Appendix A

CYBER RESILIENCE ALLIANCE

A Science and Innovation Audit Report sponsored by the Department for Business, Energy and Industrial Strategy

Review led by:

- Worcestershire Local Enterprise Partnership
- gfirst LEP
- Swindon & Wiltshire Local Enterprise Partnership
- The Marches Local Enterprise Partnership
- Skylon Park
TABLE OF CONTENTS

ACKNOWLEDGEMENTS ............................................................................................................ 3
STEERING GROUP MEMBERSHIP: .......................................................................................... 4
FOREWORD ........................................................................................................................... 7
INTRODUCTION & CONTEXT ................................................................................................. 8
   The Region ......................................................................................................................... 8
VISION .................................................................................................................................. 10
KEY STRENGTHS .................................................................................................................. 12
OPPORTUNITIES .................................................................................................................... 14
   Opportunities for R&D, Product Development and Enhancing Productivity: ........ 14
   Opportunities for Resilience: ................................................................................... 14
   Domestic and Export Growth Opportunities for the Cyber Resilience Alliance: ...... 14
GAP ANALYSIS ..................................................................................................................... 15
   Development of Skills & Talent: ............................................................................... 15
   Provision of Facilities and Infrastructure: Reflect the Breadth & Diversity of the Sector: ................................................................. 16
KEY AMBITIONS AND PROPOSALS FOR GROWTH .......................................................... 17
   Proposal 1: Innovation, Research & Development | Investing in Infrastructure ..................... 17
   Proposal 2: Encouraging Sustainable Demand: ...................................................... 18
   Proposal 3: Improving Skills and Talent: ................................................................. 19
   Proposal 4: Focused Marketing & Sector Targeting: ............................................. 20
NETWORKING AND COLLABORATION ............................................................................ 21
Acknowledgements

This report is sponsored by the Department for Business, Energy and Industrial Strategy (BEIS) and is produced on behalf of the Cyber Resilience Alliance, a consortium of over a hundred commercial, private, public, and voluntary organisations from across Worcestershire, Gloucestershire, The Marches (Shropshire, Herefordshire, and Telford and Wrekin), and Swindon and Wiltshire.

The Cyber Resilience Alliance is committed to endorsing and supporting the implementation of this Audit.

This report has been facilitated by the ongoing dedication of the Cyber Resilience Alliance Steering Group and its advisors. Sam Donaldson and Matt Rooke (RSM Economic Consulting) have also supported extensively in the collation and reporting of the region’s economic and skills base. The Steering Group also provide thanks to Technopolis for their support in providing bespoke analytical support.

Throughout this process, the Science and Innovation Audit received written or verbal evidence from over sixty leading members of business, academic and public bodies. These contributions are greatly appreciated by the Cyber Resilience Alliance, and have been a valuable call to action for the region.
Steering Group Membership:

**Gary Woodman: Worcestershire LEP**
Gary is tasked with driving forward Worcestershire LEP and leading an Executive Team to support the WLEP’s ambitions and delivery of the WLEP business plan. From his former role as Head of Policy and Education at Herefordshire and Worcestershire Chamber of Commerce, he has brought with him a wealth of business insight and networks as well as considerable experience of Government policy and delivery. Educated at the University of Wales, Cardiff, where he obtained his degree in Leisure and Recreation Management, and the University of Gloucestershire, where he studied for his postgraduate diploma in Business Administration, he previously worked for Gloucestershire County Council’s market towns and economic development arm, overseeing regeneration.

**Nicola Whiting: Titania**
Nicola Whiting is an experienced Chief Operations & Strategy Officer with a strong history of working in Cyber Security / InfoSec. Specialising in enterprise security automation software (self-healing networks), business development, trust-based selling and neuromarketing. An advocate for Autism and Women in Cyber, she provides government level advice on Diversity and writes for publications such as The Huffington Post, Defence Contracts Bulletin, Defence News Online and Signal. A well regarded public-speaker, keynote topics include “The Rise of Automated Attacks”, “The Future of Automated Cyber Defences” and “Hacking the Human Brain”. In 2017 Nicola was named by SC Magazine as one of the Top 20 most influential women working in cyber security.

