Perspective
Economics

The North West Cyber Corridor

Innovation Impact Study: Evidence Base (2023)

Contents

01 Executive Summary

This research report provides an evidence base and a call to action to support growth in the North West, through building on its existing strategic advantages and maximising opportunities in cyber security and digital. The key findings are set out below.

BUSINESS LANDSCAPE / ASSETS:

The North West has approximately 300 unique cyber security companies, making it one of the UK's leading regions in cyber. There is strong complementarity between the region's cyber capabilities and other sectors, including aerospace and defence, energy and nuclear, finance, and professional services, and manufacturing.

There are also over 150 public, defence, and research assets identified across the North West (e.g. business clusters in Greater Manchester (GM), research excellence in Lancaster, upcoming National Cyber Force (NCF) / innovation in Samlesbury, cyber degree apprenticeships in Sellafield, High Performance Computing (HPC) capabilities in Hartree Centre at Daresbury etc, Smart Cities in Liverpool City Region (LCR) etc).

52% of cyber security companies are 'pure-play' (i.e. only provide cyber security e.g. NCC Group, Darktrace, Avecto, WithSecure, ProofID, Secarma), and 48% are 'diversified' and offer products and services across several verticals. This is much higher than the UK study (28% diversified) which highlights how strongly cyber security capabilities are embedded within broader sectors in the North West (e.g. with providers such as BAE Systems, BT, Cisco, Deloitte, PwC, Accenture, Ericsson, Thales, Capgemini, ARM, Raytheon). Over a third of cyber security employers are either large (250+ staff) or medium (50+ staff). This suggests opportunity to build the skills pipeline through entry-level pathways into cyber among key employers, including the NCF and NCSC.

ECONOMIC POTENTIAL

We estimate there are currently c. 12,000 FTEs (across all sectors) working in cyber security in the North West (generating over £550m in annual salaries, and £760m in GVA each year). Growth estimates suggest the region should be aiming to grow the cyber security ecosystem with c. 30,000 FTEs by 2035. Achieving this could unlock up to £2.7bn per annum in Gross Value Added for the North West economy, and could cumulatively generate £22.4bn in GVA for the North West between 2022 – 2035.

SKILLS:

The North West contains 10 HEIs offering cyber security and computer science courses, placing it as a top region for skills provision. The number of graduates in the region in cyber and computer science is growing by c. 15% per annum, with more than 3,400 graduates in 2020/21. However, there is a need for skills and workforce planning across the region identified by the study, that suggests the region should increase its training provision in cyber related courses and initiatives by at least 1,000 people per annum[1] to meet the growth scenarios.

[1] Based on the annual estimated UK cyber workforce gap within the DSIT Cyber Skills in the UK research project of c. 11,000 individuals per annum.

Next Steps

01

Develop an agreed governance structure and strategy for the North West Cyber Corridor

In 2021, the government set out its plans to support the development of a 'Cyber Corridor' across the North West, driven by the establishment of the National Cyber Force in Lancashire.

This report evidences that there is a substantive baseline to build upon; however, it is now essential to develop an identity and structure for the Cyber Corridor initiative. The partners within the current working group should now consider the next steps to establish an agreed governance structure (encompassing regional and sub-regional leaders across public and private sectors and academia), as well as developing an initial strategy and actions for the Cyber Corridor.

02

Build a coalition of cyber security ecosystem partners

The region is home for five distinct sub-regions, all with varying cyber security strengths, capabilities and interests. We recommend that the group confirms its geographic parameters, and widens its membership structure to ensure participation from stakeholders across the region in the Cyber Corridor initiative.

03

Develop a Growth Strategy

This report provides some initial targets for growth, including reaching 30,000 FTEs by 2035, and for the cyber security ecosystem to drive c. £2.7bn in GVA per annum.

However, this will require a Growth Strategy, with consideration of areas for co-investment, skills initiatives, and identifying priority areas for intervention and support from local, regional and national partners. This should also ensure that the Cyber Corridor is well connected to national initiatives, and has a number of projects in relation to infrastructure, skills, and ecosystem ready to commit funding and participation against.

04

Establish actions across a number of distinct themes

We also recommend that the Cyber Corridor commits to actions against a number of agreed thematic areas – to ensure that stakeholders can best support impactful projects. This might include Ecosystem Development, Skills, Research and Innovation, and Diversity.

05

Brand, Identity, and Vision

The Cyber Corridor initiative will require a distinct brand and identity, and have an agreed vision to enable a successful ecosystem. The group should explore perceptions of the 'Corridor' initiative, and test whether this resonates with potential stakeholders – or if the description could be varied to allow for full engagement across the North West, whilst ensuring equitable access and participation across sub-regions.

06

Resourcing

It is also important that the Cyber Corridor initiative has sufficient resourcing following strategy development. This could include outreach and engagement roles to ensure that businesses, public sector, and academic organisations advancing the cyber security ecosystem are well engaged and participating together.

02
Introduction and Background

Perspective Economics was commissioned by Lancaster University (in collaboration with Plexal) to support in the development of an evidence base and strategic outline for the North West Cyber Corridor project. **This study covers the region of the North West of England.**

This research explores the assets, initiatives, and potential of the region with respect to its cyber security ecosystem. This includes an analysis of the region's economic assets, research and development, innovation, and skills landscape. This report has been commissioned following the recent announcement that Samlesbury will host the UK's National Cyber Force (NCF), cementing the North West's place as a leading region for cyber security activity. The NCF draws together personnel from GCHQ, the MoD, the Secret Intelligence Service (MI6) and the Defence, Science and Technology Laboratory (DSTL), under one unified command for the first time.

This is therefore a significant moment for the North West and all of its stakeholders, as it seeks to build upon this investment in cyber security and secure digitalisation in the coming decade.

In 2021, the government set out its plans to support the development of a 'cyber corridor' across the North West, driven by the establishment of the National Cyber Force in Lancashire.

> "
>
> This research explores the assets, initiatives, and potential of the region with respect to its cyber security ecosystem.

THIS REPORT PROVIDES:

- A **baseline exercise** for the North West Cyber Corridor, setting out the business landscape, cyber security assets, research and innovation, defence and national security, and an analysis of labour market demand and supply of cyber security talent in the region.
- The **strategic context**, exploring why the Cyber Corridor matters for the region.
- Undertaking of **benchmarking** for the region.
- Analysis of the **opportunities** that the Cyber Corridor provides
- Provision of **recommendations and strategy** for growing cyber security in the region.

The North West has a well-established cyber security ecosystem and has rapidly become a destination of choice for several large employers, across public and private sectors. It includes established companies such as Raytheon, BAE Systems Applied Intelligence, Northrop Grumann, Deloitte, PwC, KPMG, Sophos, Darktrace, AON, and NCC Group. In 2019, GCHQ opened new site in Heron House in Manchester, and has plans to grow to up to 1,000 staff. In 2022, the DiSHmcr (Digital Security Innovation Hub) opened, which is co-located at Heron House with GCHQ, and will be led by Barclays Eagle Labs, Plexal, Lancaster University and the University of Manchester.

This research further evidences the role of the region's cyber security ecosystem. We find over 150 public assets including eleven universities offering higher education level courses in cyber security (or similar), and approximately 300 cyber security businesses active in the region. However, there are many challenges that come with growing a cyber security ecosystem; namely, developing a skills pipeline and ensuring access to talent across the region. As such, this research explores the extent of cyber skills in the region, and provides a series of indicative targets and ambitions to best take advantage of the growing demand for cyber.

There are significant opportunities in the years ahead for the North West. The National Cyber Force announcement is key in the ambitions over the coming years, particularly with the ambition for the NCF to provide more than 3,000 roles in the region. This must be met with ensuring growth for all businesses and organisations in the North West, developing a skilled pipeline of talent at many levels, and ensuring equal access to opportunities to all people in the region.

An effective North West Cyber Corridor project will be able to bring together commercial ingenuity, public investment in skills, talent, and infrastructure, and the need for the UK to enhance its national defence and strategic advantage – all in one place.

This exercise will enable key stakeholders to understand the strengths, weaknesses, opportunities, and threats for the region, and will inform the design and implementation of the Cyber Corridor project in the coming months.

We hope that this research acts as both an informative baseline, and a stimulant for collaboration in the years ahead.

03
The North West Cyber Corridor

3.1 INTRODUCTION

This research explores cyber security related activity and potential across the entire North West of England. The Cyber Corridor spans the entirety of the North West, with extensive assets and initiatives already established particularly in the geographic 'corridor' between Lancaster and Manchester, but also in Liverpool City Region, Cumbria, and Cheshire and Warrington.

3.2 GEOGRAPHY, POPULATION, AND ECONOMY

GEOGRAPHY

The North West of England consists of five administrative countries: Cheshire, Cumbria, Greater Manchester, Lancashire, and Merseyside. There are also five Local Enterprise Partnerships (LEPs)[2] in the region: Cheshire & Warrington, Cumbria, Lancashire, Greater Manchester, and Liverpool City Region. These sub-regions are displayed in the map in Appendix A.

The Cyber Corridor is also home to the North West Cyber Security Cluster, one of UKC3's recognised regional clusters. There are a multitude of existing partnerships and collaborations that will help the development of the Cyber Corridor, such as:

- Centre for Digital Trust and Society: Security and Trust Partnership – GCHQ partnership with Lancaster University, the University of Manchester, Manchester Metropolitan University, and the University of Salford.
- Digital Innovation and Security Hub (DiSH) – a 11,000 sq ft cyber security hub at Heron House, together with GCHQ, the National Cyber Security Centre, and consortium partners from Barclays Eagle Labs, Plexal, Lancaster University and the University of Manchester.
- Cyber Foundry – a partnership between Lancaster University, the University of Manchester, Manchester Metropolitan University, and the University of Salford.
- SPRITE+ – led by five universities: University of Manchester (lead institution), Imperial College London, Lancaster University, Queen's University Belfast, and University of Southampton

POPULATION

The North West is the third most populated region in the UK. The region has a population of 7.4 million, and the most densely populated cities in the region are Manchester and Liverpool.

The 2021 Census found that the North West population has grown by 5.2% since 2011, slightly lower than the rate of growth across England (6.6%).

Salford has had the largest population increase at 15.4%, followed by Chorley (9.9%) and Manchester (9.7%). Lancaster's population grew by less at 3.3%, and Blackpool, Barrow-in-Furness, and Copeland all experienced negative population growth over the ten years.[3] The North West population is anticipated to grow by 4.4% between 2021 and 2035.

This data highlights two key implications for economic development in the region:

- The crucial role of investment and regeneration in stimulating local economies. The rapid population growth in Salford can arguably be linked to the BBC's move to MediaCity UK in 2011, and growth in residential and commercial property construction.
- The need for Levelling Up and maximising opportunities across local authorities. The North West is also home to many local areas that have declined in recent decades, due to a combination of changing economic conditions and demographic factors. However, there are industrial opportunities for these regions with the right mix of investment and skills support. Investment in defence, nuclear, and manufacturing in areas such as Barrow-in-Furness can act as a catalyst for regeneration and growth through high-paying roles. For example, BAE Systems is seeking to hire 1,200 additional people in Barrow to work on the Royal Navy's new generation of submarines, and will generate positive spill-overs for the region.

[2] LEP Network (2022) The 38 LEPs. Available at: https://www.lepnetwork.net/about-leps/the-38-leps/

[3] https://www.ons.gov.uk/visualisations/censusareachanges/

ECONOMY

KEY STATISTICS:

- The North West contributes an estimated £228.3 billion to the UK economy (10% of the UK) making the region the largest regional UK economy outside of London and the South East.
- There are 271,000 businesses in the region (2022). 89% of these businesses are micro (i.e. 1-9 FTEs), 9% small (10-49 FTEs), 1.6% are medium (50-249 FTEs), and 0.4% are large enterprises (>250 FTEs).
- Analysis of business data within the North West highlights the region's notable strengths in manufacturing, energy, financial and professional services. There are also relative strengths in each of the sub-regions, explored within subsequent sections of this report (e.g. nuclear in Cumbria, advanced manufacturing in Lancashire, life sciences in Liverpool City Region, digital economy in Manchester City Region, professional services in Warrington and Cheshire etc). alongside significant research activity across the region.
- However, this data also highlights that in employment terms, sectors such as information and communication, and public administration and defence are lagging the national average. For example, the LQ analysis (see Appendix B) suggests that the North West has approximately 54,000 fewer people working in information and communication than would be expected if it were in line with the UK average. However, this also reflects an opportunity to both enhance digitisation within dominant sectors, as well as explore opportunities for investment in job creation in digital roles.
- Whilst the digital sector makes up approximately 5% of the North West economy, it has outgrown the wider regional economy (with typical annual growth of 4.8% per annum between 2014 – 2019). DSIT (Formally DCMS) (2022) 'Assessing the UK Regional Digital Ecosystems' research found that 'digital employment, estimated at 200,000 in 2019, is weighted towards digital occupations in businesses not traditionally in the Digital Sector, indicative of higher demand for digital skills in non-digital sector industries'.
- This highlights the need for the North West to build its digital economy through both growing its core digital sector, and through embedding digital roles within all economic sectors.

The sub-sections below provide a summary of the strengths and key digital metrics for each sub-region in the North West economy.

LANCASHIRE

- Lancashire has a £34bn economy, and is home to 1.5m people, including 52,000 businesses employing over 600,000 people[4].
- It is well recognised and regarded for its strengths in advanced manufacturing, electronics, energy, automotive, and food production. In addition, it is home to the UK's largest aerospace cluster, with more than 500 businesses.
- These strengths mean that Lancashire, through public, private and academic collaboration, is pursing opportunities in areas such as cyber security, robotics, 5G, mobility, renewables, AgriTech, and ElecTech.
- Lancashire has world-leading expertise in cyber security, driven by the role of Lancaster University, which is an NCSC accredited Academic Centre of Excellence in Cyber Security Research. The region also is focused on increasing the skills supply pipeline, as Lancaster University, UCLan and Edge Hill produce over 1,000 graduates a year with relevant computing and engineering experience.

GREATER MANCHESTER

- Greater Manchester was named in the 2020 Tech Nation report as the fastest-growing major tech cluster in Europe. The digital, creative and technology sector consists of around 10,000 businesses employing 86,000 people and contributing around £5 billion a year to the city's economy.
- Manchester tech companies raised a record £532 million of funding in 2022[5], a 50 per cent increase on 2021 levels. Manchester-based companies have collectively raised over £1.8 billion in venture capital funding in the past five years.
- Greater Manchester has particular strengths in areas such as creative and media, FinTech, eCommerce and HealthTech. Manchester's labour market is demonstrating strong demand for cyber security professionals (explored in Section 5), and this is set to increase with recent investments into the area by GCHQ. Further, there is strong capacity to build upon this demand with core employers across a range of sectors such as Google, Cisco, Booking.com, KPMG, Amazon, and TalkTalk.

[4] Lancashire Digital Economy Report 2021
[5] Invest in Manchester (2023)

CHESHIRE & WARRINGTON

- Cheshire and Warrington has a particularly strong manufacturing and advanced engineering sector, driving 23% of the subregion's economy. This is approximately two and a half times larger than the national average, and is responsible for a quarter of the North West's manufacturing sector.
- It also is strong in chemicals, life sciences, energy, and finance and hosts employers such as Siemens, Barclays and AstraZeneca.

LIVERPOOL CITY REGION

- Liverpool City Region is a £33bn economy (GVA), with particular specialisms in advanced manufacturing, health and life sciences, digital and creative sectors.
- As set out in the LCR Digital Strategy and Action Plan (2021-23), the region is home to a 'fast-growing cluster of distinctive tech', including Sensor City (a dedicated IoT incubator), and major tech companies such as IBM, Atos, and Unilever at Port Sunlight.
- Liverpool City Region has an ambitious target (set out in its Economic Recovery Plan) for R&D investment to reach 5% of its GVA (twice the UK target of 2.4%) by 2027.
- The region is also home to the Science and Technology Facilities Council (STFC) Hartree Centre and the Daresbury Laboratory, based at Sci-Tech Daresbury. This is home to SuperSTEM and SuperSTEM3 – two of the world's highest resolution electron microscopes. It also hosts the Innovation Centre, a 24,000 sq ft centre with over 70 high-tech companies from life sciences, digital and engineering sectors, and has a strong partnership with IBM Research.

