plan. https://assets.publishing.service.gov.uk/media/685862e5b328f1ba50f3cea4/industrial_strategy_digital_and_technologies_sector_plan.pdf

121. UKRI (2025) Digital Security by Design (DSbD) programme outcomes. Corporate report. https://www.ukri.org/publications/digital-security-by-design-dsbd-programme-outcomes/

122. VeTSS – The Research Institute on Verified Trustworthy Software Systems (n.d.) Home https://vetss.org.uk/

123. Wallis, T. and Dorey, P., (2023) Implementing partnerships in energy supply chain cybersecurity resilience. Energies, 16(4), https://www.mdpi.com/1996-1073/16/4/1868

124. Wikipedia (2025) Red Hat: Business Model https://en.wikipedia.org/wiki/Red_Hat#Business_model

125. Woods, D.W. and Moore, T., (2019) Does insurance have a future in governing cybersecurity? IEEE Security & Privacy, 18(1), pp.21-27. https://www.danielwoods.info/assets/pdf/DW2020_governance_IEEESP.pdf

126. Woods, D.W., (2023) Lemons and Liability: Cyber Warranties as an Experiment in Software Regulation. https://i.blackhat.com/BH-US-23/Presentations/US-23-Woods_LemonsandLiabilityCyberWarranties-whitepaper.pdf

127. Woods, D.W. and Seymour, S., (2023) Evidence-based cybersecurity policy? A meta-review of security control effectiveness. Journal of Cyber Policy, 8(3), pp.365-383. https://doi.org/10.1080/23738871.2024.2335461

128. World Economic Forum (2021) 'Leave No One Behind: How to Include Civil Society in the Cybersecurity Debate' https://intelligence.weforum.org/monitor/latest-knowledge/d0c6a0aa1c244fc78fbb2b0a16cfb832

129. World Economic Forum (2024) This is venture capital's key role in driving global cyber resilience https://www.weforum.org/stories/2024/09/venture-capital-role-cyber-resilience-cybersecurity/

130. World Economic Forum Centre for Cybersecurity (2025) Bridging the Cyber Skills Gap - Why is there a cybersecurity talent shortage? https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home

131. Worth, S., Gurumoorthy, A. and Simperl, E. (2025) Developing the UK National Data Library for public benefit: 10 key reflections https://www.kcl.ac.uk/developing-the-uk-national-data-library-for-public-benefit-10-key-reflections

Pillar 1: Culture	
Recommendation 1 – Support growth journeys Government and industry stakeholders should review the incentives and validation routes available to cyber businesses. The goal is to make it easier for cyber businesses to navigate the complexity of meeting cyber demand and to shift the culture to one that selects and helps winners to grow.	**Suggestion 1 – Pilot programmes that allow NCSC and DSIT to qualify and connect cyber startups with government departments** NCSC and DSIT should be allowed to explore ambitious and experimental ways of reforming procurement, linking early-stage R&D opportunities to commercial tenders in more mature settings. This could be a joined-up government effort to use NCSC to qualify the technical credentials of cyber businesses, DSIT to connect them to departments, and to work with procurement and departments on the value for money and incentives to make this work. **Suggestion 2 – Expand the co-creation and government investment models for wider commercial participation** The NSSIF funding model and HMGCC co-creation model should serve as examples for convening and funding cyber ideas. Place-based leadership should seek to use this to incentivise startup and CISO involvement in pre-procurement workshops on problem co-creation with the NCSC.
Recommendation 2 – Stimulate informed demand Government should use guidance and regulations to stimulate growth by setting expectations for high quality reporting of cyber risks, consulting on mandating the use of Cyber Essentials, and encouraging usage of cyber insurance and principles-based assurance. The goal is to encourage organisations across sectors to prioritise cyber security in alignment with their organisational risks, thereby reducing incidents, increasing resilience, supporting broader economic growth, and driving demand for more UK cyber services.	**Suggestion 10 – Mandate Cyber Essentials in selected supply chains** DSIT and CISOs representative of critical or otherwise relevant sectors should agree on key controls to mandate across supply chains, starting with Cyber Essentials. A phased approach should embed these requirements into procurement frameworks for government departments, critical infrastructure, and large businesses. Over time, alignment with standards like NIST SP 800-161 should be considered. As the scheme evolves, NCSC should lead on building the evidence base for its effectiveness, working with academic and insurance sector experts. **Suggestion 11 – Map standards and regulations to help navigate compliance** NCSC, DSIT and DBT to continue their mapping and harmonisation efforts, prioritising international alignment and communication to organisations with significant export markets. **Suggestion 12 – Share guidance early to reduce burden** NCSC to share emerging cyber guidance early to help communities anticipate and share best practices and deal with overlaps and gaps. This could be particularly valuable for critical infrastructure operators whose budgets are regulated through long-term funding cycles and currently lack alignment with the updates of the Cyber Assessment Framework . **Suggestion 13 – Improve guidance on the reporting of cyber risk** Government should seek evidence and develop proposals on the quality of corporate reporting on what cyber risks exist for a business and how they are managed. The evolving proposals should help businesses tighten the connections between cyber risks and the material risks they are obliged to report on. **Suggestion 14 – Support pre-procurement engagement for SMEs** The UK Government (Crown Commercial Services) and innovation incubators (for example but not limited to programmes such as Cyber Runway) should implement formal pre-engagement mechanisms to help SMEs showcase their cyber security solutions and educate procurement teams ahead of tender processes. This could include regular market engagement days, innovation showcases, and technical briefings specifically aimed at introducing SME capabilities to public sector buyers. **Suggestion 15 – Accelerate the development of Principles Based Assurance** We call for an accelerated adoption of the Principles Based Assurance in codes of practice and development of appropriate assessment facilities. This action will need pre-engagement activities and incentives between vendors and buyers, to make it real, and so involve DSIT, the NCSC, and supported by evidence from the academic leaders (e.g. Research Institute for Sociotechnical Cyber Security). **Suggestion 24 – Convene innovation work on cyber insurance** DSIT and regional cyber growth leaders should convene further work with the insurance industry and SMEs to explore the future of business innovations within the cyber insurance industry.