**Professor Ian Oakes: University of Wolverhampton**
Over the last 20 years, Professor Oakes has held a number of senior management posts in higher education before joining the University of Wolverhampton in 2008 as Pro Vice-Chancellor with responsibility for the University’s research and enterprise agenda and developing the growing knowledge transfer arena at regional, national and international levels. More recently he was promoted to the role of Deputy Vice-Chancellor as well as Chief Executive of University of Wolverhampton Science Park.
Professor Kamal Bechkoum, Professor of Computing, is Head of The School of Business & Technology at The University of Gloucestershire. He is a Gloucestershire Commissioner for Cyber, Science and Innovation and the University lead of a £3m Cyber Security project, working with other organisations to produce highly skilled cyber professionals in Gloucestershire and beyond. Professor Bechkoum has also worked at Cranfield, De Montfort, Wolverhampton, Derby, and Northampton where he was Executive Dean of the School of Science and Technology with university executive responsibility for research and enterprise and intellectual capital. He holds a PhD in Software Techniques for Computer Aided Engineering from the University of Cranfield, UK and is a Fellow of the British Computer Society and a Chartered IT Professional.

Professor Richard Benham is the world’s first formal Professor of Cyber Security Management and lectures at Coventry Business School and at the UK’s National Cyber Skills Centre where he is Professor in Residence. He is also a Visiting Professor in in Cyber Security Management at The University of Gloucestershire and previously in Policing at Staffordshire University. Outside of the UK, Prof Benham is a SWIFT Institute Scholar and speaks at one of the World’s leading Business schools, IMD in Switzerland. In 2013 he published “The Cyber Ripple Theory®” which is widely recognised as the World’s first Cyber Management Theory and includes the human elements of Cyber Security. In 2017 he was chosen to join the DL100 and was nominated for UK Digital Champion of the Year. He is currently the Digital Champion for the South West.

Mark Pearce: Skylon Park: Mark is the Managing Director of Hereford Enterprise Zone Limited, a private/public partnership company charged with catalysing business investment at Skylon Park, the only Enterprise Zone in the country with a defence and security focus. In his 6 years at Skylon Park, over 37 acres of land has been sold, 41,000 sq m of new workspace built or committed, 38 businesses moved in and over £20m of private sector investment secured, with more sales and projects in the pipeline. An economic development professional of nearly 30 years standing, Mark worked previously at the West Midlands Regional Development Agency, Advantage West Midlands (AWM) for over 10 years, latterly as Corporate Director. He oversaw significant investment into urban and rural regeneration in the West Midlands including longstanding Board representation at Hereford Futures, the £100m+ mixed use project that has transformed Hereford City Centre.
Dev Chakraborty: Gloucestershire LEP: Dev is currently the Deputy Chief Executive for GFirst LEP, Gloucestershire’s Local Enterprise Partnership. Dev has over 25 years experience in marketing, sales and media roles in the South West, including 10 years of senior management and board level experience. Dev was part of the original team that launched Cornwall’s award winning, commercial radio station, Pirate FM then becoming Managing Director of Star FM in Bristol. Immediately prior to his role at GFirst LEP he was a Business Guide at the Growth Hub working with high growth businesses across Gloucestershire.

Kathryn Jones: Marches LEP: Kathryn joined the Marches LEP team in October 2017 as Partnership Manager. She has a background in economic development and has managed international, regional and local business support projects, including research and development grant programmes and business growth initiatives. More recently, she has worked in the further and higher education sectors promoting the importance of skills development in driving economic productivity.

Colette Mallon: Swindon and Wiltshire LEP: Colette leads Business Engagement for the SWLEP. She has specific responsibility for building relationships with businesses, government, stakeholder organisations and other LEPs to support the delivery of the Swindon and Wiltshire Strategic Economic Plan.
Foreword

The UK is a globally leading digital economy, and our prosperity is reliant upon our ability to secure our businesses, data and networks from cyber threats. The Cyber Resilience Alliance region\(^1\) consists of some of the UK’s brightest minds and cutting-edge technology addressing cyber security challenges every day. As cyber-attacks become more frequent and more damaging, our region offers the talent and resources that lead the way in supporting the UK’s efforts to be one of the the most secure, capable, and cyber resilient countries in the world.

We are home to over a hundred businesses and organisations (and growing) active in cyber security product and solution development including large names such as Northrop Grumman, BT, Raytheon, BAE Applied Intelligence, Lockheed Martin, and Nationwide Building Society; highly regarded cyber security firms such as Anomali, Anon AI, and Titania; and rapid growth in innovative start-ups including PixelPin and Ripjar.

Outside of London, we are the UK’s leading region in cyber security, with an estimated 5% UK market share, despite having 3% of the UK’s population. However, our close-knit community has historically been rooted in securing the UK: during World War II the UK Government moved its radar technology to Malvern; which now holds the UK’s largest cluster of cyber security firms. In 2001, QinetiQ, a major defence and security firm, was established through the privatisation of the Defence Evaluation and Research Agency (part of the Ministry of Defence), alongside the creation of the UK’s Defence Science and Technology Laboratory (Dstl) in Porton Down. Over 5,000 of our community work in GCHQ in Cheltenham at the heart of UK security matters, and we also host the Ministry of Defence Joint Cyber Unit based in Corsham, and the Special Forces in Herefordshire.