CUMBRIA

- Cumbria has a £12bn economy (GVA), and is home to over 23,000 businesses, typically concentrated in manufacturing, accommodation and food.
- The county has particular expertise in nuclear, and this is reflected by the role of Sellafield and Low Level Waste Repository (LLWR), which employ over 12,000 workers and support over £700m in direct GVA to the region.
- Cyber security is a crucial programme for Sellafield Ltd, which works with its parent company, the Nuclear Decommissioning Authority (NDA) to invest in cyber security capability and skills. The NDA is expected to invest £80m over the next five years in cyber security[6], and plays a particularly important role in cyber. Sellafield will also attract approximately 300 apprentices in 2023, including within cyber security.

[6] https://www.prospectmagazine.co.uk/sponsored/cyber-security-at-sellafield-nuclear-energy

04
Strategic Context

4.1
INTRODUCTION

Cyber security has become an area of strategic significance for the UK, as it seeks to both protect and promote its interests in a landscape that's being reshaped by technology, whilst also identifying new economic opportunities that can be maximised through a strong cyber security sector, and robust sectors across the economy.

Cyber security has become an area of strategic significance for the UK, as it seeks to both protect and promote its interests in a landscape that's being reshaped by technology, whilst also identifying new economic opportunities that can be maximised through a strong cyber security sector, and robust sectors across the economy.

Whilst the UK is considered one of the world's leading cyber powers (alongside the United States and Israel), there is an opportunity to address several challenges such as the pronounced skills shortage and ensuring capability in cyber defence and offensive cyber operations. This is particularly noted within the Levelling Up Agenda, whereby it is essential to by spreading job opportunities across the country and move key public sector roles outside of London.

The North West Cyber Corridor builds upon the already existing regional strength in cyber security. Establishing the Cyber Corridor provides incentive for further investment in the area, supporting the wider NCF investment in excess of £5 billion by 2030.

> "The North West Cyber Corridor builds upon the already existing regional strength in cyber security."

4.2 STRATEGIC ALIGNMENT

The Cyber Corridor project will complement a range of other policies, strategies, and action plans across the North West and the UK as a whole. We set out some of these key strategies below.

NATIONAL

- Levelling Up the United Kingdom (2022)
- National Cyber Strategy (2022)
- Government Cyber Security Strategy (2022 – 2030)
- Project Gigabit (2022)
- Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy (2021), Refreshed in 2023

REGIONAL

Local Industrial Strategies

- Greater Manchester Local Industrial Strategy (2019)
- Lancashire Local Industrial Strategy
- Liverpool City Region Combined Authority Local Industrial Strategy (2020)
- Cheshire & Warrington Local Industrial Strategy (2019)
- Cumbria LEP Local Industrial Strategy (2019)

Digital Strategies

- Greater Manchester – Doing Digital Differently (2022)
- Lancashire Digital Strategy (2022)
- Liverpool City Region Digital Strategy (2021-2023)
- Cheshire and Warrington Digital Strategy (2019) & Digital Infrastructure Plan (2019)
- Cumbria LEP Digital Strategy & Digital Infrastructure Plan

LOCAL

There are also a number of ongoing strategic investments in cyber security within the region, in addition to the NCF site at Samlesbury, including:

- Manchester's Digital Innovation and Security Hub (DiSH), a £10m cyber security innovation centre, co-located with GCHQ and NCSC at Heron House.
- The North West Cyber Resilience Centre, a joint venture between GM Police and Manchester Digital.

- The GM and Lancashire Cyber Foundry projects, a £6m initiative focused on secure digitalisation projects to support SMEs across GM and Lancashire, with partnership between Lancaster University, University of Manchester, University of Salford, and Manchester Metropolitan University.
- HOST Cyber, in partnership with Salford City Council provides an affordable 24/7 SOC to SMEs, and is supported by partnerships with GCHQ, Cyber Foundry, and the region's universities.
- Lancaster University's recent £19m investment in the Security and Protection Science at Lancaster Initiative, and its backing for the Electech Innovation Cluster in the Morecambe Bay and South Lakes area, to build on Lancashire and Cumbria's excellence in electronics.

4.2 STRATEGIC AMBITIONS

As set out, there are several strategies, policies and investments across the North West which aim to advance growth and innovation, particularly through the region's cyber security capabilities. The North West Cyber Corridor must therefore be cognisant of the following factors, and these are explored within subsequent chapters of this evidence base review:

FACTOR	SECTIONS
Developing a robust cyber security ecosystem baseline:	
The North West is frequently cited within the DSIT Cyber Security Sectoral Analysis as a hotspot for cyber security activity. However, it is crucial to develop and refine a more detailed baseline of cyber security activity across all sectors, as well as understand the granular and unique strengths and opportunities across the North West (and its five sub-regions).	**Section 5: Evidence Baseline** explores the number of cyber security businesses and assets in the region, and considers their economic contribution. **Section 6: Benchmarking** explores how the size of the North West cyber ecosystem compares to other regions (in the UK and elsewhere) as well as mapping hotspots within the North West itself. **Section 7: Economic Potential** explores potential growth scenarios and KPIs for the North West over the coming decade.
The role of skills: Supply, Demand and Workforce Gap:	
There are three key questions for the region: - How much cyber security talent is employed in the region? - What is the demand and opportunity for the cyber security related workforce? - How much additional talent is required, and what initiatives can support the region to close the cyber workforce gap?	**Section 5: Evidence Baseline** explores the supply and demand for cyber security talent in the region. **Section 6: Benchmarking** explores the demand for professionals in the North West, and also explores the supply of talent compared to other regions. **Section 7: Economic Potential** explores how the cyber security ecosystem can grow over the coming decade, and implications for skills and workforce planning.
Innovation and R&D	
The North West is home to several universities offering cyber security courses and world-leading research. It is contains several research assets and R&D intensive businesses. This report explores the extent of innovation, R&D, academic excellence, and collaboration in cyber security in the region.	**Section 5: Evidence Baseline** explores the research and innovation strengths within the region. It also explores the role of advancing innovation and R&D among key assets in the region, and advancing secure digitalisation.
Defence and National Security	
The North West is at the heart of the UK's national defence and security ecosystem. The region is home to the GCHQ, NCSC, MoD, national intelligence, and will host the National Cyber Force at Samlesbury. Defence sustains an estimated 35,000 jobs in the region, including c. 10,000 roles at BAE Systems in Barrow, and 12,000 in advanced aerospace in the Samlesbury Aerospace Enterprise Zone.	**Section 5:** explores the role of defence and national security within the region, and the increasing need for cyber security skills within the defence and public sector.
Advancing Secure Digitalisation:	
The region is home to particular strengths in manufacturing, electronics, professional services, and finance. There is clear opportunity for secure digitalisation across dominant 'traditional' sectors, to both help increase security in these sectors, but also provide commercial opportunities for managed security services providers in the region.	**Sections 8 and 9** set out a Gap Analysis and Recommendations for the region, including how and where opportunities exist for the Cyber Corridor to embed cyber security within all sectors across the region.

05
Evidence Baseline

5.1
INTRODUCTION

This chapter provides an evidence baseline for the North West's cyber security ecosystem.It sets out the region's assets, businesses, and education institutions.

This analysis is informed through a deep-dive review of regional data, including analysis comparable to the DSIT Cyber Security Sectoral Analysis (2023) and Cyber Skills in the UK Labour Market (2023).

A strong cyber security ecosystem is fundamental to the growth of any modern digital economy. This chapter explores the current position of the ecosystem, and informs subsequent growth estimates for the region over the next decade.

5.2 BASELINING THE CYBER SECURITY ECOSYSTEM

There are a range of metrics that can be used to explore the size, scale and potential for the region's cyber security ecosystem.

This includes:

- Identifying Cyber Security Businesses in the North West
  - Number and Location of Active Cyber Security Businesses and Offices
  - Economic contribution of the cyber security sector (through revenue, Gross Value Added, and employment)
  - Type of cyber security businesses in the region, and core specialisms
  - Levels of investment (e.g. external investment raised, foreign direct investment) and R&D participation
- Identifying aligned industries and sectors in the region with demand for cyber security products, services and talent
- Identifying Research and Public Assets relevant to the cyber security ecosystem (e.g. the role of the public sector, defence, universities, colleges, and research initiatives).
- Understanding the supply and demand for cyber security talent in the region, through exploration of vacancy data, and supply of graduates, apprenticeships, and retraining initiatives.

5.3 CYBER SECURITY BUSINESSES IN THE NORTH WEST

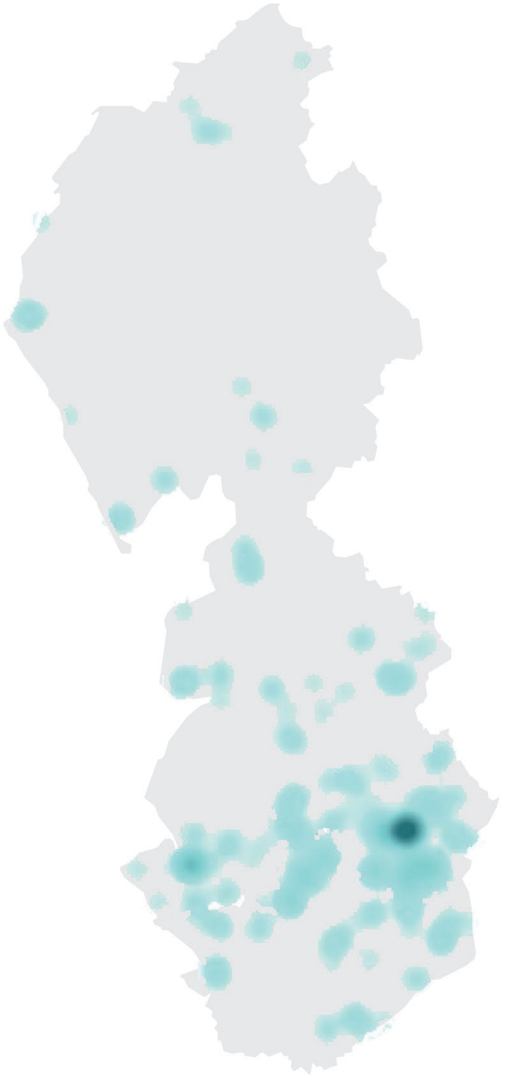
The DSIT UK Cyber Security Sectoral Analysis (2023) identifies 1,979 businesses within the UK that offer cyber security products or services. These businesses have an estimated 4,970 offices across the UK.

It highlights that the UK's cyber security sector also employs c. 58,000 Full-Time Equivalents,(FTEs) (an increase of 10% since the previous year), and that revenue and Gross Value Added have reached £10.5bn and £6.2bn respectively.

THE DSIT CYBER SECURITY SECTORAL ANALYSIS SUGGESTS THAT THE NORTH WEST IS HOME TO:

- 298 cyber security companies, with 456 cyber security offices. Of these 144 are registered in the region (i.e. headquartered), and a further 154 are registered in other regions but have a presence in the North West.
- The region is home to approximately 9% of the UK's cyber security sector (in terms of office count), and that 15% of UK registered cyber security businesses have at least one office in the North West.
- This data highlights that the North West is the UK's largest cyber security ecosystem outside of London and South East.
- Just over half (53%) of cyber security offices are based in Greater Manchester, followed by Cheshire and Warrington (21%), Liverpool City Region (12%), Lancashire (8%) and Cumbria (6%). Manchester has the second highest number of cyber security offices in the UK (272).
- There is a concentration of private activity within Greater Manchester; however, as set out previously, other areas across the North West have commercial specialisms within aerospace, defence, electech, and advanced manufacturing – all of which have considered and concentrated cyber security expertise and excellence.

THE NORTH WEST'S CYBER SECURITY BUSINESSES (MAP)



SIZE AND STRENGTHS:

- Of the cyber security businesses with an active office in the region, 23% (68) are large, 12% (37) are medium, 24% (71) are small, and 41% (122) are micro.
- The report also distinguishes between 'dedicated (pure-play)' cyber security businesses where the majority of their activity related to cyber security provision, and 'diversified', where the firm offers wider products or services. The data suggests that 54% of firms are 'dedicated' and 46% of firms are 'diversified' in the North West.
- Both the size and provision data suggests that the North West is relatively unique in its ability to attract large multinational firms, and this offers significant opportunity with respect to scaling the workforce in the coming decade, particularly through routes such as apprenticeships and retraining. This is explored in subsequent chapters.
- Review of the company level data also highlights regional excellence in:
  - Attracting large multinational businesses to the region with active presence in cyber security (e.g. Cisco, BT, BAE Systems, IBM, Darktrace, Deloitte, PwC, KPMG, EY, Capgemini, Microsoft, Ericsson, QinetiQ, and Thales all have an active presence).
  - A significant base of pure-play cyber security employers registered in the region e.g. NCC Group, BeyondTrust (formerly Avecto), CyberIAM, Cyfor, Secarma, and Capslock.
  - Emerging strengths in novel technologies such as quantum security (e.g. Quantum Base), identity governance (e.g. ProofID), and AI for cyber security (e.g. Mindgard, a spin-out from Lancaster University).

EMPLOYMENT:

- The study also highlights that the North West is estimated to be home to approximately 9% of the UK's cyber security sector's workforce. This translates to just over 5,000 FTEs working within the region's private cyber security sector.
- However, this figure is estimated to be much greater when considering the **entire cyber security workforce across all sectors.** Using the DSIT Cyber Security Sectoral Analysis (2023), and the modelling within the DSIT Cyber Skills in the UK Labour Market (2023) research, we estimate there are approximately **12,000 FTEs in the North West's cyber security workforce across all of the private and public sector and academia.**

REVENUE :

- The UK Cyber Security Sectoral Analysis estimated that the sector generated £10.5bn in the most recent financial year (21/22). Of this, the 141 firms registered in the North West generated an estimated £493m in cyber security related revenue, and employed an estimated 3,700 cyber security FTEs.
- However, given the region's strength in attracting inward investment, we note that all 298 firms active in the region have combined cyber security revenues of £4.9bn (just under half of the UK's revenue estimate) across their entire UK operations.
- This highlights the dual opportunity that exists in the North West – both to further increase its reputation in attracting investment from other regions and internationally, as well as grow its strong regional indigenous base.

INVESTMENT:

- The UK Cyber Security Sectoral Analysis also explores external investment (i.e. where firms have raised investment typically in exchange for equity from external investors such as Venture Capital firms or angel investors).
- In 2022, dedicated cyber security firms in the UK raised an estimated £302m across 76 deals. This is considerably lower than 2021 (£1,013m) and 2020 (£814m) levels.
- In 2022, cyber security firms in the North West raised £38.1m across 6 deals (including significant investments into Lunio (PPC Protect) and ProofID. This places it third for external investment behind London and the South East. In total, cyber security firms in the North West have raised the same value of investment as the other nine regions of the UK in 2022.
- However, investment data can be subject to significant annual variation, particularly when a small number of high-growth companies raise significant investment rounds. In the previous year (2021), the North West raised a much smaller £3.8m across 9 deals, with similar performance in 2019 and 2020. This means it is crucial to continue to grow attractive start-ups and scale-ups, and encourage further external investment to the region (e.g. through initiatives such as Cyber Runway and NCSC for Start-Ups).

KEY STATISTICS FOR THE NORTH WEST'S CYBER SECURITY SECTOR:

298

Number of Businesses

12,000

FTEs in the cyber security workforce (9% of the UK total)

£38M

Raised in external investment 2022 – third highest region in the UK

SUMMARY

The North West has a vibrant cyber security sector, with an encouraging mix of large, diversified multinationals recruiting for cyber security talent, and emerging start-ups with novel products and solutions. With almost three hundred cyber security businesses, and in excess of 5,000 FTEs, this places the North West as one of the UK's largest cyber security sectors outside of London and the South East.

The sector is also well positioned against the region's specialisms in defence, aerospace, advanced manufacturing, professional services and public sector. However, this data also highlights that the region could benefit from further external investment and collaboration with these adjacent sectors. This is explored in further detail in subsequent sections.

5.4. IDENTIFICATION OF CYBER SECURITY RELATED ASSETS

The cyber security sector is only one component of the North West's cyber security ecosystem. There is a vibrant wider ecosystem with businesses, academia, researcher, and public sector that will shape and influence the Cyber Corridor. This section explores:

- **The role of over 150 wider public, private and research assets**[7] relevant to cyber security in the region. These are not typically 'cyber security businesses', but include a wider range of organisations critical to the success of the ecosystem. The North West Cyber Corridor is host to significant defence, public, and research assets – these are explored in detail, and set out with Appendix C.
- The role of adjacent industries and sectors with regional strengths, such as aerospace and defence, advanced manufacturing, and professional services.