Recommendation 3 – Foster public participation in cyber skills and growth UK cyber professionals should engage with UK civil society on the sector's role in national resilience and prosperity. This means emphasising the role cyber teams play in 'keeping the lights on' and the importance of skills initiatives from schools to professional development for cyber founders and leaders. The goal is to build broader UK support for the role of cyber, making it easier for businesses to prioritise cyber, for people to learn cyber skills, and for the industry to attract, grow and maintain talent.	**Suggestion 3 – Include marginalised demographics in product development** Cyber technologists developing products and services to engage with marginalised demographics e.g. via representative organisations such as Age UK for elderly people. This will enable better understanding of user's product needs, whether as a business imperative or commitment to responsible innovation. **Suggestion 4 – Convene 'cyber in public interest' events** DSIT, cyber businesses and civil society organisations to convene a forum on developing cyber technologies in the public interest . These could be modelled on similar efforts by the Finnish authorities . The goal is to co-create technologies developed in the public interest and prevent wasted public spending caused by low adoption rates or delays in technology rollout. **Suggestion 5 – Use immersive methods to engage civil society** Leading third sector organisations and small business associations to adapt and use immersive methods (similar but not exclusive to the 'Exercise in a box') to engage civil society in the challenges and roles of cyber professionals. **Suggestion 6 – Focus on the way cyber language is used with the public** From marketing departments advertising cyber conferences, HR leads recruiting for new roles to journalists reporting on emerging incidents, everyone has a role in shaping the language we use. The cyber community should adopt language reflecting the positive role cyber security plays in the wider society. This could be achieved in conjunction with commissioning studies on the role of language in engaging diverse communities. **Suggestion 7 – Incentivise organisations to create cyber career entry roles** DSIT should consider introducing incentives to help organisations hire and train less experienced people in cyber roles. This could be through developing components of Tech First, apprenticeship schemes and graduate programmes These incentives could be linked to policies for stimulating informed demand for cyber. **Suggestion 8 – Double down on skills** Developing cyber skills needs to be embedded more deeply in more places. Building on the NCSC materials, cyber leaders (across DSIT, DBT, Department for Education, and regionally) need to keep supporting and communicating the value of all of the initiatives, from schools programmes and professional development to mentoring cyber founders. **Suggestion 9 – Review the Computer Misuse Act** Recognising there is an enforcement challenge, the Government should review whether amendments to the Computer Misuse Act can be made to address the negative impact it has on skills development and broadening UK cyber growth and resilience.

Pillar 2: Leadership

Recommendation 4 – Appoint a UK cyber growth leader

Government should appoint a leader to provide expertise and drive coordinated action across the cyber security industry and within Whitehall. This role would encompass some of the previous Cyber Ambassador's responsibilities in advancing export growth and supporting national security objectives. It would also include responsibility for driving this growth plan forward.

The goal is to ensure cyber growth is prioritised and integrated across several policy areas.

Recommendation 5 – Appoint growth leaders in places of cyber strength

Appoint place-based leaders to be responsible for convening and driving cyber growth initiatives and outcomes. These leaders should have industry experience, support the UK cyber growth leader and be independent from central and regional government.