This Science and Innovation Audit has helped to bring together our community of business, entrepreneurs, academics, policy practitioners, and defence, security and cyber expertise in a new way: to identify common strengths, challenges and opportunities for growth.

We are particularly strong in public administration, defence, security, health, and manufacturing. These are all industries that not only require cyber security solutions, but will actively drive the need for innovation, new products, and growth in the industry.\(^2\)

Our people are ambitious and determined to cement the Cyber Resilience Alliance region as a leading place for UK and global cyber security practice helping to grow the region, secure the UK’s assets, and to support cross-sectoral and cross-boundary initiatives that can create innovative, world-leading and secure products and services in the UK economy.

We have the skills, infrastructure, and resources in place to continue growing the sector, but we recognise the challenges ahead. That’s why we are investing heavily in infrastructure, skills and talent, research and knowledge transfer, and focusing our efforts in making the region the leading location for cyber security firms outside London.

---

\(^1\) Worcestershire, Gloucestershire, The Marches, and Swindon & Wiltshire LEPs.

\(^2\) The UK Cyber Exports Strategy identifies the six most promising sectors for UK cyber security exports in 2018 (Government, Financial Services, Automotive (and Autonomous Vehicles), Energy and Critical National Infrastructure, Health, and Infrastructure)
Introduction & Context

In Autumn 2015 the UK Government announced regional Science and Innovation Audits (SIAs) to catalyse a new approach to regional economic development. SIAs enable local consortia to focus on analysing regional strengths and identify mechanisms to realise their potential.

In Gloucestershire (GFirst), Worcestershire, The Marches (Shropshire, Herefordshire, and Telford and Wrekin), and Swindon and Wiltshire Local Enterprise Partnerships (LEPs), the Cyber Resilience Alliance was formed in 2017 to focus on our strength in cyber security. This report presents the results which includes broad-ranging analysis of the Cyber Resilience Alliance’s capabilities, the challenges and the substantial opportunities for future economic growth.

The Region\(^3\)

The Cyber Resilience Alliance region consists of four Local Enterprise Partnerships (LEPs), stretching from north of Shrewsbury to south of Salisbury (over 180 miles). The region spans more than 5,200 square miles (10.4% of England’s total geography), with 2.59 million residents, of which 1.58m are aged between 16-64 (3.8% of the UK’s working age population). At its heart, it includes the urban settlements of Worcester, Cheltenham, Gloucester, Hereford, Telford, Swindon and Shrewsbury which are well-connected to the rest of the country via strong rail links and the M5 motorway corridor that runs from Birmingham through to Bristol (through the centre of Worcestershire and Gloucestershire LEPs).

The region is synonymous with UK defence and security and is home to some of the world’s largest defence firms (BAE Systems Applied Intelligence in Gloucester, Babcock in Swindon, and Lockheed Martin in Wiltshire), as well as the UK’s highest levels of public security (Ministry of Defence in Corsham, Special Forces in Hereford, and GCHQ in Cheltenham).

Within the Cyber Resilience Alliance region, we recognise the considerable concentration of cyber skills within the population\(^4\), largely due to proximity to GCHQ which in recent

---

\(^3\) See Section 3: Introduction to the SIA Region

\(^4\) See Section 4 Strengths and Innovation, and Section 5.2 Size and Scale of the Cyber Resilience Alliance Sector
years has also encouraged a wide range of spin-outs and investment from cyber security organisations.

The key to industrial success in the future is not just establishing cyber businesses. It is also about embedding cyber skills and principles of 'secure by design' into the existing industrial infrastructure. This will provide competitive advantage, and increase opportunities for employees to develop skills that make them and their business more attractive in a global market. We also recognise that skills being currently developed could be vulnerable to future automation, with a need to ensure there is a route to maximise high value skills and increase resilience moving forward.

This audit is therefore structured to test two main hypotheses:

1. There is a strong concentration of skills in cyber security within the region, which can be used to embed cyber resilience through a wider industrial base, including making a strong contribution to the growth of the UK’s cyber security sector directly, and supporting industries within which their demand for secure solutions will incubate, support and grow the region’s economy.

2. Sustainable business needs to be competitive and trusted. Do traditional businesses do enough to understand and embrace cyber resilience, and how can they best invest accordingly?

The Audit will identify opportunities to build linkages between the strong regional cyber security expertise and the wider community.
Vision

To maximise the opportunities of the cyber security sector in the Cyber Resilience Alliance, we set out the following evidence-informed vision for the region.