Overall we find evidence of:

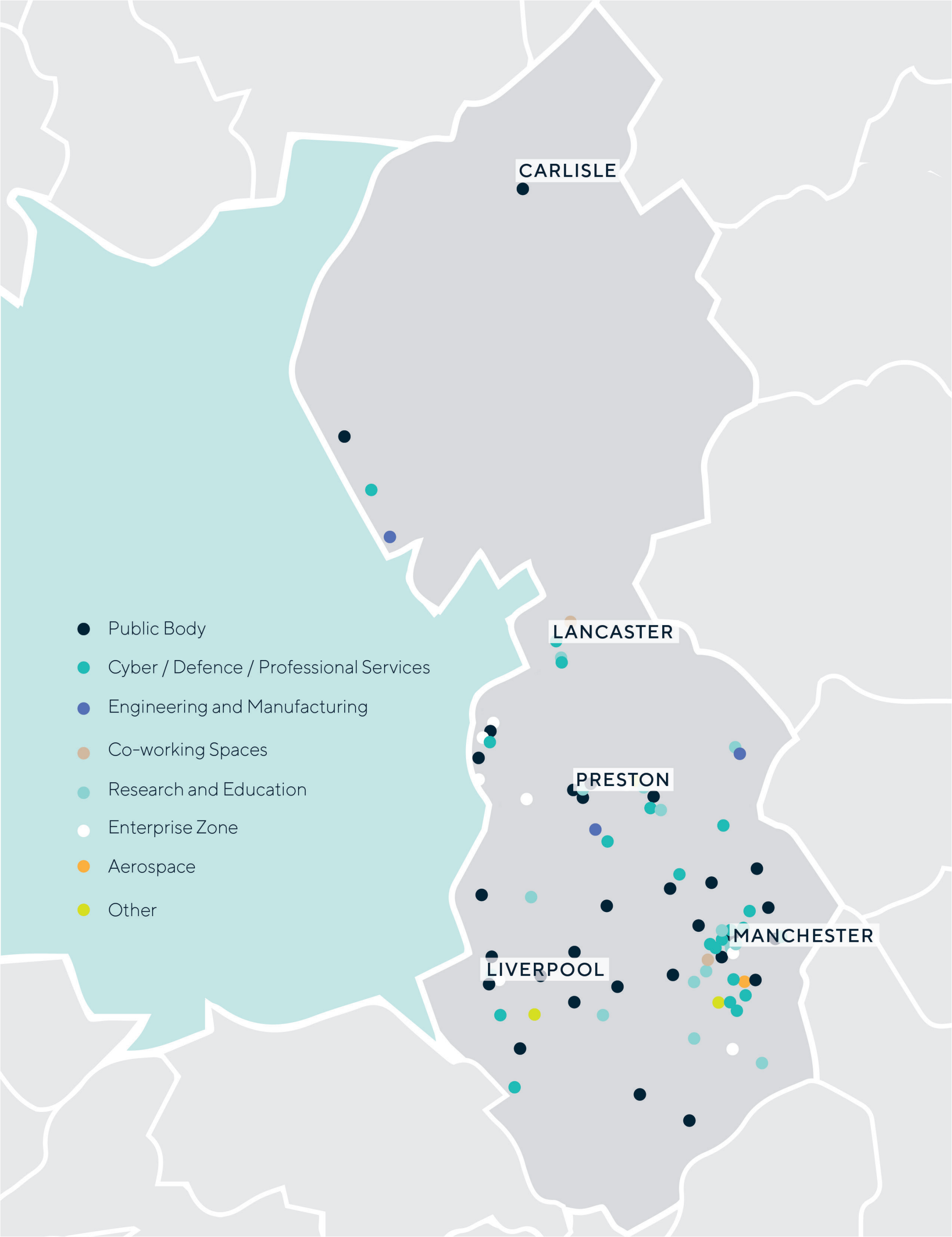
- **Strong research and education provision**, with twelve universities offering cyber security and computer science courses, and a dozen other colleges and training initiatives in the
- At least **20 high quality co-working and incubation spaces** with a digital and cyber security focus, including the newly opened Digital Innovation Security Hub (DiSH) at Heron House, Fraser House and InfoLab21 in Lancaster, and several Bruntwood SciTech sites in Cheshire (Alderley Park), Liverpool (Science Park), Manchester (Circle Square, Citylabs and Manchester Science Park), and SciTech Daresbury.
- A **complementary range of high-quality university collaboration initiatives:** Several of the region's universities place a strong emphasis on commercialisation and knowledge sharing within cyber security. This is reflected in, for example, close collaborations between the University of Manchester and Lancaster University, through projects such as DiSH, Cyber Foundry, the Centre for Digital Trust and Society, and Sprite+. Further, initiatives such as the North West Cyber Security Cluster will also enable cross-sectoral collaboration.

- **Increasing co-investment from defence and public sector bodies:** A critical component of growing the cyber ecosystem and skills base is that of aligned investments from key assets. NCF's proposed £5bn investment in the region will be catalytic; however, this will complement other investments across the North West, such as GCHQ and NCSC's new Manchester office, and private investments such as BAE Systems' expansion in Barrow-in-Furness.
- **A unique range of R&D assets:** The region is also home to significant research strengths and assets that can be used to advance the cyber security ecosystem. For example, in 2019, the Hartree Centre at STFC's Daresbury Laboratory announced a partnership with Siemens and Atos to develop an Industrial Digitalisation Accelerator (IDA) to explore Industry 4.0 opportunities.

[7] These have been identified through a deep-dive of key regional assets. This figure may likely be higher as the Cyber Corridor initiative grows in the region.

SUMMARY MAP:

A full list of assets is set out within Annex D. We summarise some of the key assets on the next page:



SUMMARY OF KEY ASSETS:

- Cumbria has particular expertise in nuclear, and this is reflected by the role of Sellafield and Low Level Waste Repository (LLWR). Cyber security is a key component of the NDA's work. The region also has engineering and defence expertise e.g. through QinetiQ, Jacobs, Westlakes Science Park, and BAE Systems in Barrow-in-Furness.

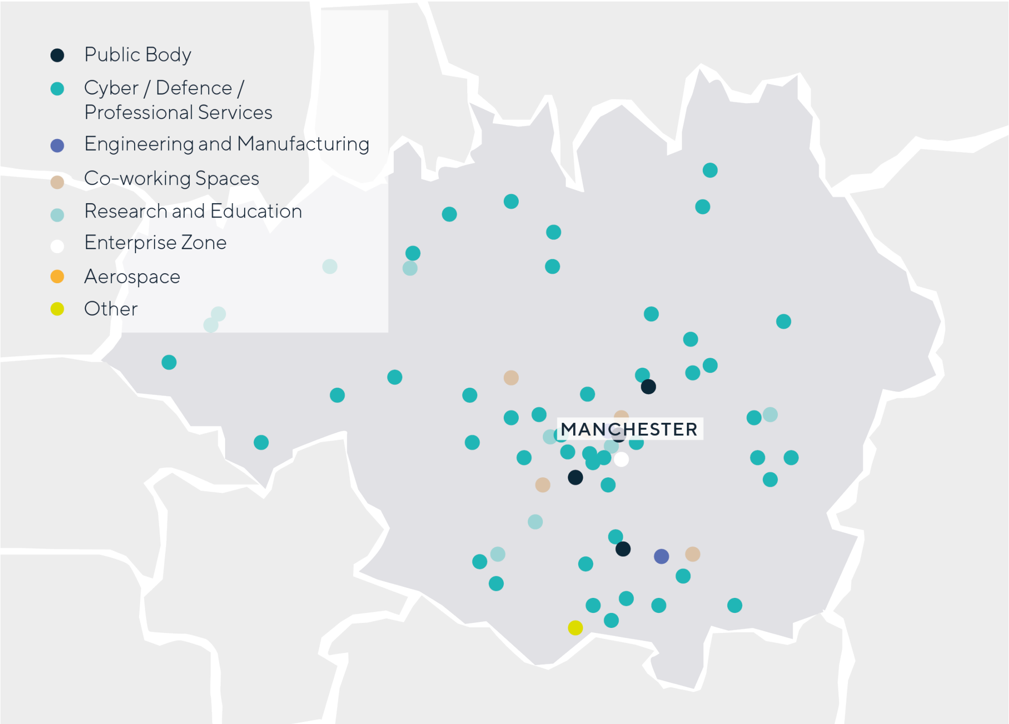
- Lancashire has over 40 relevant assets, including the NW Aerospace Alliance, BAE Systems, the Lancashire Cyber Alliance, several MoD sites, Advanced Manufacturing Research Centre at Blackburn. It also hosts NCSC accredited Academic Centre of Excellence in Cyber Security Research Lancaster University, and UCLan.

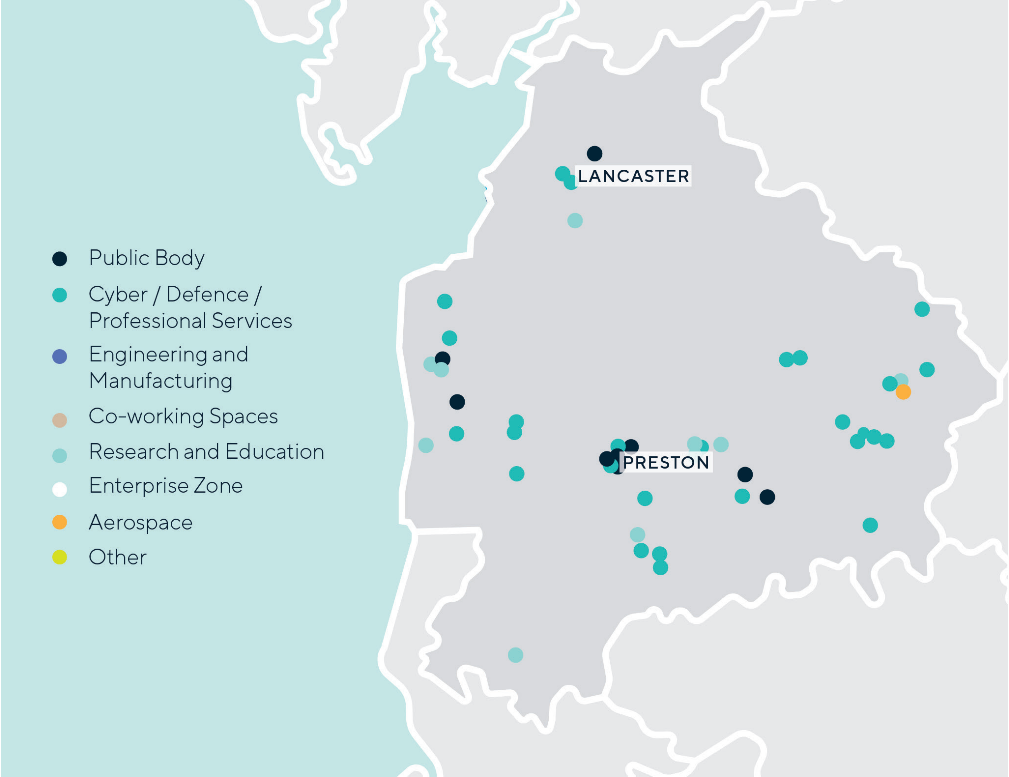
- Liverpool (City Region) is home to three leading universities (University of Liverpool, LJMU, and Liverpool Hope), as well as Knowledge Quarter Liverpool, amidst a number of digital, cyber, IoT and HealthTech initiatives e.g. Sensor City, and Liverpool Science Park.

- STFC Hartree is also strategically positioned in adjacent Daresbury. The Cheshire Science Corridor also crosses the Cheshire & Warrington sub-region linking together established science based businesses including URENCO, Sellafield, Rolls Royce, Essar, AstraZeneca and Waters Corporation.

- GM is home to more than 70 relevant cyber and digital assets, including DiSH, GCHQ/ NCSC Manchester Digital, SciTech, GM Police, University of Manchester, Manchester Metropolitan University, University of Salford, University of Bolton, and a large range of multinational employers such as Raytheon, Thales, BT, TalkTalk, and large consultancies.

SUB-REGIONAL DEEP-DIVE: GREATER MANCHESTER AND LANCASHIRE





5.5. RESEARCH ECOSYSTEM

The North West is home to twelve universities offering courses in cyber security and computer science, including:

- Lancaster University
- Manchester Metropolitan University
- University of Liverpool
- Liverpool John Moores University
- University of Central Lancashire (UCLan)
- University of Salford
- Edge Hill University
- University of Bolton
- Liverpool Hope University
- University of Chester
- University of Cumbria

These are critically important as they support the region through advancing research and commercialising novel IP, develop the next generation of talent through courses, and provide supportive infrastructure and initiatives to support the region's ecosystem such as business accelerators and business engagement.

The following section explores the research base within the North West, setting out the region's research activity in cyber and related fields. We explore this using the UKRI's Gateway to Research API. Please note that this is derived from UKRI GTR using a Boolean search for 'cyber security' projects, and may therefore not fully capture all projects related to this activity; however, is considered representative. This identifies research participation from the c. 300 businesses and c. 150 assets active within the region in cyber security related research projects.

We explore the role of universities in course provision and the volume of students and graduates within the following subsection.

The following tables set out publicly funded research and innovation activity in cyber security over the period 2012 to 2022. Table 5.1 summaries the projects in which the lead academic partner is positioned in the North West, alongside the value of awards provided to these projects. Location quotients (LQ) show whether the North West has a high or low concentration of research activity relative to the UK average.

A LQ greater than 1 signals a level of activity/ specialisation that exceeds what would normally be expected nationally, while below 1 indicates a lower concentration relative to the national average.

TABLE 5.1 NORTH WEST BASED ORGANISATIONS AS PROJECT LEADS FOR PUBLICLY FUNDED RESEARCH PROJECTS (2012-2022)

	PROJECTS LED BY ORGANISATIONS FROM THE NW	% OF UK PROJECTS	LQ	VALUE OF PROJECTS LED FROM NW (£)	% OF UK FUNDING	LQ
Cyber Security	54	7%[8]	0.72	£15,269,267[9]	4%	0.42
All topics	8,631	11%	1.07	£3,087,570,233	10%	1.00

Source: Perspective Economics analysis of UKRI GTR (2012-22)

The North West has contained project leads in 54 cyber security projects over the last ten years, amounting to 7% of cyber security projects in the UK. The LQ for this figure is slightly lower than expected. Further, funding for cyber security projects (where leads are based in the NW) only accounts for 4% of UK funding (LQ of 0.42). However, this is a small sample of projects, and research quality and impact should also be considered. It is worth noting that many research initiatives (such as internal university funding decisions to expand teaching or cyber infrastructure) may not be captured by UKRI GtR as this tracks public investment in R&D. Further, analysing projects **under all topics** with lead researchers in the North West highlights that the region is leading 11% of UK projects and receiving 10% of the funding. This suggests that the North West is performing relatively well (compared to the UK) with respect to research activity; however, enhanced focus on supporting North West institutions and businesses to get involved in cyber related research projects should be undertaken.

TABLE 5.2 NORTH WEST BASED ORGANISATIONS AS PROJECT PARTICIPANTS FOR PUBLICLY FUNDED CYBER SECURITY RESEARCH PROJECTS (2012-2022)

	PROJECTS LED BY ORGANISATIONS FROM THE NW	% OF UK PROJECTS	LQ	VALUE NW PARTICIPATED PROJECTS (£)	% OF UK FUNDING	LQ
Cyber Security	62 (involving 80 participations by 21 unique organisations)	8%	0.82	£61,224,197	6%	N/A

Source: Perspective Economics analysis of UKRI GTR (2012-22)

[8] We have identified 54 cyber security projects led by organisations from the North West. There are 770 projects across the UK with a known region.

[9] We have identified £15.3m of funding allocated to cyber security projects in the NW (out of £375.3m with a known location across the UK).

The region has participated in 8% of the UK's cyber security projects – the LQ suggests that this level of activity is lower than expected given the national average. However, the projects that the North West has participated in amount to 16% of the total funding given to cyber security projects in the UK.

Table 5.3 shows the organisations active in the North West that have participated in cyber security research projects (on UKRI GTR), alongside the number of projects each organisation has participated in. Lancaster University has participated in the highest number of projects, participating in 34% of the 62 cyber projects identified in the region, followed by University of Manchester and University of Liverpool (19% each).

We have identified twelve private organisations that have engaged with cyber security projects (either the project is in the region, or the organisation is based in the region) over the last decade. Whilst this contains some interesting and significant companies (e.g. NCC Group, Sellafield, HP), the count of projects is relatively low, suggesting a need for regional universities to further partner or include private sector organisations within research projects.

Initiatives such as Cyber Foundry and DiSH will be important factors in increasing private participation in cyber security research projects in the region.