The goal is to ensure places use their strengths to grow, create, and attract more cyber businesses.

Suggestion 16 – Choose a few places for Cyber Growth Centres

Government should work with place-based stakeholders to identify areas of strength and establish Cyber Growth Centres. These Centres should be coordinated at the national level and have an obligation to engage with adjacent regions not directly served by a co-location centre.

Suggestion 17 – Support growth leaders with funding and structure

No current place has everything it needs to be a Cyber Growth Centre. To enable leaders to drive growth, they will need both support, for example through being employed within a common organisational structure such as the Digital Catapult, and access to funds, whether through local, regional, or national mechanisms.

Recommendation 6 – Expand the NCSC role

The Government should expand and appropriately resource the NCSC to help drive cyber growth. The NCSC is a 'crown jewel' for cyber resilience, which is their primary mission. They also have the capability to guide and steer for growth outcomes. Given the importance of resilience, growth should be added without diverting attention from their existing priorities.

The goal is to use the deep expertise of NCSC in support of cyber growth, guiding and validating cyber businesses, research, futures, and technologies.

Suggestion 21 – NCSC to support place based cyber growth leaders

Expand the role of NCSC to support the place based cyber growth leaders. This should include supporting selected startups through each of recommendations 7, 8 and 9.

Suggestion 22 – NCSC to work with place based cyber growth leaders assessing startups

Recognising that assessing businesses for admission into schemes such as the Cyber Resilience Test Facilities is resource intensive, both in terms of people and testing facilities, the Cyber Growth leaders should work with NCSC and test facility leadership to support startups.

Pillar 3: Places

Recommendation 7 – Develop futures-oriented communities

Place-based leaders should use their convening role to look forward and shape future markets. To do this, they should bring together CISOs, academia, small and large industry, government, and other stakeholders to share perspectives on, and pursue solutions to emerging cyber challenges.

The goal is to drive initiation, co-creation and delivery of innovative projects into the market, and to build a culture of anticipation.

Recommendation 8 – Places to nurture distinct tech areas

Places should be strategic in prioritising technologies and application areas based on their cyber strengths and sector connections in alignment with the Industrial Strategy and the UK Government Resilience Action Plan. Cyber innovation in AI, cyber-physical systems, and tooling for fundamentals should be considered as initial priority areas.

The goal is for the UK to have place-based cyber strengths that are more than the sum of their parts, each contributing to UK cyber growth.

Suggestion 18 – Use places used to convene stakeholders on futures

Cyber Growth Centres should act in a convening role to bring together stakeholders to engage in futures planning and ensure that the place and the country innovate to remain resilient in the face of future technologies and threats.

Suggestion 19 – Engage with places to identify strengths to focus on

The choice of location and themes for Cyber Growth Centres requires further exploration, namely a rapid study to engage with regional leaders to make informed choices on both. From the current review (see section 5.2) this report suggests that AI, cyber physical systems, quantum, tooling for fundamentals and digital secure by design should each be considered as key themes for growth.

Suggestion 23 – Identify commercialisation opportunities for cyber safe AI

Work with the 'AI Opportunities Action Plan 2025' to ensure cyber programmes and commercialisation opportunities are developed. Place based Cyber Growth Centre leaders should convene futures sessions between researchers and businesses in AI and cyber and the demand side to identify and co-create new products and services.

Recommendation 9 – Places to provide safe environments

Create safe havens with infrastructure and data for multiple groups of stakeholders (not just those with security clearances) to explore, 'role-play', co-create and share how to assemble and test solutions to current and emerging challenges.

The goal is to build broader cyber resilience capability, which will both serve in moments of crisis and be a pool of talent for cyber growth.

Suggestion 20 – Target a few places to create safe environments

Cyber Growth Centres should provide the means for multiple groups of stakeholders to come together to explore, exercise, co-create, and share how to assemble and test solutions to both current and emerging challenges. This includes the Cyber Growth Centres providing safe havens where real data from Security Operations Centres can be made available for exercises.

Underpinning principles

Underpinning principle 1 – The UK cyber sector should act as one team

Many stakeholder groups have overlapping but distinct interests, and there are plenty of examples where they have built trust and supported each other. Collecting from the above recommendations, the community should start to operate as a single team growing cyber in the UK. This starts with celebrating, building on and catalysing the social capital in the UK cyber community.

Underpinning principle 2 – Growth + resilience + value for money

The broader benefits of cyber resilience and growth should be recognised as part of 'value for money'. Too often, purchasing and investment decisions are driven by a cost-based view of 'value' missing the wider importance of UK cyber innovation for future resilience, sovereignty, and growth.