Firstly, we want to double the size (measured by employment) of the cyber security sector in the region, aligning the potential of our people with high-value employment into firms that can be global leaders.

We will plan interventions in line with anticipated and sustainable growth (approximately 10% per annum).

By 2025, we aim to have 10,000 (FTEs⁵) employed in the sector.⁶

Secondly, this Science and Innovation Audit has confirmed many of the propositions set out within our Expression of Interest: the region is particularly strong in cyber security with respect to the number of firms (more than fifty cyber security firms⁷), and over a hundred organisations and firms actively shaping cyber security products, services and development. As a result, we want the region to be known nationally and internationally as the UK’s largest cluster of cyber security activity outside London.

Registered Cyber Security Companies within the Region: A Rapidly Growing Sector…

Target: 10,000 FTEs by 2025

Current: 5,000 Cyber FTEs (2018)

Source: Bureau van Dijk

---

⁵ Full Time Equivalent staff
⁶ See Section 5.3 Employment Estimates and Projections
Thirdly, with this recognition, we want to ensure that the region continues to promote an entrepreneurial start-up culture & attracts new investment. As a result, by 2025, we estimate that the region’s sector will contain more than one hundred active cyber security firms – and with further investment and support, this figure could be even higher, particularly given the attractiveness of the region (competitive operational costs for business, a growing talent pool, and strong clusters of cyber innovation). Further, we will endeavour to identify opportunities for firms in manufacturing, defence, automotive, financial services and other sectors to embrace cyber security as a core component in product development.

This aligns to the findings of this Audit that nominal R&D expenditure has increased within the West Midlands and South West since 2008 at twice the national rate (grown 43% between 2008-14 compared to 21% across the UK). In recognition of the rapid growth in BERD\(^8\) in the region, and the potential for disruptive technologies to require cyber security solutions (particularly in advanced manufacturing and automotive), we will support cyber security firms to identify UK supply chain opportunities that can further grow R&D expenditure in the region, improving the quality and value of our strong manufacturing base.

Finally, we recognise there is a long-standing productivity gap in the region. GVA per capita in the region is £22,804 (2015). This means that productivity is 10% lower than the UK’s GVA per capita (£25,351). Tech Nation (2017) identify an average advertised digital salary of £36,236 in Worcester and Malvern. Further, there is also a nationally recognised ‘cyber dividend’ with regard to salaries. Technopolis analysis indicates that in the last six months of 2017, median advertised salaries in cyber security in the region ranged from £45,000 (Tewkesbury) to £82,500 (Worcester) – with a national median of £57,000 per annum.

With regard to productivity and earnings, there is clear potential for growth in the cyber security sector to improve the region’s GVA per capita, and support efforts to narrow the productivity gap over the next decade.

Further, the Audit set out to explore how the expertise within the region could be utilised to best develop talent and embed cyber resilience within firms across industries. There are strong initiatives in the region to achieve these aims, including (but not limited to) the Cyber Club, the Malvern and West of England Cyber Security clusters, and the IASME consortium\(^9\). Our vision for the region is to embed cyber resilience through the promotion of initiatives that encourage wider investment in cyber security products and processes across all industries.

Long-term, it is our ambition that the Cyber Resilience Alliance Region is recognised as a world-leading cluster, and there are many opportunities for our businesses and organisations to embed and promote cyber resilience globally, and to lead within cyber security export markets.

\(^8\) Business Expenditure on Research & Development. See Section 4.2 Research Strengths and 4.3 Innovation Strengths and Growth Points

\(^9\) See Section 5.5 Local Science and Innovation Talent
Key Strengths

The Cyber Resilience Alliance region is host to strong research collaboration between government, universities, research institutions, and businesses. Despite a relatively small working age population (1.6 million), the Cyber Resilience Alliance is highly regarded with several internationally recognised cyber security clusters (Malvern, Worcester, and Cheltenham in particular).

Map of the Cyber Resilience Alliance Business, Commercial, Public, and Academic Assets:

Source: RSM, CRA Market Intelligence
The region is particularly strong in...

Research:

The SIA area has an LQ of 2.2 for cyber security projects led, demonstrating that the area is twice as likely as the national average to have organisations leading publicly-funded cyber security research. This indicates that Cyber Resilience Alliance area has above average concentrations of cyber security research.

R&D Investment:

Within the Cyber Resilience Alliance, there is evidence that government, business, higher education institutions, and non-profit organisations are increasing expenditure in research and development. As shown in Section 4.3, nominal R&D expenditure has increased within the West Midlands and South West since 2008 at twice the rate nationally (grown 43% between 2008-14 compared to 21% across the UK).

Commercial Activity:

Within the UK itself, London is recognised as a cyber security hotspot, with more than two hundred cyber security firms estimated in the city, and many more vying for cyber security talent to support the operations and development of financial services, legal services, media and telecommunications etc.