TABLE 5.3 NORTH WEST BASED ORGANISATIONS PARTICIPATION IN PUBLICLY FUNDED CYBER SECURITY RESEARCH PROJECTS (2012-2022)

ORGANISATION	TYPE	INVOLVEMENT IN NUMBER OF CYBER PROJECTS IN NW	% OF NW CYBER PROJECTS[10]	VALUE OF PROJECTS (CYBER) INVOLVED IN	% OF VALUE
Lancaster University	University	21	34%	£10,410,536	17%
Manchester University	University	12	19%	£16,953,164	28%
Liverpool University	University	12	19%	£3,318,629	5%
NCC Group	Private	7	11%	£13,912,672	23%
Manchester Metropolitan University	University	4	6%	£11,054,776	18%
GCHQ	Public	4	6%	£4,331,037	7%
Zaiku Group Ltd	Private	4	6%	£201,910	0%
KPMG	Private	2	3%	£6,205,237	10%
Clearswift Ltd	Private	2	3%	£228,284	0%
Capslock Education Ltd	Private	2	3%	£274,890	0%
PWC	Private	1	2%	£6,003,076	10%
Manchester Cyber Foundry	Collaboration	1	2%	£3,011,795	5%
BAE Systems Plc	Private	1	2%	£2,851,861	5%
Sellafield Ltd	Private	1	2%	£642,163	1%
Hewlett Packard Enterprise (HPE)	Private	1	2%	£283,382	0%
Akimbo Core Ltd	Private	1	2%	£218,689	0%
Digital Interruption Ltd	Private	1	2%	£95,138	0%
University of Salford	University	1	2%	£81,802	0%
Quantum Base Ltd	Private	1	2%	Unknown	-

EXAMPLE RESEARCH PROJECTS:

THE ACADEMIC CENTRE OF EXCELLENCE IN CYBER SECURITY RESEARCH (ACE-CSR)

- Lead Research Organisation: Lancaster University.
- Funding: £81,802.
- Hosted in the university's flagship cross-disciplinary Security Lancaster Research Centre.
- The centre has master's students, doctoral students, and post-doctoral researchers, with most students and staff stationed in a specific area of Infolab21. The centre participates in and leads a range of major research programmes, such as the Security and Safety Stream within the EPSRC Hub on Cyber Security and the Internet of Things.
- The key goal is to maximise the impact of the status and funds provided to the ACE-CSR, targeting cyber security stakeholder groups in industry, policing, and government organisations. Lancaster is also home to the UK's hub for behavioural and social science research into security threats: the Centre for Research and Evidence on Security Threats (CREST). CREST conducts independent research whilst informing cyber security policy and practice and providing skills training to future leaders of research.

UKRI (2017-2023) Academic Centre of Excellence in Cyber Security Research – Lancaster University. Available at: https://gtr.ukri.org/projects?ref=EP%2FR00692X%2F1

TURING AI FELLOWSHIP: PROBABILISTIC ALGORITHMS FOR SCALABLE AND COMPUTABLE APPROACHES TO LEARNING (PASCAL)

- Lead Research Organisation: Lancaster University, with support from GCHQ , the Heilbronn Institute of Mathematical Research, Transport Research Laboratory, the University of Washington and the Alan Turing Institute.
- **Funded Value: £1,097,294 (Jan 2021 – Dec 2025).**
- "The PASCAL research programme is focused on developing an end-to-end framework, from data to decisions, that naturally accounts for data uncertainty and provides transparent and interpretable decision-making tools. The algorithms developed throughout this research project will be generally-applicable in a wide range of application domains and appropriate for modern computer hardware infrastructure. All of the research and associated algorithms will be widely available through high-quality open-source software that will ensure the widest possible uptake of this research within the international AI research community. PASCAL will focus on two primary applications areas: cybersecurity and transportation, which will stimulate and motivate this research and ensure wide-spread impact within these sectors.

UKRI (2021-2025). Available at: https://gtr.ukri.org/projects?ref=EP%2FV022636%2F1#/tabOverview

[10] Figures sum to more than 100% as projects can contain multiple organisations, and financial contribution is not always segmented by organisation involved.

SCorCH: Secure Code for Capability Hardware

- Lead Research Organisation: University of Manchester, in partnership with ARM and Amazon.
- Funded Value: £1,034,989 (Dec 2020 – Dec 2023).
- Through creating the ICSF Digital Security by Design Challenge, the Industrial Strategy Challenge Fund and EPSRC have identified an opportunity to have a significant impact on the landscape of embedded systems, IoT and Edge computing. This is through a focus on Capability Hardware. This project will join this effort in contributing to a shared vision of fully-verifiable safe and secure software, where underlying hardware/software architectures are built with strong symbolic and mathematical guarantees. This will benefit users of software for capability hardware, developers, and automated reasoning tools.

UKRI (2020-2023) Available at:
https://gtr.ukri.org/projects?ref=EP%2FV000497%2F1#/tabOverview

The region also hosts a range of public and private defence and security assets that have a high demand for cyber security research and capability enhancement.

NATIONAL CYBER FORCE:

The National Cyber Force (NCF) is a partnership between defence and intelligence. The NCF is responsible for managing and observing cyberspace to counter any possible threats, such as:

- Threats from terrorists, criminals, and states that use the internet to do harm across borders.
- Threats to confidentiality, integrity and availability of our data and services in the cyberspace.

MINISTRY OF DEFENCE

The North West hosts a range of MoD sites, and has responsibility for national security and defence. It is a core partner with the NCF, bringing cutting edge intelligence and research techniques to cyber defence and intelligence. The Cyber Resilience Strategy for Defence[11] is the MoD's updated cyber strategy and includes strategic priorities for Secure by Design (capabilities are protected from the outset and throughout their life cycle and are built to be resilient against cyber-attacks), Governance, Risk and Compliance, and Rapid Detection and Response within cyber defences.

[11] HM Government (2022) Cyber Resilience Strategy for Defence. Available at: https://www.gov.uk/government/publications/cyber-resilience-strategy-for-defence

GCHQ (INCL. NCSC)

GCHQ is the Government Communications Headquarters, one of the three UK Intelligence and Security Agencies, along with MI5 and the Secret Intelligence Service (MI6). It also established the National Cyber Security Centre (NCSC), which protects critical services from attacks, and improves the underlying security of the UK. GCHQ and the NCSC established a new site in Heron House, Manchester in 2019, and supports the DiSH MCR, an innovation hotbed co-located to support cyber security start-ups.

PRIVATE SECTOR

The North West is also a strong location for private sector aerospace and defence firms. It includes significant investments from:

- **Raytheon Intelligence and Space**, which invests heavily in cyber security and AI, and recently opened a £4m cyber centre in Salford Quays. Raytheon also supports HOST Cyber – an innovative Security Operation Centre, and the 'Cyber Salford' project which will develop greater awareness of cyber security and careers across the region.
- **BAE Systems** is the third largest global defence supplier with long-established positions in air, maritime and land domains, and has key sites at Warton, Samlesbury, Preston, and Barrow-in-Furness. In addition to its considerable advanced manufacturing presence, BAE Systems has over 4,500 cyber and intelligence experts globally.
- **Thales** provides defence, security, transport and aerospace solutions. It has c. 6,500 staff in the UK, but it has the highest concentration of roles in the North West with 1,600 Thales supply chain jobs. Its Cheadle site in Greater Manchester has over 600 employees and has been part of the business since 1977. It is a centre of excellence for software design and development with teams working on emerging technologies including artificial intelligence.

CASE STUDY: PROMOTING KNOWLEDGE EXCHANGE IN CYBER SECURITY

Lancaster University places a strong emphasis on generating impact within the North West. It holds both NCSC and EPSRC accreditation as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR) and as an Academic Centre of Excellence in Cyber Security Education (ACE-CSE). It has established partnerships with industry through:

- Cyber Works at Lancaster University offers a range of knowledge exchange opportunities to businesses in cyber security. This includes secure digitalisation support, Knowledge Transfer Partnerships (KTPs), entrepreneurship programmes, internships and promoting the University's Enterprise Zone. Funding: £81,802
- Cyber Foundry: The Cyber Foundry is a series of multi-million pound secure digitalisation projects that will help SMEs across both the Greater Manchester and Lancashire regions to defend, innovate and grow their businesses.
- DiSH aims to support 500 new start-ups and create over 1,000 jobs in the region. The consortium of partners appointed by Manchester City Council to create the DiSH, including Lancaster University, Barclays Eagle Labs - in partnership with Plexal - and The University of Manchester, are also providing a range of cyber initiatives from the site.
- The newly announced Security and Protection Science at Lancaster project, a major new £19m initiative to boost the University's teaching and research capabilities around cyber security including recruitment of over 30 new academics across a variety of disciplines to focus on digital threats and support major national cyber security initiatives in the North West. The facilities will be central to Lancaster's flagship Data Cyber Quarter and consist of eight specialist laboratories and a semi-immersive decision theatre. The University's iconic InfoLab building will also be upgraded as part of the project. This will create one of the largest educational facilities of this type in the country and will support education offerings in underpinning technologies through BSc degrees in Computer Science, Cyber Security and Data Science, Masters courses in Data Science and Cyber Security, a Cyber Leaders Executive MBA, and professional training and reskilling.

5.6 DEMAND FOR CYBER SECURITY TALENT

The DSIT Cyber Skills in the UK Labour Market (2023) research highlights that across the UK, there are typically:

- 5,900 job postings advertised each month in **technical / core** cyber security roles, and a further 7,400 **broader** cyber security roles in the UK (in 2022).
- Approximately 10% of these vacancies were posted in the North West region, of which just over half are in Greater Manchester (56%), one in six in Lancashire (16%), one in seven in Liverpool City Region (13%), and the remaining roles across Cheshire (8%) and Cumbria (3%).

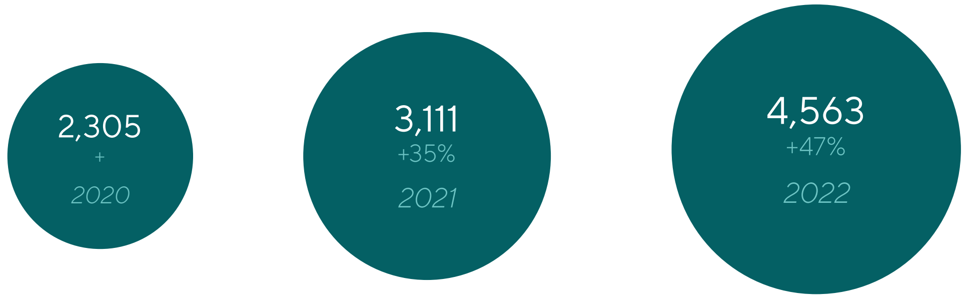
> The North West has the third highest demand for cyber security professionals (10% of UK job postings with a known location) behind London (35%) and the South East (12%).

Building on this report, we use the Lightcast platform (a database that tracks online job postings) to undertake further analysis of the demand for cyber security talent in the North West. We undertake this analysis from January 2021 to December 2022.

DEMAND FOR CYBER SECURITY TALENT:

There has been a sharp increase in demand for cyber security professionals in the last few years within the North West (consistent with wider UK trends). Our analysis suggests there are were at least 4,500 job postings for technical cyber security roles in the North West in 2022, almost twice the levels demanded in 2020.

NUMBER OF CORE (TECHNICAL) CYBER SECURITY JOB POSTINGS IN THE NORTH WEST



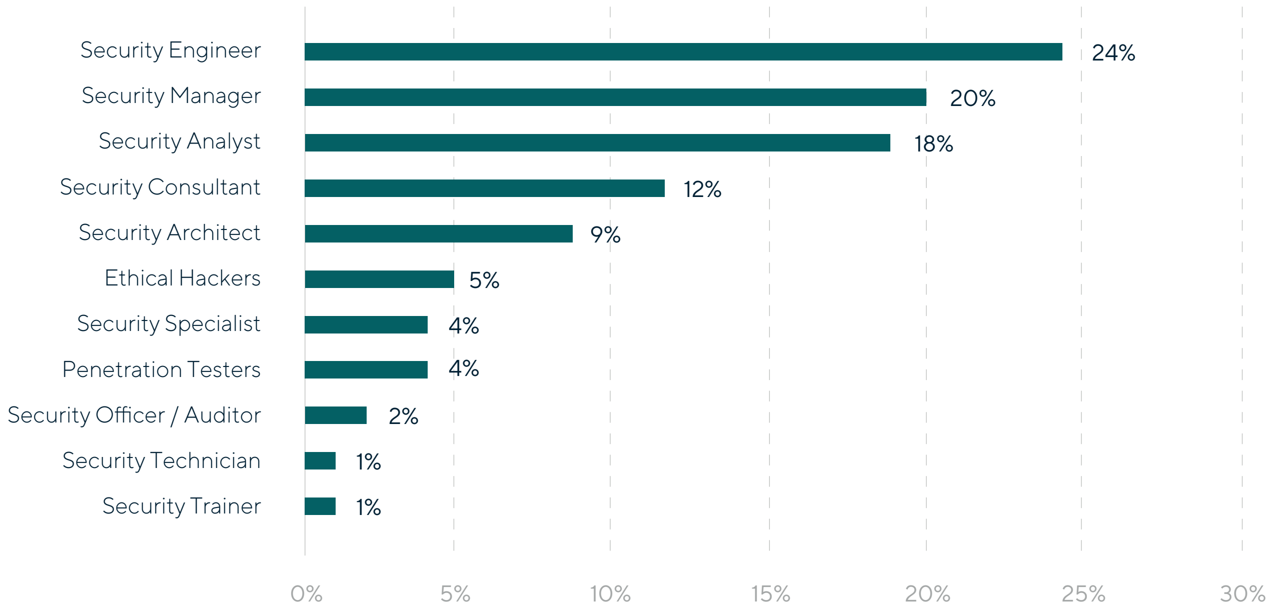
Source: PE analysis of Lightcast vacancy data

Further, we have also identified a further 5,100 job postings within the North West in 2022 where the job posting requests some knowledge or understanding of cyber security, but may not be a 'core or technical' cyber security role (e.g. Governance, Risk and Compliance roles, or other network roles). These figures may indeed be higher where employers are posting roles 'remotely', or are using alternative forms of recruitment (e.g. direct recruitment through agencies).

This highlights the significant demand for cyber security talent within the region, and this is only set to grow with incoming investments by GCHQ, NCSC and NCF in the region, who will require considerable volumes of talent to resource new centres of excellence in areas such as threat intelligence, risk, programming, incident response, and offensive cyber.

TOP JOB POSTINGS

Review of cyber security related job postings in the North West highlights highest demand for security engineers, managers, analysts and consultants.



Source: PE analysis of Lightcast vacancy data (2022)

This demand is comparable to that set out within the DSIT Cyber Skills in the UK Labour Market research at a national level. In order to increase the size of the cyber security ecosystem in the region, there is also a need for supporting entry-level and early stage pathways into cyber. Our analysis suggests that, in the North West:

- 17% of job postings require less than one years' experience (where stated)
- 40% require at least 2 to 3 years' experience in cyber security (or similar)
- 29% require 4 to 6 years' experience in cyber security
- 15% require at least 7 years' experience

This highlights a need to promote early-stage pathways, and work with employers and industry to develop these.

TOP EMPLOYERS

In 2021 and 2022, the North West had a number of large employers in high demand for cyber security talent. Within job vacancy analysis, often many employers will use recruitment agencies; however, we have identified that key employers in recent years have included Barclays, PA Consulting, BT, CGI, BAE Systems, Avanade, KPMG, Accenture, The Hut Group, Boeing, Jacobs and the NHS.