However, the Cyber Resilience Alliance Science and Innovation Audit has enabled an overview of the firms and organisations active within the region and provides an evidence base that the region hosts the second largest cluster of cyber security activity outside of London.

Further, the region has a prominent defence and security community, which directly supports the growth and sustainability of the cyber sector. As a result of this community rooted in security, the region is a hotbed for cyber security innovation in the UK.

Infrastructure that supports innovation:

The region is focused upon developing its entrepreneurial and innovation support network, with emphasis on high-tech, cyber, digital and manufacturing industries. The region is home to a wide range of universities, research institutes and councils, public sector organisations, businesses, and incubation and innovation spaces active in developing the cyber security sector. This Audit has identified over a hundred assets and organisations active in supporting cyber security product and service development. Further, the region is in close proximity to several world-leading businesses, universities and research institutions active in cyber security, advanced manufacturing and automotive technologies.
Opportunities

The cyber security sector clearly presents several opportunities in the region, not just for economic growth at the sectoral level, but also through securing the crucial technological developments across wider society. Ultimately, cyber security is about embedding trust in society, economy and technology, and the Cyber Resilience Alliance region will provide the expertise to support wider transformational advancement in the UK.

There are clearly opportunities that arise from automation, Artificial Intelligence (AI) and Machine Learning, and within securing the rapid roll-out of Internet of Things (IoT) devices across the country.

Opportunities for R&D, Product Development and Enhancing Productivity:

In recent years, there has been a concerted effort on behalf of manufacturing to increase investment in research and development in the region. Given the opportunities that arise from automation, Artificial Intelligence, and machine learning for firms across the region, there are also core opportunities for the region’s cyber security sector to benefit from commercial partnerships to secure these technologies.

This increased investment in transformative digital technology in the region, combined with world-leading secure solutions, will generate considerable opportunity to enhance productivity and living standards in the region.

Opportunities for Resilience:

As stated, the most recent DCMS Cyber Breaches Survey (2017) indicates that 34% of businesses have no spend on cyber security, and that four in ten experienced some form of breach last year. We will seek to further develop initiatives to tackle gaps in cyber resilience in the region e.g. funding for advice, Cyber Security vouchers, Cyber Club etc.

There is clear opportunity for the region to act as a regional testbed for initiatives that support cyber resilience to be scaled up to national level (evidence informed pilots and interventions).

Domestic and Export Growth Opportunities for the Cyber Resilience Alliance:

As identified in the UK Cyber Exports Strategy (DIT, 2018) – our region has an established, expert and innovative sector made up of companies across a full range of capabilities.

UK cyber security exports are set to grow to £2.6bn by 2021, and will be primarily driven by governments, financial services, automotive, energy and Critical National Infrastructure, healthcare and infrastructure.
Gap Analysis

Whilst the cyber security sector has demonstrated rapid expansion and growth in the region in recent years, there remain gaps that are restricting the growth and potential of the sector, and present challenges for the future sustainability and talent flow in the industry.

Within cyber security, these gaps impact not only the sector directly, but impact the UK’s capacity to defend its national infrastructure and provide an adequate cyber response function regarding national security. Within the region, given the concentrated presence of cyber security businesses and critical national infrastructure, there is a fundamental need to address these gaps and to ensure a sustainable model for the growth of UK cyber security.

This audit has identified the following core gaps that must be considered in future interventions to support the sector within the region.

Development of Skills & Talent:

We are struggling to attract people with the correct experience and skillsets in cyber security.” (Gloucestershire SME involved in IT infrastructure security)

Several of the SME cyber security firms in the region consulted throughout this Audit process highlighted the significant gap in the region regarding a skills shortage. As reflected in Section 5.4, there are hundreds of unfilled vacancies in the region within cyber security. This is for several reasons, including:

- The perception that the City of London has the ‘pull’ to attract some of the nation’s best talent, leaving other parts of the UK with more limited potential for recruitment. This highlights the need to showcase the Cyber Resilience Alliance region as attractive to live and work in;
- A perceived gap within the skills accredited (Level 7+) and the applied and commercial skills required by businesses;
- Demand for labour considerably exceeds supply: this is creating a labour market with salary costs potentially prohibitive to new innovative start-ups (e.g. salaries in the region of £50,000+ for staff with one to two years’ experience);
- The current provision of skills and talent (formal university / higher education, and conversion courses and training schemes) offers a strong model to address many of these gaps, with the Universities of Gloucestershire, Worcester and Wolverhampton taking welcome steps to grow the talent pipeline; however, given the sector’s robust growth, there is a gap between what is needed and what can be produced.

Consultees did note, however, that the Cyber Resilience Alliance region is not the only cyber security cluster vying for cyber security specialists, commenting on the need for the region to vie with talent across the entire UK.
Provision of Facilities and Infrastructure: Reflect the Breadth & Diversity of the Sector:

This Audit has identified the wide range of funding and infrastructure initiatives across the region and wider UK for cyber security. The region is host to several of the UK’s leading examples of cyber security incubation and acceleration including the Wyche Innovation Centre, and the national GCHQ Cyber Accelerator programme. There are also several planned investments in cyber security infrastructure over the next few years to support sectoral growth including the Cheltenham Cyber Park, and the Marches Centre for Cyber Security. However, several consultations in the region have indicated that within the sector, investment in infrastructure has focused upon schemes supported by government and security agencies. Whilst this is welcome in growing the sector, it is viewed that there are gaps in:

• **Availability and Affordability of Grade A Office Space (all sizes):** As set out by Savills, cyber security firms are set to take up to one million sq. ft in office space across the UK by 2022. Given the demand within the sector, combined with the need for firms to ensure working space that complies with their respective standards and accreditation (ISO 27001, Cyber Essentials etc), many consultees have identified the perceived shortage of high quality office space at all levels (for small to large teams), and the prohibitive costs associated with office rental. Increasing the supply, particularly around clusters, will relieve increasing office costs, and also enable collaboration between adjacent firms – thereby supporting the region’s ambition to rapidly grow the sector.

• **Provision of Product Testing and Validation Labs:** One essential process within the industry is testing products and services to provide greater assurance to consumers of the overall validity of the product being offered. As such, there are several testing labs/facilities across the UK, providing CTAS and CHECK testing accreditations which identify any weaknesses utilising publicly known vulnerabilities and common configuration faults. However, joining these schemes can be prohibitively expensive for SMEs, and take up is therefore viewed not as high as it could be with the provision of support.

NCSC has released several certified product schemes which test the validity of cyber security products and services, providing greater assurance to consumers of the reliability and effectiveness of the products they purchase, including Commercial Product Assurance, Commercial Evaluation Facilities, Commodity Information Assurance Services, Tailored Evaluation, and TEMPEST and EMS (see Appendix J).

However, some consultees argue that there is a gap that exists for an independent body to provide testing and validation labs in the region. This would enable private firms to test their products in a space that would not necessitate a standard approach i.e. sharing all relevant code or IP with a national body (see Proposal 1 – National Cyber Lab).

There is also a perceived gap that internationally – investment in UK cyber security is often conflated with London, and that the region will need to invest in a coherent vision, brand and message to promote the area as a highly attractive location for living and working.
Key Ambitions and Proposals for Growth

To best tackle the gaps within the region’s cyber security sector, and to take advantage of the opportunities provided by technological transformation, this section sets out our key proposals and suggested interventions for the region.

Across the four Local Enterprise Partnerships, we estimate a financial commitment to the sector over the next five years in the region of £80m (£16m per annum)\(^\text{10}\)

Proposal 1: Innovation, Research & Development | Investing in Infrastructure

Business Expenditure on Research and Development (BERD) within the region has been increasing in recent years, and this is arguably being driven by several large manufacturing and automotive firms within the West Midlands and South West of England. There is therefore considerable potential to utilise existing clusters and networks between these firms and innovative cyber start-ups in the region to provide commercial opportunities, and to accelerate growth.

Further, the Cyber Resilience Alliance will encourage strong utilisation of upcoming investments in cyber security infrastructure, given the expectation that such initiatives (e.g. Cheltenham Cyber Park and the Marches Centre for Cyber Security) will result in increased innovation and collaboration between newly established innovative spin-outs and start-ups.

To further enable innovation and encourage continued investment in Research and Development (R&D) in the region, the Cyber Resilience Alliance propose:

1. **Promoting Existing Infrastructure Expenditure:** The region must ensure that recent proposed investments are maintained and supported; however, these must also receive investment to join-up initiatives across the region e.g. to identify the best possible incubation space for new firms depending upon their capability, capital and ambitions. Any fragmentation of cyber security infrastructure in the region may cause a disjointed approach to seeking investment for the region.

2. **New Infrastructure: ‘National Cyber Lab’:** The Audit has confirmed the initial requirement for exploring the feasibility and potential investment in a ‘new specialised data centre with a flexible cyber range and dirty lab to offer organisations the chance to engage and use these facilities in the development of cyber technology and cyber defence’ which can be industry-driven.