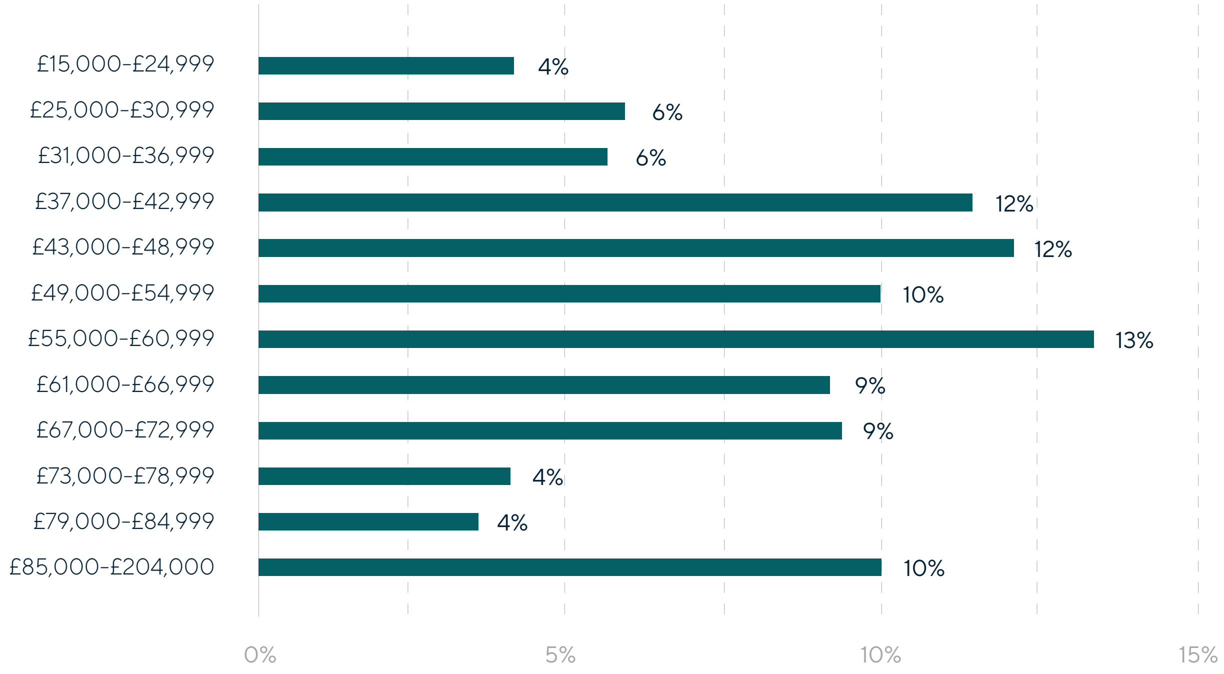
This offers a robust base for working with industry to help develop new pathways into cyber security in the region.

REMUNERATION

The North West is an attractive area to live and work in, particularly in cyber security roles. Using the Lightcast platform, we estimate remuneration across the region for core cyber security roles in 2022. This suggests that the **mean salary for a core cyber security role in the North West in 2022 was £56,800** (median £54,000). This is slightly lower than the UK mean of £59,400; however, is particularly strong for the region and has a considerable pay premium compared to wider sectors.

Further, advertised salary distribution highlights that entry-level roles have the potential to be higher than wider mean salaries within the region's economy, with substantial earnings potential thereafter with increased experience. This means that retraining and reskilling initiatives in the region could have substantive implications for regional productivity and skills.

PERCENTAGE OF CORE CYBER JOB POSTINGS OFFERING THE FOLLOWING SALARIES (WHERE SALARY OR SALARY RANGE IS ADVERTISED)



Source: PE analysis of Lightcast data (n = 1,591 roles with salary provided in the North West, 2022)

5.7 BUILDING THE SKILLS SUPPLY AND CYBER SECURITY WORKFORCE

In order to meet the high demand for cyber security talent, and to provide the resources required to innovate and grow the ecosystem – the Cyber Corridor initiative will take a much required emphasis on skills development.

The DSIT Cyber Skills in the UK Labour Market (2023) suggests that the UK cyber security workforce has c. 133,400 individuals.

Of these, an estimated 9% (c. 12,000 people) are based in the North West.

The data therefore suggests that there are approximately 5,000 FTEs working in the North West's cyber security sector, and a further 7,000 FTEs working in wider cyber security related roles in other industries and public sector.

The following sub-sections explore the provision of cyber security skills in the region, including university course provision, retraining and reskilling initiatives, and further education. This informs an estimate of the 'skills gap', which in turn provides the case for further development of cyber skills in the region.

UNIVERSITY AND HIGHER EDUCATION COURSES

According to HESA data (2022) set out in the DSIT Cyber Skills in the UK Labour Market research, the **North West has ten higher education institutes that offer cyber security and computer science courses at undergraduate and/or postgraduate level.** There are a further two universities in the region that offer only computer science courses, Cumbria University and Liverpool Hope University.

In the academic year 2020/21, there were almost 13,500 students enrolled at all levels in cyber security and computer science courses in the North West. This figure is growing each year, with approximately 12,000 students enrolled in the previous year. This suggests that the volume of students enrolled in cyber and computer science courses has increased by 13% in the most recent year.

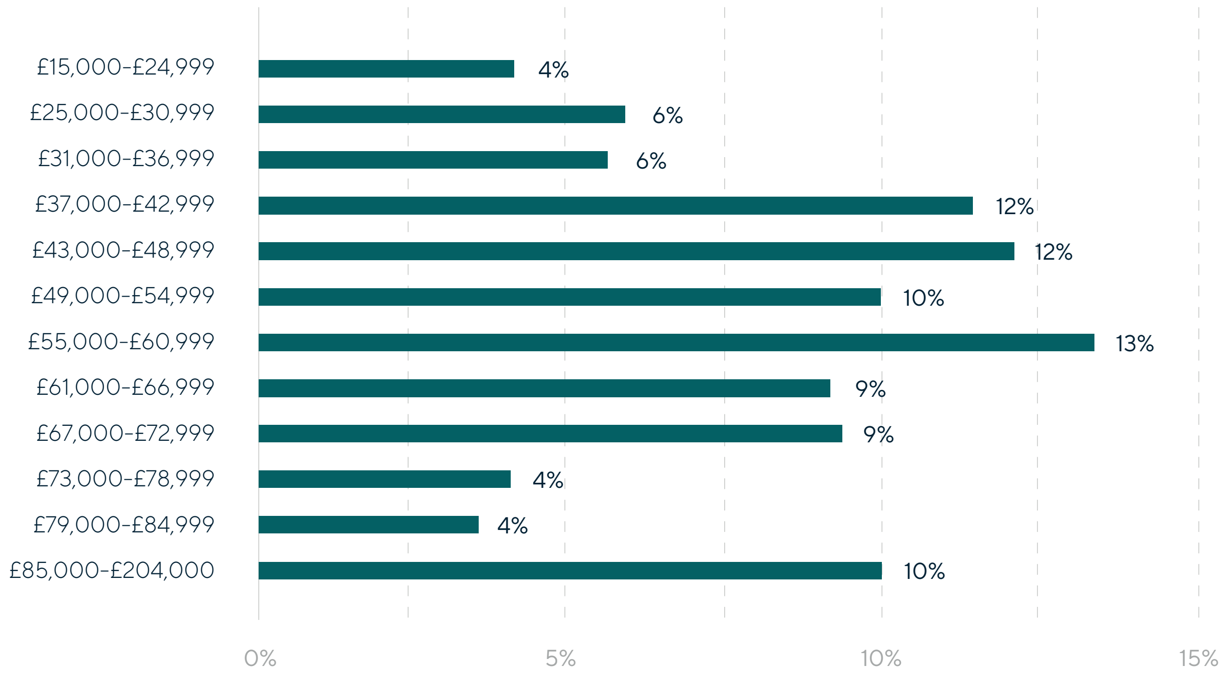
The North West also produced 3,390 graduates[12] in cyber security and computer science in 2020/21 (approximately 10% of the UK supply). This figure is also growing, particularly at postgraduate level.

From September 2023, the University Academy 92 will also provide a Cyber Security BSc, with degrees awarded by Lancaster University, further boosting the future supply of cyber graduates in the North West[13].

[12] 325 in cyber security and 3,065 in computer science.

[13] University Academy 92 (2022) Cyber Security https://ua92.ac.uk/courses/cyber-security-bsc-hons/

NUMBER OF CYBER SECURITY AND COMPUTER SCIENCE GRADUATES AT NORTH WEST UNIVERSITIES (ACADEMIC YEAR 2020/21)



Source: Analysis of Jisc / HESA data (2020 – 2021). Base: Students Graduated= 3,390; Undergraduate=2,113 & Postgraduate=1,277

However, recent DSIT cyber skills research has shown that there is a pronounced and persistent gender gap throughout cyber in both education and the workforce. This is also a challenge in the North West, with only **15% of cyber security and 23% of computer science graduates identifying as female.**

GRADUATE OUTCOMES

Within 15 months of completing their studies, graduates can answer the Graduate Outcomes Survey, which asks students what they are currently doing in relation to further study or employment, their current role or activity, their location, and their earnings (where applicable).

This data relates to graduates from academic year 2019/20 (which would typically have completed the survey in 2021). There were

We explore graduate activity, retention in the region, and salaries below.

GRADUATE ACTIVITY:

- Analysis of the HESA dataset highlights that there were 3,037 cyber security and computer science graduates from universities in the North West in the academic year 2019/20.
- 372 (12%) graduated from cyber security courses and 2,665 (88%) graduated from other computer science courses.
- Of the 3,037 graduates from the North West, 1,463 (48%) responded to the graduate outcomes survey 15 months after graduating.

For the survey respondents:

- 72% of these graduates that studied cyber security or computer science courses in the North West reported being in full-time employment.
- Approximately 7% stated that they were unemployed, and the remainder were typically in further study, employed part-time, or in caring or other duties.
- For those in employment, the median salary is between £25,000 to £30,000[14].

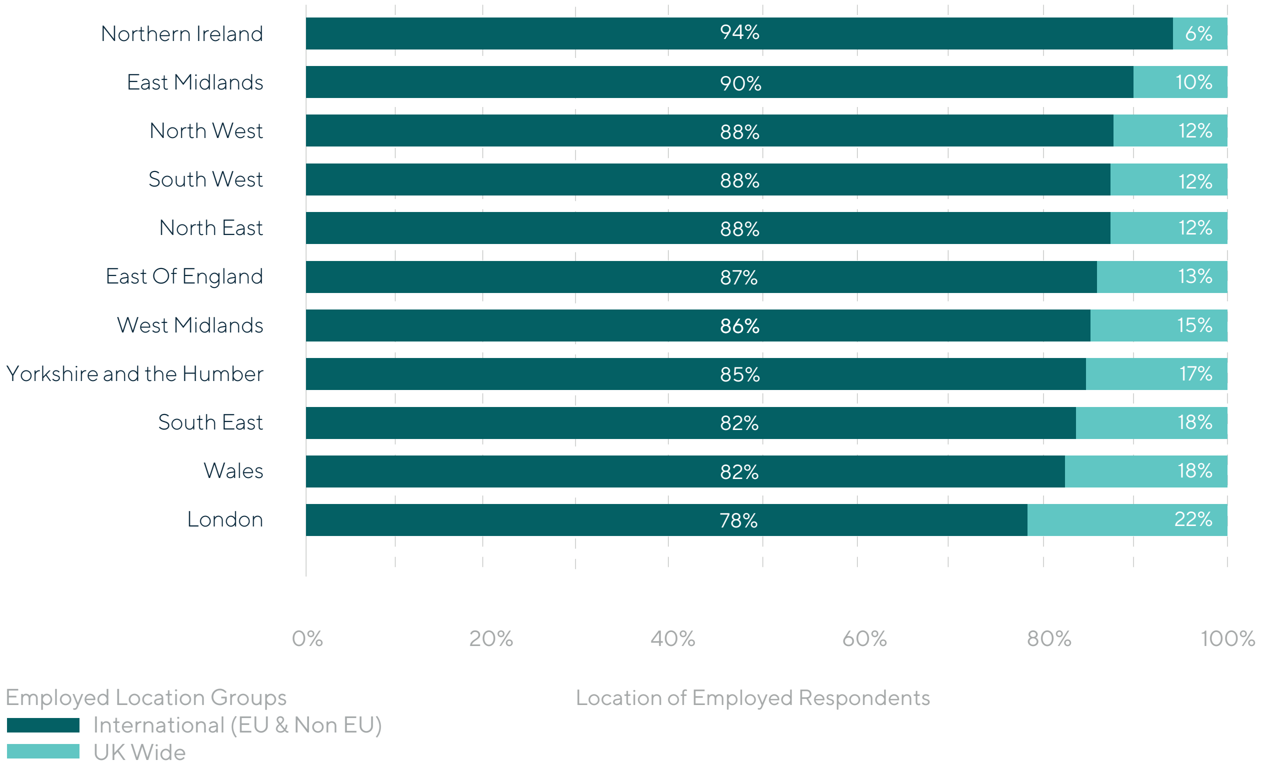
Further, we explore the location of students both during their course (i.e. the region of the university), and where the respondent has provided an employment location. Please note that this data is not fully complete (e.g. many respondents may not answer or may provide a general location such as England).

[14] Please note due to Standard Occupational Classification coding, we do not provide an estimate at the North West level for how many of these graduates may enter a cyber security role. However, we assumed based on the DSIT Cyber Skills in the UK Labour Market, that approximately 85% of computer science and 95% of cyber security graduates are likely to enter an IT related role.

This data suggests that:

- Approximately 18,600 graduates from 2019/20 completed the Graduate Outcomes Survey. Of these, we can match approximately 12,600 to a known location within the UK or internationally. 85% of respondents state that they now work in the UK, and 15% internationally. However, international responses to the survey may be lower.
- For the c. 10,700 respondents that work in the UK, approximately 900 are based in the North West.
- This data suggests that approximately 8-9% of graduates from UK universities that secure employment in the UK within 15 months are based in the North West.
- Further, the North West also has one of the higher rates of retention of students within the UK workforce (i.e. 88% of Graduate Outcomes Survey respondents that studied computer science or cyber security in the North West remained in the UK).

LOCATION OF WORKPLACE BY HIGHER EDUCATION INSTITUTION REGION



(n=12,600)

NORTH WEST RETENTION OF STUDENTS:

- Further, it is important to estimate both how many students in North West universities stay within the region and secure a role, and how many leave the region either to other parts of the UK or internationally.
- In addition, many students may also move to the North West from other regions.
- For the c. 900 respondents that work in the North West following graduation, approximately 540 (60%) studied in the North West. A further 10% studied in Yorkshire, 6% in the West Midlands, 5% in the East Midlands, 3% in Scotland, 3% in the South East, 3% in the North East, 2% in the South West, 2% in London, and 2% in Wales.
- For the c. 1,000 that studied cyber security or computer science in the North West and responded to the Graduate Outcomes Survey, 540 (54%) stayed in the region, 12% reported to have left the UK to work internationally, and the remaining 34% work in other regions of the UK, including 10% that moved to London.
- There is more limited data available for the estimates of employed graduates that enter a cyber security role directly. However, the DSIT Cyber Skills report estimates that approximately 4,000 graduates from both cyber and computer science courses are likely to enter the cyber security workforce (as of 2022).
- We estimate that up to 10% (c. 400 graduates) of these will be based in the North West. However, as reflected by the high demand for cyber security professionals (e.g. 4,500 core cyber security job vacancies posted each year in the region), this highlights the need to increase supply of talent in cyber security through other means such as further education, apprenticeships and reskilling initiatives.

FURTHER EDUCATION AND RETRAINING AND RESKILLING INITIATIVES

In addition to Higher Education, there is an important role for a wider range of skills bodies in the region. The supply of cyber skills and talent in the North West is boosted by the range of cyber focused further education options available in the region.

There are multiple further education providers in the region, with several foundation degrees in cyber security that set students up for careers or further study in the cyber sector.

COURSE	LEVELS	DESCRIPTION	LOCATION
Networking and Cyber Security	Foundation Entry BSc	The foundation entry route to the three-year honors degree – the foundation year prepares students for Higher Education level study and introduces them to computer science topics.	Blackburn College
Network Engineering (Cyber Security)	Foundation Degree	This course provides people with the first steps to becoming a cyber security professional – students will carry out a placement as part of the course, providing them with the professional skills needed for their future.	Blackpool & The Fylde College
Cyber Security and Networking	Foundation Degree	Providing students with a broad-based grounding in professional computing alongside cyber specific modules.	Nelson & Colne College University Centre
Computing (Cyber Security)	Higher National Certificate (HTQ)	Helps students to develop a range of specialist skills to meet the demands of employers through core units such as networking and a specialist unit in cyber security.	Tameside College
Cyber Security	Certificate of Higher Education	Providing students with the knowledge and skills to work with and implement cyber security policies, technologies, and solutions.	University Academy 92

Several colleges in the North West also provide **Level 3 qualifications in cyber security**, such as:

- Cyber Security Principles – Blackpool and The Fylde College
- Cyber Security Practices – Cheshire College South and West
- Cyber Security – The City of Liverpool College
- Computing with Programming, Games Development & Cyber Security – Blackburn College

The Lancashire Colleges partnership aims to enhance collaborations between Further Education Institutions in the Lancashire Area[15]. TLC provides education and skills to 95,000 people, targeting those from disadvantaged backgrounds in particular. The colleges within the network have widespread partners in the private and public sectors, setting participants up for their careers. Members that offer cyber courses include Blackburn College and Blackpool & the Fylde College, and Burnley College offers a Level 3 qualification in computing.