Given the proximity of government schemes and NCSC validation facilities, this could be scoped to become a centre of national significance e.g. a National Cyber Lab, with potential sites across the wider region – linking into wider infrastructure in the region e.g. Berkeley C11 Cyber Security Centre testing labs for University of Gloucestershire students, and the launch of UK Cloud’s UKCloudX\(^\text{11}\) service in the region (a dedicated facility which provides High Assurance cloud provision for defence and government). Membership of this centre would not only allow access to the sites but also access the subject matter experts and a

\(\text{10}\) See Annex A (Business Cases) for further detail and rationale.

\(\text{11}\) See [https://ukcloudx.com/](https://ukcloudx.com/)
collaborative environment where partnerships could be formed to chase the larger programmes and research funding. It would further allow access to cyber skills from the traditional industrial base. This could provide the potential for international recognition of the cluster (having industry-led testing facilities with international standards to encourage product exports). This would reflect a significant financial commitment by the region to supporting the cyber security centre.

3. **Sustained Investment in Aligned Technology:** Increased investment and adoption of innovative technologies in the region e.g. Worcestershire 5G test bed, provides regional firms with significant gains in productivity, but simultaneously requires cyber security support given the proliferation in devices and data. This provides real opportunity for sectoral growth – where the Cyber Resilience Alliance is a technological world-leader, **being a world-leader in securing these technologies is a natural extension.**

**Proposal 2: Encouraging Sustainable Demand:**

We will support interventions that promote the growth of the cyber security sector through domestic and export sales, and through the provision of innovative new products and technologies.

We identify the following mechanism to support this proposal:

4. **Encouraging Regional Demand:** It is the view of this Audit that the region is home to world-leading and innovative expertise. However, there remains a view by regional stakeholders that London is considered internationally as central to the UK’s cyber security activity.

It is therefore crucial to provide a narrative that encourages growth at the regional level, through:

- **Highlighting the strengths, offer and capabilities of the region’s cyber security expertise** through investment in suitable marketing, and schemes such as ‘Meet the Buyer’, Knowledge Transfer Partnerships, and sharing examples of how cyber security in the region can benefit a range of sectors e.g. agri-food, manufacturing and automotive. This could include sponsoring cyber security clusters within the region to engage with wider sectoral groups (automotive, aerospace, manufacturing, agri-food);

- Utilising the existing Local Enterprise Partnership structures to **identify opportunities to bring together cyber security firms and businesses in need of secure solutions**;

- Promoting a **marketing narrative emphasising the strengths of the region as a suitable location for cyber security investment and employment**, including space, affordable housing, high living standards, transport access and infrastructure, availability of talent, and **close proximity to bodies of national significance** in cyber security (GCHQ, MoD) and Academic Centres of Excellence in Cyber Security and active cyber security universities.
Proposal 3: Improving Skills and Talent:
For any sector to be successful, it requires a sufficient and skilled workforce. The cyber security sector has experienced considerable skills and talent shortage in recent years, and this has been reflected within remuneration levels and the extent of unfilled vacancies within the sector.

However, there is substantial demand within the sector, that can facilitate high-value employment within the region where the skills and talent are invested in sufficiently to a) increase supply of labour and b) increase the skills being requested by industry. The Cyber Resilience Alliance therefore propose to:

5. Facilitate Workforce Planning in the Cyber Security Sector for the Region: We propose within the Cyber Resilience Alliance to establish a working group to monitor labour supply and demand in the region to enable targeted investment and interventions. This will need to consist of regional decision-makers involved in education (across all levels), business, government and the third sector.

Further, there is compelling evidence within the region that reskilling and lifelong learning initiatives work well in meeting labour shortages and encouraging new talent into the sector. Indeed, the region’s strength in national defence and security provides cyber security as a natural career progression for many of our long-term serving personnel and provides new perspective and innovation in the sector. We will seek to encourage initiatives that encourage neurodiversity in the sector (such as the Community Cyber Operations Centre), that attract younger talent to get involved in cyber security (e.g. Cyber Schools Programme), and those schemes that seek to move people away from potential cyber-crime into security roles.

6. The Cyber Resilience Alliance is a prime location for innovative approaches in encouraging new talent into the sector, and we will monitor and seek to support funding requirements accordingly given the potential for significant increases in regional productivity as a result of increased sectoral employment.

7. Finally, the Cyber Resilience Alliance is home to several university accredited courses in cyber security. There are also several universities adjacent to the region that offer courses in cyber security including University of Warwick, University of Birmingham, University of Bristol, Bath Spa, and University of South Wales – demonstrating the importance of neighbouring institutions. There has been considerable growth and interest in cyber security courses in the region. We propose that the region has potential to become home to one of the UK’s first ‘Centres of Excellence in Education within Cyber Security’, similar to the EPSRC accredited Academic Centres of Excellence in Cyber Security Research (or the National Security Agency (NSA) /Department of Homeland Security (DHS) Centers of Academic Excellence in Cyber Defence program12) - which receive international acclaim, yet focus on how to teach cyber security in an applied format of benefit to employers in the region such as Raytheon, BT, Lockheed Martin and QinetiQ and support ‘life-long learning’ in the region.