Cyber skills are also formed through active experience in the industry. For this reason, apprenticeships in cyber security are invaluable to the cyber sector in the North West as they provide young people with practical cyber skills. There are a range of **cyber security apprenticeships in the North West**, including:

- Cyber Security Analyst Apprenticeship – working at the University of Salford in Greater Manchester, providing the opportunity to gain valuable cyber skills and knowledge through the completion of a Level 4 Cyber Security Risk Analyst Apprenticeship.
- Cyber Risk & Strategy Apprenticeship – Deloitte's BrightStart Apprenticeship programme based in Manchester, providing apprentices with a foundational level of cyber knowledge and consultancy skills.
- Cyber & Security Degree Apprenticeship – a full-time apprenticeship at Barclays that provides a competitive salary alongside gaining a degree qualification. This apprenticeship is based in Knutsford, where the apprentice will carry out challenging, real-world work.

RESKILLING AND RETRAINING INITIATIVES:

There are a range of cyber focused **retraining and reskilling initiatives** throughout the North West, each contributing to the provision of cyber skills, with the potential to help closing the cyber skills gap.

Some initiatives are aimed at training and educating young students, whilst others target adults who may desire to retrain or upskill in cyber. This also includes national initiatives such as the Armed Forces Career Transition Partnership, which has an established history of supporting veterans move into IT and cyber security roles, and the DSIT Cyber Explorers, Retrain in Cyber, and the NCSC's CyberFirst initiatives.

We set out some example regional initiatives (relating to cyber and digital skills) on the next page:

[15] The Lancashire Colleges. Available at: https://www.tlc.ac.uk/about-tlc/

UNIVERSITY ACADEMY 92: DIGITAL ACADEMY

- Located in Manchester with potential to provide opportunities for the whole North West.
- The Digital Academy[16] will provide enhanced and cutting-edge learning in an employer led and industry co-developed curriculum.
- The goal is to prepare, educate and develop a diverse range of people for a digital career. The academy acts as a digital ecosystem with a focus on digital learning.
- UA92 will also offer (from September 2023) a BSc in Cyber Security, accredited by Lancaster University.

CAPSLOCK

- Capslock is an accredited cyber security bootcamp (registered in Manchester, active across the country) with the goal of reskilling adults across the UK.
- It enables individuals to become cyber security professionals in six months – there is a career outcome focus, setting participants up for high paid competitive roles.
- The programme collaborates with industry leaders such as Lloyds Banking Group, BT and Dell.
- Participants have the option to gain five industry-recognised cyber certificates whilst they are studying, including a core Certified Cyber Security Practitioner qualification.
- They have supported hundreds of individuals to retrain in cyber security, with employers including ITV, BBC, AWS, MoD, BAE Systems and more.
- On average, successful participants have an average salary of £33,300 after completing the programme – an average increase of over £13,000 per learner.

AMAZON INITIATIVES

- The Amazon Future Engineer Bursary[17] is a national programme aimed at supporting female students from low-income households who wish to study computer science at UK universities including the University of Manchester.
- AWS RE/START[18] is a collaboration between Amazon and Generation – it is a free 12-week bootcamp with the goal of kickstarting young people's careers in tech, located in Manchester.
- AWS Start-up Garage[19] provides new businesses with help in tackling technical and business challenges.

COMPTIA

- Globally renowned provider of training and professional certification opportunities in advanced cybersecurity skills through the new digital skills training initiative.
- The Cyber Ready North West programme[20] targets the Lancashire and Greater Manchester area.

HOST & NIYO ENTERPRISE

- MediaCityUK's innovation hub HOST partnered with the socio-creative organisation Niyo Enterprise in its North West expansion with the goal of empowering more black women to pursue tech careers.[21]
- Aiming to create a supportive community with access to digital skills training and secure employment in the tech industry – all whilst challenging the gender diversity disparity.
- The effort to include and support black women has been applied to all of HOST's Skills City academies, including Black Codhers and Black Disrupters.

HOST & CYBER SALFORD

- HOST collaborates with Salford City Council, Cyber Resilience Centre, and partners Raytheon Technologies within the Cyber Salford project.[22]
- The goal is to make Salford one of the most cyber enabled places in the UK and to connect the entire Salford community – this initiative aims to reach all the Salford population such as young people, new businesses and those who are self-employed.
- The initiative will give these people education, training, and tools to increase their cyber security awareness and to encourage innovation in the area.

[16] University Academy 92 (2022) UA92 to build world leading digital academy. Available at: https://ua92.ac.uk/news/ua92-to-build-world-leading-digital-academy/

[17] Amazon (2022) Amazon Future Engineer bursary scheme. Available at: https://www.amazonfutureengineer.co.uk/bursary

[18] Generation (2022) Launch a career in tech with AWS RE/START. Available at: https://uk.generation.org/manchester/aws-restart/

[19] Amazon (2020) How AWS Start-Up Garage events can kick-start your tech business. Available at: https://www.aboutamazon.co.uk/news/small-businesses/how-aws-startup-garage-events-can-kick-start-your-tech-business

[20] CompTIA (2020) CompTIA Builds Cybersecurity Skills in the Greater Manchester and Lancashire Tech Communities. Available at: https://www.comptia.org/newsroom/press-releases/comptia-builds-cybersecurity-skills-in-the-greater-manchester-and-lancashire-tech-communities

[21] Media City (2021) Barrier breaking partnership to empower black women into tech careers in the North West. Available at: https://www.mediacityuk.co.uk/newsroom/barrier-breaking-partnership-to-empower-black-women-into-tech-careers-in-the-

THE CENTRE FOR ENTERPRISE – SKILLS BOOTCAMPS

- Manchester Metropolitan University has partnered with Manchester Digital, Heroworx Institute, and Specialists Hub (funded by DfE) to provide a Skills Bootcamp in Digital. This includes computing fundamentals., as well as technical cyber security and risk analyst material.
- These skills bootcamps last 14 to 16 weeks focused on reskilling or upskilling employed and unemployed individuals so that they can secure roles in the region. The bootcamps are focused on the digital and tech sectors due to the fast growth they are experiencing and the high salaries available in this area.

SKILLS IMPLICATIONS FOR THE REGION:

The DSIT Cyber Skills in the UK Labour Market research highlights that whilst the range of skills initiatives and talent supply relating to cyber security is growing, it is not growing quickly enough to keep up with demand.

At the UK level, this is referred to as the 'cyber workforce gap', and it is estimated that **there was a net annual shortfall of c. 11,200 people in 2022** (with the cyber security ecosystem requiring c. 18,200 people per annum to meet demand and replace those exiting roles – and only 7,000 people entering the cyber security workforce each year through further and higher education, apprenticeships, and reskilling. At a regional level, based upon the estimated 10% of the UK workforce estimates, we can assume that the North West will need to train and upskill more individuals into cyber security – particularly to meet the demands of industry and the wider cyber security ecosystem over the coming decade.

> At a minimum, we estimate that the North West should explore how to encourage a further 1,000 – 1,200 individuals to train or move into cyber security related roles each year to meet demand.

Much of this could be addressed through increasing provision of higher and further education access, promoting reskilling and retraining initiatives, and encouraging life-long learning and career conversion. There is also significant economic benefit through growing cyber security employment in the region. This is set out in Section 8, which explores how the ecosystem should aim to support at least 30,000 jobs in cyber security by 2035.

[22] HOST (2021) HOST launches Cyber Salford to create the most cyber enabled place in the UK. Available at: https://www.hostsalford.com/

[23] Manchester Metropolitan University (2022) The Centre for Enterprise Skills Bootcamps. Available at: https://www.mmu.ac.uk/business-school/business/sme-support/skills-bootcamps/

06
Benchmarking the Region

6.1
INTRODUCTION AND KEY MARKERS

The previous section provided a baseline for the region's cyber security ecosystem. This highlights many of the strengths and assets within the North West, and confirms the national and international significance of the North West as a cyber security hotspot.

This section provides a summary of some of the key metrics and measures, which the Cyber Corridor can use to measure progress and benchmark the region. We apply a Red-Amber-Green (RAG) rating against a range of business, asset, investment, research, and skills measures below, and consider the performance of the North West compared to national and other regional estimates.

As cyber security is continually evolving, many of these measures are experimental (e.g. there is no Standard Industrial Classification code for cyber security) and therefore captured by estimates set out within research such as the DSIT Cyber Security Sectoral Analysis, and Cyber Skills in the UK reports.

MEASURE	RAG	COMMENT
Cyber Security Ecosystem		
Number of Cyber Security Businesses	🟢	– 298 cyber security businesses active in the North West (2022). 15% of UK registered cyber security businesses have at least one office in the North West. – The North West is the UK's largest cyber security ecosystem outside of London and South East.
Number of Cyber Security Employees	🟡	– We estimate that 9% (c. 12,000 people) of the UK's cyber security workforce are based in the North West. – Of these, approximately 5,000 FTEs work in the North West's cyber security sector, and a further 7,000 FTEs in wider cyber security related roles in other industries and public sector. – However, there is a need to boost the supply of skilled talent to sustainably grow this figure (e.g. to 30,000 FTEs by 2035).
Evidence of Aligned Industries & Assets	🟢	– There are over 150 relevant assets mapped within this study. We note strengths in defence and security, aerospace, advanced manufacturing and professional services. – There is also strong demand for cyber professionals in the region, with c. 10% of cyber security vacancies posted.
External Investment Raised by Cyber Security Sector	🟡	– Cyber security businesses raised £38m raised in external VC investment in 2022 – making this the third largest region in the UK. – However, historic investment trends have been lower, and continued emphasis should be placed on supporting external investment across the sector.

Inward Investment	🟢	- Of the cyber security businesses with an active office in the region, 23% (68) are large – highlighting considerable inward investment. It has a strong track record large multinational businesses to the region with active presence in cyber security (e.g. Cisco, BT, BAE Systems, IBM, Darktrace, Deloitte, PwC, KPMG, EY, Capgemini, Microsoft, Ericsson, QinetiQ, and Thales all have an active presence). - Further, recent investments by NCF, GCHQ and the major universities will have a ‘crowding-in’ effect on private investment.
R&D activity: Volume & Value of Cyber Security Research Projects	🟡	- The region has participated in 8% of the UK’s cyber security projects – the LQ suggests that this level of activity is lower than expected given the national average. However, the projects that the North West has participated in amount to 16% of the total funding given to cyber security projects in the UK. - Whilst this contains some interesting and significant companies (e.g. NCC Group, Sellafield, HP), the count of projects is relatively low, suggesting a need for universities and public sector to further partner or include private sector organisations within research projects.
Evidence of support infrastructure (e.g. accelerators, initiatives)	🟢	- We identify at least 20 high quality co-working and incubation spaces with a digital and cyber security focus, including the newly opened Digital Innovation Security Hub (DiSH) at Heron House, Fraser House and InfoLab21 in Lancaster, and several Bruntwood SciTech sites in Cheshire (Alderley Park), Liverpool (Science Park), Manchester (Circle Square, Citylabs and Manchester Science Park), and SciTech Daresbury. - Sustained resource-based funding to ensure these spaces and initiatives are maximised is recommended to sustain these investments, and maximise impact.

Skills and Access to Talent:		
Number of universities offering cyber security and related courses	🟢	- The North West has ten higher education institutes that offer cyber security and computer science courses at undergraduate and/or postgraduate level. There are a further two universities in the region that offer only computer science courses, Cumbria University and Liverpool Hope University.
Number of cyber security (and computer science) graduates	🟡	- **In the academic year 2020/21, there were almost 13,500 students enrolled at all levels in cyber security and computer science courses in the North West.** This figure is growing each year, with approximately 12,000 students enrolled in the previous year. This suggests that the volume of students enrolled in cyber and computer science courses has increased by c. 13% in the most recent year. - **The North West also produced 3,390 graduates[24] in cyber security and computer science in 2020/21 (approximately 10% of the UK supply).** This figure is also growing, particularly at postgraduate level.
Graduate outcomes (including regional retention)	🟢	- 72% of graduates that studied cyber security or computer science courses in the North West reported being in full-time employment. - Approximately 7% stated that they were unemployed. - For the c. 1,000 that studied cyber security or computer science in the North West and responded to the Graduate Outcomes Survey, 540 (54%) stayed in the region, 12% reported to have left the UK to work internationally, and the remaining 34% work in other regions of the UK, including 10% that moved to London. - However, the region does attract other graduates from areas such as Yorkshire, and the West Midlands – with Manchester being particularly attractive to graduates.
Evidence of wider skills and retraining initiatives	🟡	- The North West has a strong base of further education, apprenticeship, and reskilling programmes. - However, these could be scaled further to help meet the skills gap and access to talent.

[24] H325 in cyber security and 3,065 in computer science.

6.2 INTERNATIONAL CASE STUDIES

There are a range of successful regional cyber ecosystems globally. We set out some case studies below:

Maryland, Virginia (US)

- Maryland's cybersecurity network includes "12 major military installations; 400 Federal, academic, and private research centres; and 50 Federal agencies. The University of Maryland is headquartered between the DoD's Cyber Command in Maryland and the Cyber Corridor in Virginia." (UoM)
- Virginia is also home to over 650 cyber security companies[25], the highest per capita in the United States.
- "Established in 2012 through a partnership with the FBI, the Virginia Cyber Security Partnership is a collaboration between public and private sectors designed to establish trust for combating Cyber threats. The Partnership has more than 220 active members, and has held more than 35 events throughout the Commonwealth."
- Virginia has an estimated 67,850 people working in cyber security alone, and many of Virginia's universities are at the forefront of cyber security research and development. Virginia's population of more than 8.2 million and a workforce of more than 4.2 million.
- **This means that Virginia, with a very similar population to the North West of England, has a cyber security workforce approximately five times larger. This provides an opportunity for the North West to target significant cyber security workforce growth.**

Israel

- Israel is one the world's largest cyber security ecosystems. In 2022, Israeli cyber security firms raised $3.2bn.
- There are over 400 cyber security firms in Israel, with significant clusters in areas such as Beer Sheba, Tel Aviv, Petah Tikva and Netanya.
- Israel places a strong emphasis on higher education, research and development, investment and defence. In early 2023, the Israeli government announced that Unit 8200 (the intelligence function of the Israeli Defence Forces) are now training over 20,000 Israeli students[26] to boost the country's cyber defence capabilities.

Cyber Ireland

- Ireland has a thriving cyber security ecosystem, with almost 500 companies employing over 7,500 people, generating over €1.1bn in GVA for the Irish economy.
- It has significant clusters driven by both FDI activity and emerging indigenous start-ups, particularly in Dublin and Cork. This is supported by cluster initiatives such as Cyber Ireland, and focus on higher education provision.
- Cyber Ireland has set a target to reach 17,000 FTEs by 2030, and the North West's cyber ecosystem is comparable in size and dynamic to the wider Irish cyber ecosystem.

[25] https://www.cyberva.virginia.gov/media/governorvirginiagov/cyber-va/documents/virginiacybersecurity_printfinal-4.pdf

[26] https://www.jpost.com/israel-news/article-730160

07
Economic Potential and Growth Ambitions

7.1 INTRODUCTION

The previous sections set out a baseline for the region's cyber security ecosystem, which suggests there is considerable opportunity to grow the ecosystem further.

The NCSC's innovation partner, Plexal, has set out the key ingredients that any successful ecosystem should contain:

INGREDIENTS OF A SUCCESSFUL ECOSYSTEM:

- **Mission:** a defined outcome, on a global scale, that many people will be inspired by.
- **Infrastructure:** a physical place, connectivity, transport, power, labs, flexible workspace, testbed space and events space.
- **Leadership:** an identifiable person or organisation that sets the tone, the target and the pace.
- **Influence:** being respected enough to inform legislation, standards, reform and policy.
- **Finance:** access to funds so that actors in the ecosystem are incentivised and able to participate
- **Intellectual property:** enabling new products to be built.
- **Customer focus:** never forget to understand who your customer is and what they need.
- **Network of networks:** interconnections to adjacent ecosystems to create value.
- **Experimentation:** enable trials, labs, proofs-of-concepts.
- **Programme:** a thematic approach to creating progress - it could an incubator, accelerator or an innovation challenge.
- **Diversity of thought:** you should always bring groups together that wouldn't normally interact.
- **Measurement:** measure everything.

Sourced from NCSC For Startups: An Ecosystem Based Approach to Cyber Security (Andrew Roughan, Plexal)

The Cyber Corridor initiative provides a sense of mission – **to grow the North West's cyber security ecosystem, to nurture and attract talent, and to develop leading cyber security capability driven by world-leading research and innovation.**

It will also maximise the **infrastructural** investments made by the private sector, academia, and organisations such as the NCF and GCHQ – and unite these under a shared leadership and influence through the Cyber Corridor network. It will also promote skills, diversity, and access to cyber security as a career across the entire region.

The Cyber Corridor initiative will also use this research to measure and test growth in the coming years, and we set out the current and potential growth scenarios for the region with respect to its cyber security ecosystem.

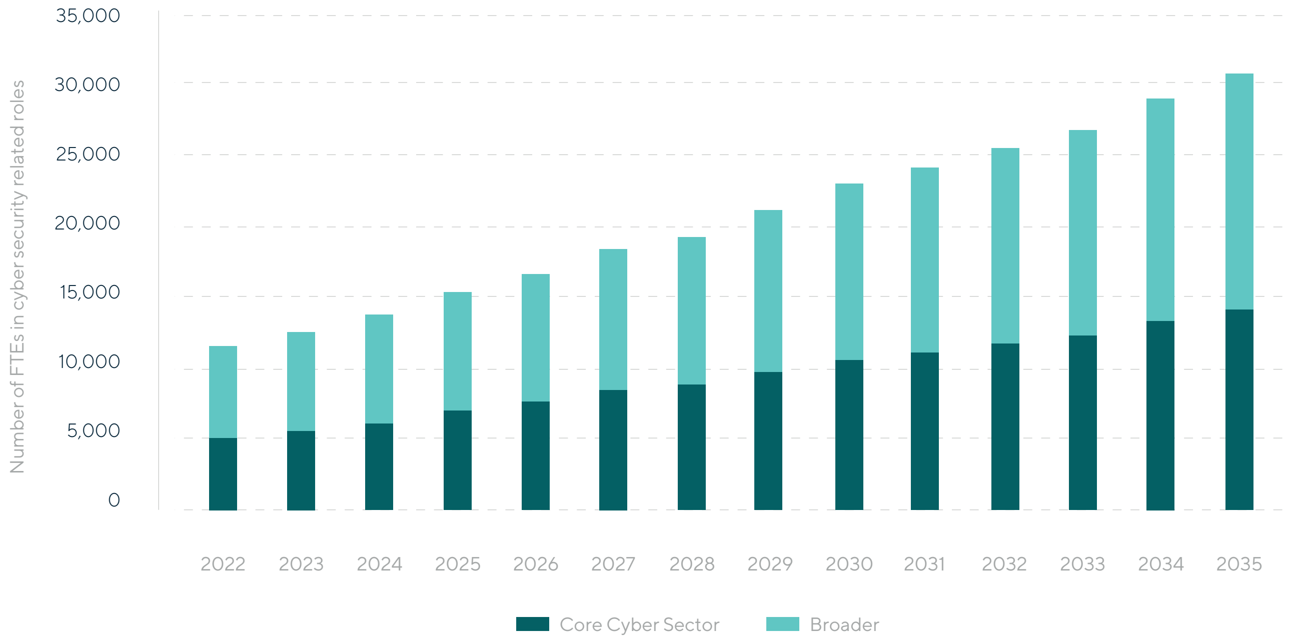
Overall, we estimate that the cyber security ecosystem could support over 30,000 jobs in the region by 2035, generating c. £2.7bn per annum in direct GVA.

	CURRENT (2022)	TARGET (2035)
Employment	12,000 FTEs in the wider cyber ecosystem (i.e. 5,000 in cyber sector and 7,000 in broader economy)	30,000 FTEs (13,000 in cyber sector and 17,000 in broader economy)
Gross Value Added	£760m (estimate)	£2.7bn

EMPLOYMENT

- We estimate the current cyber security workforce in the North West consists of c. 12,000 FTEs (approximately 5,000 within the cyber security sector based on the DSIT Cyber Security Sectoral Analysis, and a further 7,000 in wider sectors based on the DSIT Cyber Skills in the UK Labour Market research).
- Since the Cyber Security Sectoral Analysis was first published in 2017, employment has typically grown by approximately 10% per annum.
- For the c. 5,000 working within the cyber security sector, we assume this could grow by c. 10% per annum until 2030, and 5% per annum thereafter (until 2035). This growth trend suggests the cyber security sector in the North West could have approximately 13,700 cyber security professionals.
- For the c. 7,000 cyber security professionals working in wider sectors in the region, we apply a mid-growth estimate of 7% per annum to 2035. Much of the growth within the wider cyber security ecosystem in the North West is expected to be generated through investments made by NCF in Samlesbury, and GCHQ in Manchester.
- This growth trend suggests wider sector employment for cyber security professionals could reach c. 16,600 FTEs by 2035.
- **In total, this suggests an indicative cyber security related employment target for the North West of c. 30,000 FTEs by 2035.**
- However, this will require substantial investment in skills and workforce planning to ensure that the region develops greater volumes of talent, and attracts people to the North West.

EMPLOYMENT GROWTH SCENARIO TO 2035



Source: Perspective Economics scenario to 2035.

7.2 GVA POTENTIAL

Achieving 30,000 FTEs by 2035 would also stimulate significant economic growth for the region. As set out previous, cyber security is a high-value sector for the North West economy, and this is reflected in employer demand, salaries, and Gross Value Added.

- The DSIT Cyber Security Sectoral Analysis (2023) estimates that GVA per employee within the UK sector is approximately £107,400. This typically consists of salary / remuneration and firm-level profitability.
- Within the North West, we estimate that GVA per cyber security role is approximately £96,700 (c. 90% based on historic data[27]).
- Further, we also estimate that average North West cyber security related salaries are approximately £39,600[28].
- **As a conservative estimate, we calculate baseline (2022) direct GVA for the NW cyber security ecosystem at £760m[29].**

[27] E.g. £54,500 (NW) / £60,100 (UK) used in the 2022 study = c. 91%. (rounded down to 90%).

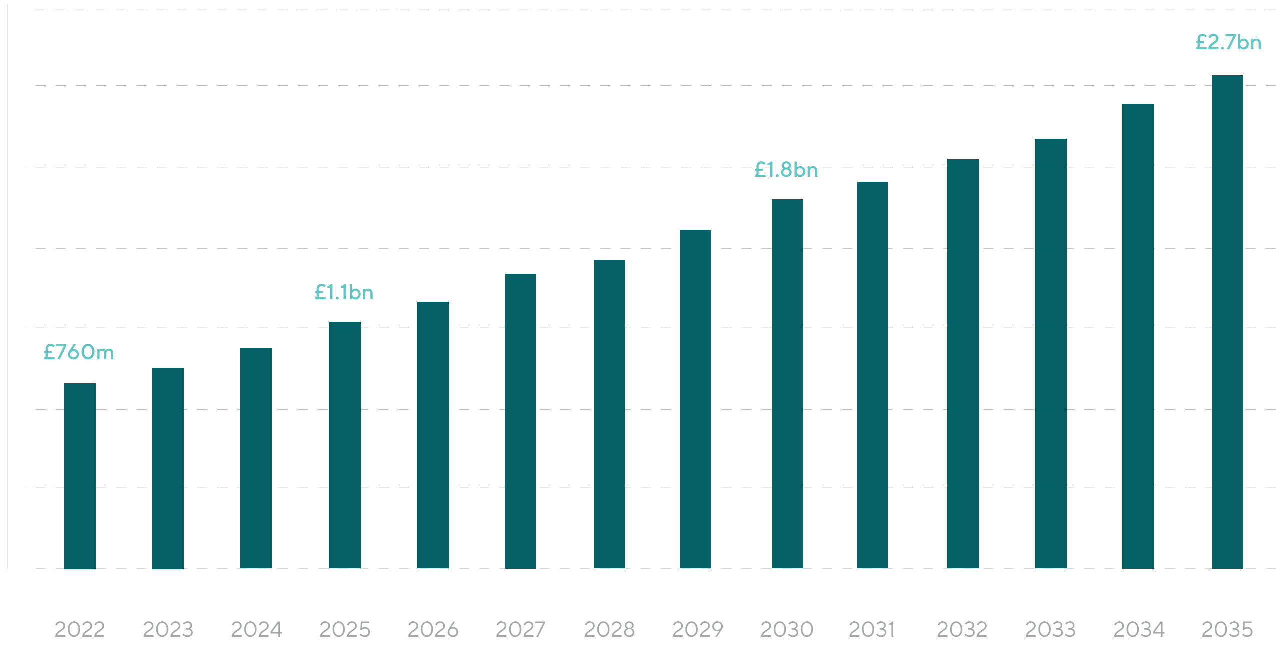
[28] This uses the broader cyber security vacancy average remuneration figure of c. £43,500 within the Cyber Skills in the UK Labour Market research and applies a 90% weighting.

[29] Calculated using the (c. 5,000 FTEs in cyber security sector * £96,700) + (7,000 wider roles x salary only, £39,150) = £735m.

GROWTH POTENTIAL

- Assuming a 2.5% salary increase for the cyber security sector, and 2% elsewhere, and assuming employment grows in line with the previous scenario – we estimate that direct GVA from the region's cyber security ecosystem could reach c. £2.7bn per annum[30] by 2035.
- **Over the period from 2022 – 2035, this could generate cumulative GVA in excess of £22.4bn for the region.**

GVA GROWTH SCENARIO TO 2035



Source: Perspective Economics scenario to 2035.

08
Gap Analysis

An effective North West Cyber Corridor will be made possible by the strong regional specialism in cyber across the public sector, the private sector, and academia.

Further, the focus on secure digitalisation as well as 'pure-play' cyber security means that the region is uniquely placed to support sectors such as manufacturing, aerospace and defence, and professional services, which in turn will create more opportunity for the growth of cyber and digital start-ups and spinouts.

We set out some of the key considerations for the success of the Corridor below.

Political and Policy Factors:

There are a range of political and policy factors that may impact the North West Cyber Corridor. The Strategic Context section highlights that there are several policies in place with the aim of promoting growth in the cyber security sector, both at a regional level and at national level.

- The realisation of the Cyber Corridor will require collective leadership throughout the North West. With 23 local authorities, five LEPs, and two combined authorities in the region, it is of utmost importance that there is consistency across the board regarding policies and that collaboration is fully embedded, given the collective strength and opportunity for cyber security across the entire North West.
- There is a need to align regional and national policies so that the ambitions of the Cyber Corridor are known and achieved through both regional and national initiatives. This is particularly important as the region seeks to grow its cyber security workforce, and meet the skills challenges ahead. Strategic alignment will ensure that the region is well-placed to avail of skills and education funding, as well as secure relevant support for growth and infrastructure projects.
- Recognition at a national level will help to strengthen the North West's position as not only a leader in cyber security in the UK, but also as a world leader in cyber security. The Cyber Corridor is also a major location for securing the UK, through initiatives such as the National Cyber Force. Long-term funding in national security and defence should therefore consider the role of the region's security sector and skills base.

Economic Factors:

- Supply side analysis has highlighted the **cyber skills shortage** across the UK, and immediate actions should be undertaken with respect to skills provision to grow the Cyber Corridor sustainability e.g. support for university provision, reskilling and retraining initiatives, support for military leavers, and the role of apprenticeships.
- **Whilst high salaries can be positive with respect to productivity and living standards, higher salaries in private sector roles** can result in skills shortages for technical cyber security roles in the public sector. Therefore, enhanced engagement between industry, academia, and public sector is required to help promote knowledge exchange and innovation to help grow the entire ecosystem, and ensure access to talent.
- This report highlights the role of 'crowding-in', where public investments in cyber security may further attract inward investment. These should be monitored and maximised. Further, the cyber security sector should be support to access external **investment** and growth, through initiatives such as Cyber Runway, DiSH, and NCSC for Start-Ups.
- However, further action to support businesses engage with R&D and innovation projects in cyber security could be advantageous to maximise innovation-led growth, and commercialisation of the region's world-leading cyber security research.

Social Factors:

- The Cyber Corridor can undertake a range of actions to help improve the diversity and access to roles within the cyber security ecosystem. This report highlights that gender diversity in particular remains a challenge within the workforce and graduate supply. This could include initiatives to increase awareness of cyber security as a career (e.g. alongside industry and ecosystem partners), promoting good practice, supporting retraining initiatives, and encouraging diversity in cyber leadership roles.
- Where the region can meet the ambition of c. 30,000 roles by 2035, this offers significant opportunity to promote access to cyber security across the wider region e.g. working with partners to offer skills opportunities – particularly within areas of deprivation or un/underemployment, and supporting those out of work into roles.
- There is also a need for the Cyber Corridor initiative to benefit wider society and businesses. For example, initiatives such as Greater Manchester and Lancashire Cyber Foundry have been important in supporting a range of SMEs benefit from cyber security and secure digitalisation more generally.

Technological Factors:

- This research has highlighted that the region is home to both pure-play cyber security firms, and organisations with wider offerings that require security solutions. In addition, the region has the potential to become a hotbed for technological innovation in approaches aligned to industrial strengths. For example, the defence and security sector will have high demand for intelligence and security analysts, and advanced manufacturing firms will have demand for those with skills in SCADA and ICS.
- As such, growth in the Cyber Corridor has the potential to improve efficiencies and specialism among broader sectors, as well as reducing attack vectors.
- There has been a surge of innovation in the region's digital sector with new technologies such as AI, automation, sensors, and 5G, all of which are used in vehicles, manufacturing, and energy. Many of these technologies require more stringent cyber security than they currently have, and thus the tech industry will benefit from working close with the Cyber Corridor initiative.
- To further embed cyber security within the region's supply chains, and maximise use of digital assets, the Corridor should work alongside initiatives such as the North West Cyber Security Cluster, and the North West Cyber Resilience Centre, as well as partners such as UKRI, STFC, and Innovate UK KTN, and the region's LEPs and combined authorities.

09 Next Steps

This report provides an actionable baseline for the North West Cyber Corridor. It highlights unique strengths and opportunities to grow the cyber security ecosystem in the years ahead. We set out some initial recommendations and suggested actions to help develop the Corridor initiative.

01

Develop an agreed governance structure and strategy for the North West Cyber Corridor

This report evidences that there is a substantive baseline to build upon; however, it is now essential to develop a shared identify and structure for the Cyber Corridor initiative. Key partners within the current working group should now consider the next steps to establish an agreed governance structure (encompassing regional and sub-regional leaders across public and private sectors and academia), as well as developing an initial strategy of actions for the Cyber Corridor.

02

Build a coalition of cyber security ecosystem partners

The region is home for five distinct sub-regions, all with varying cyber security strengths, capabilities and interests. We recommend that the group confirms its geographic parameters, and widens its membership structure to ensure participation from stakeholders across the region.

03

Develop a Growth Strategy

This report provides some initial targets for growth, including reaching 30,000 FTEs by 2035, and for the cyber security ecosystem to drive c. £2.7bn in GVA per annum.

However, this will require a Growth Strategy, with consideration of areas for co-investment, skills initiatives, and identifying priority areas for intervention and support from local, regional and national partners. This should also ensure that the Cyber Corridor is well connected to national initiatives, and has a number of projects in relation to infrastructure, skills, and ecosystem ready to commit funding and participation against.

04

Establish actions across a number of distinct themes

We also recommend that the Cyber Corridor commits to actions against a number of agreed thematic areas – to ensure that stakeholders can best support impactful projects. This might include Ecosystem Development, Skills, Research and Innovation, and Diversity. This is particularly significant within skills – where we expect that the region will need to explore how to encourage a further 1,000 – 1,200 individuals (in addition to existing provision) to train or move into cyber security related roles each year to meet demand.

05

Brand, Identity, and Vision

The Cyber Corridor initiative will require a distinct brand and identity, and have an agreed vision to enable a successful ecosystem. The group should explore perceptions of the 'Corridor' initiative, and test whether this resonates with potential stakeholders – or if the description could be varied to allow for full engagement across the North West, whilst ensuring equitable access and participation across sub-regions.

06

Resourcing

It is also important that the Cyber Corridor initiative has sufficient resourcing following strategy development. This could include outreach and engagement roles to ensure that businesses, public sector, and academic organisations advancing the cyber security ecosystem are well engaged and participating together.