---

12 [https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/](https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/)
Proposal 4: Focused Marketing & Sector Targeting:

The Audit has also validated that cyber security clusters work where there is a clear awareness of the anchor-driven strengths to encourage talent and investment to flow into the region. Within the Cyber Resilience Alliance, there is national and international recognition that cyber security activity is strong; however, there is a risk that this can become disjointed through recognition of several smaller clusters contained within e.g. Malvern, Gloucestershire, Cheltenham, and Wiltshire etc. Indeed, the geography of the region can also often mean that the West Midlands and South West can be assumed to mean ‘Birmingham’ and ‘Bristol’ respectively; which presents a challenge to the region regarding being known on the map.

This evidences the need for the Cyber Resilience Alliance to establish a unified consortium, brand and approach to attract investment and talent.

We propose to:

8. Sustain a Cyber Resilience Alliance representative body, combining representation from each of the four Local Enterprise Partnerships (government, business and academia), to promote the sector. The management and governance of this body could be agreed in consultation with local, regional, and national government bodies.

9. Establish a Cyber Resilience Alliance website / dedicated support to demonstrate how a start-up / SME / large multinational can do business in the region (e.g. access to space, labour, grants and loans, R&D tax credits, university / research support) to ensure coherency;

10. Establish formal Cluster Partnerships, potentially ‘twinning’ the Cyber Resilience Region with comparable initiatives in the United States or other countries with prominent or emergent sectors (e.g. Israel, China, or Brazil);

11. Marketing: Promote the region as a high-growth location with a growing and talented labour supply, with support from LEPs to invest, start and grow – where firms will be surrounded by other world-leading innovative firms and public bodies (drawing upon the Midlands Engine Cyber momentum).

12. Intelligent sectoral targeting: The Cyber Resilience Alliance will identify and track firms active in sectors aligned to the four LEPs growth priorities (manufacturing, agri-food, professional services) in addition to export potential (Government, Financial Services, Energy and CNI, Healthcare, and Infrastructure), and will identify their respective approach to cyber security (spending, research, relationships with regional suppliers etc.).

13. Enhancing Opportunities for Investment: We will explore opportunities to bring more events, and conferences (and specialist VC investors) to the region to showcase the talent and expertise of the region.
Networking and Collaboration

The consortium delivering this audit brings together a wide range of academic, research, innovation and commercial strengths in the fields of cyber security and economic development.

It is led by Worcestershire Local Enterprise Partnership with support from Gloucestershire, Swindon & Wiltshire and The Marches LEPs, and has focused on the needs of the research and business community within cyber security, through concentrating on the economic impact, exploitation, and investment potential of cyber capabilities and capacity across the region, while taking cognisance of academic teaching, and IP generation as underpinning elements.

Throughout this process, the Science and Innovation Audit received written or verbal evidence from over sixty leading members of business, academic and public bodies. These contributions are greatly appreciated by the Cyber Resilience Alliance, and have been an valuable call to action for the region.

The Cyber Resilience Alliance have also utilised this exercise to promote collaborative and joint-up initiatives across the region in cyber security and beyond. This includes:

- The Cyber Valley marketing initiative being supported by the Midlands Engine Cyber necessitating close co-operation between Skylon Park, Marches LEP, and Worcestershire LEP who have been leading the initiative. This also means that the trade partnership within Cyber Maryland are aware of the Cyber Resilience Alliance concept, and collaboration being undertaken to grow the region;
- Cheltenham will host the National Cyber Awards 2018 in November, supported by the Cyber Trust, Cyber Security Challenge, and GFirst LEP. This event rewards those who are committed to cyber innovation, cyber crime reduction and protecting the citizen online, and has been supported through relationships developed as a result of this SIA.
- The four Local Enterprise Partnerships involved within this exercise are committed to work collaboratively to identify, share and learn from interventions and infrastructure investment in the region. This means sharing ideas, innovation and working space to give companies in the region the best opportunities to grow.

Further, the Cyber Resilience Alliance will work as closely as possible with other SIA regions to identify opportunities to grow the wider UK cyber security sector. It is considered that this SIA is particular complementory to the Midlands Engine SIA (Wave 1), Innovation South (Wave 2), Oxfordshire Transformative Technologies (Wave 2), and Applied Digital Technologies, South Wales Crucible, and Upstream Space SIAs (Wave 3).