10 Appendices

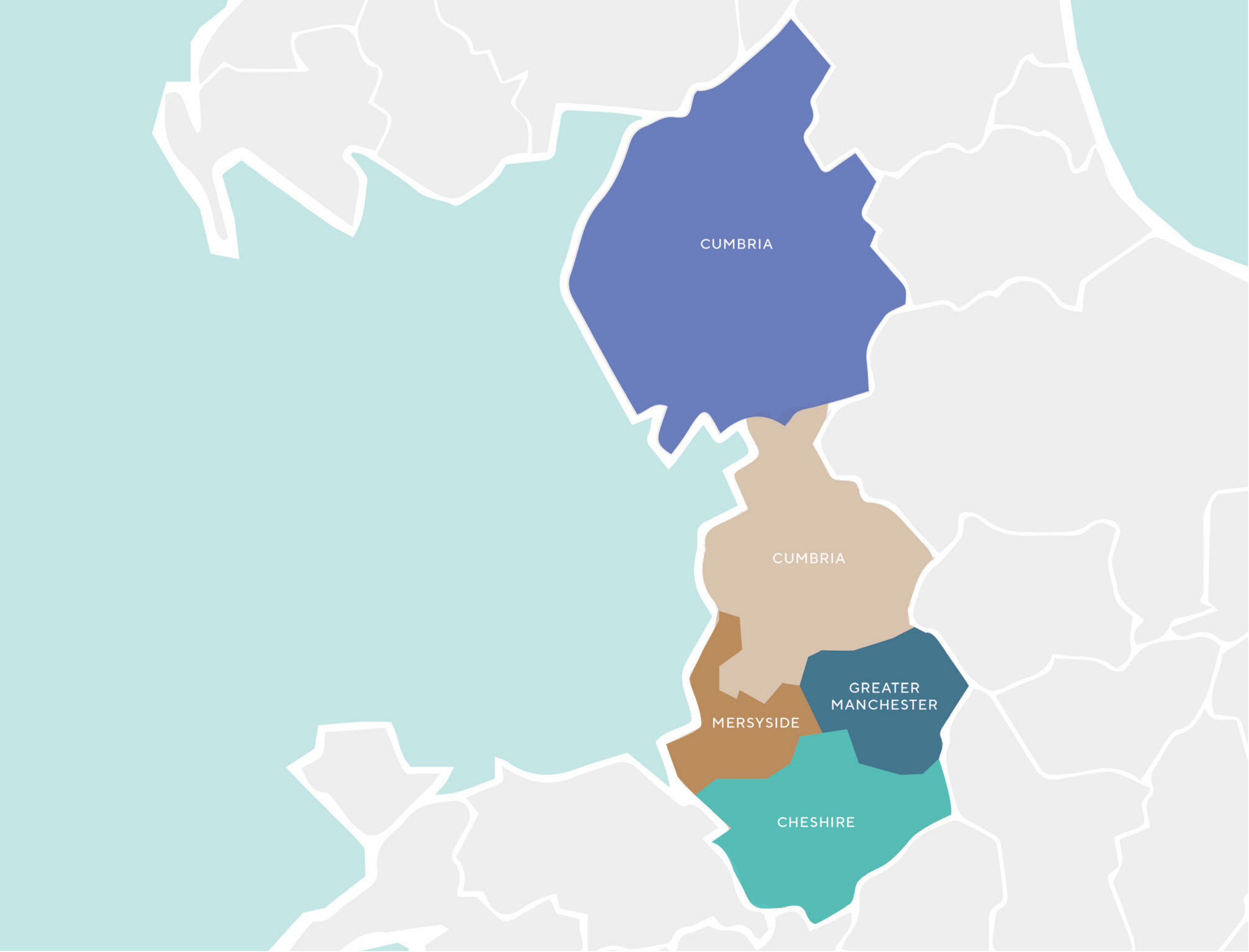
APPENDIX A: GEOGRAPHY OF THE NORTH WEST

The North West of England consists of five administrative countries: Cheshire, Cumbria, Greater Manchester, Lancashire, and Merseyside. There are also five Local Enterprise Partnerships (LEPs) in the region: Cheshire & Warrington, Cumbria, Lancashire, Greater Manchester, and Liverpool City Region.

Within the North West, there are several enterprise zones. These include:

- Cheshire Science Corridor
- Corridor Manchester
- Lancashire Enterprise Zone
- Manchester Airport City
- Mersey Waters Enterprise Zones

The Cyber Corridor is also home to the North West Cyber Security Cluster, one of UKC3's recognised regional clusters.



APPENDIX B: KEY ECONOMIC STATISTICS FOR THE NORTH WEST ECONOMY

The North West contributes an estimated £228.3 billion to the UK economy (9.5%) making the region the largest regional UK economy outside of London and the South East.

The region's unemployment rate of 3.5% is lower than the UK average by 1% (2022). However, the region has an employment rate of 74%, which is 1.1% lower than the national average of 75.1%, suggesting a need to support the economically inactive into roles.[31]

BUSINESSES

The number of businesses in the region has seen a steady increase, growing by 1.5% from 267,000 in 2020 to 271,000 in 2022 . Within the North West, 89% of businesses were micro enterprises (241,185), 9% were small enterprises (24,345), 1.6% were medium enterprises (4,375), and 0.4% were large enterprises (1,040).

The composition of enterprise sizes in the North West is relatively similar to the UK average. The North West also had the second highest business birth rate at 12.9% in 2020, coming second to London's business birth growth of 14%. This may suggest that the region fosters entrepreneurism, something that has the potential to boost the development of the Cyber Corridor.

INDUSTRIAL COMPOSITION

Within the North West, the industry with the largest number of businesses is the wholesale and retail trade sector. Table 1 sets out the number of businesses in each industry in the North West in 2021, compared with the UK.

Location quotients (LQ) are used to show whether the North West has a high or low concentration of businesses in each industry relative to the UK average. A LQ greater than 1 signals a level that exceeds what would normally be expected nationally, while below 1 indicates a lower concentration relative to the national average.

The location quotient shows that the North West has a large proportion of businesses in water supply, wholesale and retail trade, and financial and insurance activities. It also indicated that sectors such as mining and quarrying, electricity, information and communication, and public administration and defence are lagging the national average.

TABLE 1: UK BUSINESS COUNTS – ENTERPRISES BY INDUSTRY (2021)

INDUSTRY	NW	UK	LOCATION QUOTIENT
Financial and insurance activities	7,430	61,315	1.24
Water supply; sewerage, waste management and remediation activities	955	8,275	1.18
Wholesale and retail trade; repair of motor vehicles and motorcycles	46,575	406,420	1.17
Transportation and storage	15,310	138,405	1.13
Human health and social work activities	11,600	104,550	1.13
Accommodation and food service activities	18,275	167,005	1.12
Manufacturing	15,130	140,095	1.1
Other service activities	11,535	108,280	1.09
Administrative and support service activities	23,135	230,220	1.03
Real estate activities	10,435	105,370	1.01
Education	4,520	45,495	1.01
Professional, scientific, and technical activities	41,460	452,975	0.93
Construction	32,360	359,710	0.92
Arts, entertainment, and recreation	5,355	68,260	0.8
Agriculture, forestry, and fishing	10,870	141,030	0.79
Public administration and defence; compulsory social security	560	7,695	0.74
Information and communication	15,020	212,960	0.72
Electricity, gas, steam, and air conditioning supply	355	5,835	0.62
Mining and quarrying	70	1,250	0.57
Total			

Source: Nomis, UK Business Counts - enterprises by industry and employment size band.

Table 2 sets out jobs by industry in the North West as of June 2022. This highlights that there are over 3.8 million jobs in the region. The highest proportion of jobs, 15.1%, are within the wholesale and retail trade, vehicle repair industry.

The location quotients highlight that when compared with the UK, the North West has a much lower concentration of jobs in agriculture, forestry and fishing, mining and quarrying, and information and communication.

The manufacturing, wholesale and retail trade, and health and social work sectors have more jobs in the North West than the national average, as shown by the differences for these areas.

Significantly, this suggests that North West has approximately 54,000 fewer people working in information and communication than would be expected if it were in line with the UK average.

However, this also reflects an opportunity to both enhance digitisation within sectors, as well as explore opportunities for investment in job creation in digital roles, particularly in areas such as Manchester and Lancaster.

TABLE 2: WORKFORCE JOBS BY INDUSTRY SECTION (SIC2007) – SEASONALLY ADJUSTED (JUNE 2022)

INDUSTRY	NW	UK	LOCATION QUOTIENT	IMPLIED DIFFERENCE
Electricity, gas, steam and air conditioning supply	20,424	139,289	1.25	4,085
Manufacturing	346,095	2,616,352	1.22	62,219
Wholesale and retail trade; repair of motor vehicles and motorcycles	585,526	4,765,171	1.14	69,798
Human health and social work activities	545,065	4,615,996	1.09	42,827
Arts, entertainment and recreation	115,244	1,009,436	1.07	7,683
Transportation and storage	209,421	1,816,234	1.06	11,635
Administrative and support service activities	358,326	3,225,133	1.02	7,790
Professional, scientific and technical activities	368,813	3,324,600	1.02	7,764
Accommodation and food service activities	264,866	2,468,634	0.99	-3,895
Public administration and defence; compulsory social security	168,191	1,638,674	0.93	-11,734
Education	312,605	3,078,224	0.93	-23,445
Other service activities	84,708	876,166	0.92	-7,701
Water supply; sewerage, waste management and remediation activities	20,881	230,302	0.83	-4,176
Real estate activities	57,542	636,966	0.83	-11,508
Financial and insurance activities	93,870	1,068,277	0.80	-23,468
Construction	195,532	2,265,204	0.79	-50,838
Information and communication	120,418	1,603,685	0.69	-54,382
Mining and quarrying	2,141	56,481	0.50	-2,141
Agriculture, forestry and fishing	17,088	338,886	0.44	-21,360
Total	**3,888,000**	**35,827,217**		

Source: Nomis, UK Business Counts – enterprises by industry and employment size band. https://www.nomisweb.co.uk/sources/ukbc

APPENDIX C: LIST OF ASSETS IDENTIFIED

ASSET	TYPE	LOCATION
Aeroco Group International	Aerospace	Stockport
Northwest Aerospace Alliance	Aerospace	Lancashire
Manchester Digital	Co-working spaces	Manchester
The Hive	Co-working spaces	Lancaster
Beehive Lofts	Co-working spaces	Manchester
Cheshire SciTech	Co-working spaces	Macclesfield
Colony	Co-working spaces	Manchester
Department	Co-working spaces	Manchester
DiSH	Co-working spaces	Manchester
FlagShip Manchester	Co-working spaces	Manchester
Fraser House	Co-working spaces	Lancaster
Infolab21	Co-working spaces	Lancaster
Liverpool SciTech	Co-working spaces	Liverpool
Lofthouse	Co-working spaces	Stretford
Manchester SciTech - Circle Square	Co-working spaces	Manchester
Manchester SciTech - Citylabs	Co-working spaces	Manchester
Manchester SciTech - ID	Co-working spaces	Manchester
Manchester SciTech - Science Park	Co-working spaces	Pencroft Way
MediaCityHQ	Co-working spaces	Salford
Regus - Docklands Preston	Co-working spaces	Preston
NWCRC	Cyber Security Services	Oxford Road
HOST Cyber	Cyber Security Services	Salford
QINETIQ Ltd	Defence & Security Company	Cumbria
BAE Systems	Defence and Security Company	Blackburn
Thales	Defence and Security Company	Manchester
The Defence Works	Defence and Security Company	Salford
Capslock	Education	Manchester
GM Stem Centre	Education	Manchester
UK Skills Academy	Education	Preston
Blackpool and the Fylde College	Education	Blackpool
Blackburn College	Education	Lancashire
Custodia Technology	Education	Cheshire
Hugh Baird College	Education	Liverpool
Macclesfield College	Education	Macclesfield
Nelson and Colne College Group	Education	Nelson
Tameside College	Education	Ashton-under-Lyne
Trafford College	Education	Altrincham
Museum of Science and Industry	Education	Manchester
Jacobs	Engineering Company	Cumbria
Actemium	Engineering Company	Preston
GMET Group	Engineering Company	Millom
Sci-Tech Daresbury	Enterprise Zone	Keckwick Lane
Blackpool Airport Enterprise Zone	Enterprise Zone	Blackpool
Cheshire Science corridor	Enterprise Zone	Macclesfield
Hillhouse International Enterprise Zone	Enterprise Zone	Thornton-Cleveleys
Manchester Corridor	Enterprise Zone	Manchester

ASSET	TYPE	LOCATION
Mersey Waters	Enterprise Zone	Bolton
Samlesbury Enterprise Zone	Enterprise Zone	Cumbria
Secure Digitalisation University Enterprise Zone	Enterprise Zone	Ellesmere Port
Warton Enterprise Zone	Enterprise Zone	North West
Liverpool Local Government	Government Organisation	Widnes
Wigan Local Government	Government Organisation	Liverpool
Sefton Local Government	Government Organisation	Preston
Cumbria Local Government	Government Organisation	London
Blackburn with Darwen Local Government	Government Organisation	Rochdale
Stockport Local Government	Government Organisation	Manchester
Lancashire Local Government	Government Organisation	Birkenhead
Salford Local Government	Government Organisation	Manchester
Cheshire East Local Government	Government Organisation	Sandbach
Oldham Local Government	Government Organisation	Oldham
St Helens Local Government	Government Organisation	Saint Helens
Cheshire and Warrington LEP	Government Organisation	Cheshire
Blackpool Local Government	Government Organisation	Blackpool
Tameside Local Government	Government Organisation	Ashton under Lyne
Warrington Local Government	Government Organisation	Warrington
GCHQ	Government Organisation	Square
Manchester Local Government	Government Organisation	Manchester
Trafford Local Government	Government Organisation	Partington
Bury Local Government	Government Organisation	Bury

ASSET	TYPE	LOCATION
Bolton Local Government	Government Organisation	Bolton
Sellafield Ltd	Government Organisation	Cumbria
Chesire West and Chester Local Government	Government Organisation	Ellesmere Port
Defence Business Services	Government Organisation	North West
Halton Local Government	Government Organisation	Widnes
Knowsley Local Government	Government Organisation	Liverpool
Lancashire Enterprise Partnership	Government Organisation	Preston
NCSC	Government Organisation	London
Rochdale Local Government	Government Organisation	Rochdale
The Greater Manchester Cyber Security Advisory Group	Government Organisation	Manchester
Wirral Local Government	Government Organisation	Birkenhead
MadLab	Innovation and Technology	Manchester
PixelMill	Innovation and Technology	Manchester
Tech Nation	Innovation and Technology	England
Manchester Airport	International Airport	Manchester
Liverpool John Lennon Airport	International Airport	Liverpool
Honeywell	Manufacturer	Manchester
Lancashire Cyber Alliance	Not-for -Profit CIC	Preston
NWCSC	Not-for -Profit CIC	North West
PWC	Professional Services	Manchester
Grant Thornton	Professional Services	Manchester
Deloitte	Professional Services	Manchester

ASSET	TYPE	LOCATION
KPMG	Professional Services	Manchester
EY	Professional Services	Salford
Praetura Asset Finance	Professional Services	Blackburn
Lancashire Constabulary	Public Defence	Lancashire
RAF Woodvvale	Public Defence	Liverpool
MoD	Public Defence	Fylde
MoD	Public Defence	Lancaster
MoD	Public Defence	Preston
MoD	Public Defence	Wyre
MoD	Public Defence	Lancashire
Greater Manchester Police	Public Defence	Manchester
Fulwood Barracks	Public Defence	Preston
MoD	Public Defence	Manchester
Transport for Greater Manchester	Public Defence	Manchester
Future Everything	R&D Organisation	Manchester
Zaiku Group Ltd	R&D Organisation	Liverpool
Advanced Manufacturing Research Centre	R&D Organisation	Blackburn
Centre of Excellence in Digital Systems	R&D Organisation	Lancaster
Cyber Edge	R&D Organisation	Ormskirk
Fujitsu	Software company	Manchester
Hewlett Packard Enterprise (HPE)	Software company	Manchester
CGI UK Ltd	Software company	Manchester
CircleLoop	Software company	Rossendale

ASSET	TYPE	LOCATION
InKnowTech	Software company	Manchester
Pentagull	Software company	Blackpool
REDCENTRIC PLC	Software company	Harrogate
Relative Insight	Software company	Lancaster
Splunk	Software company	Salford
TymeOnline	Telecommunications	Blackburn
BT	Telecommunications	Manchester
TalkTalk Telecom Group Ltd	University	Salford
Lancaster University	University	Lancaster
The University of Manchester	University	Manchester
The University of Bolton	University	Bolton
Liverpool John Moores University	University	Merseyside
The University of Liverpool	University	Liverpool
University of Chester	University	Chester
The University of Central Lancashire	University	Preston
Liverpool Hope University	University	Liverpool
The Manchester Metropolitan University	University	Manchester
The University of Salford	University	Manchester
Edge Hill University	University	Ormskirk
Greater Manchester Cyber Foundry	University	Manchester
Siemens & Awen Collective	University Collaboration	Manchester
Sprite+	University Collaboration	North West
Centre for Digital Trust and Society	University Collaboration	Manchester
Cyber HQ	University Collaboration	Preston

APPENDIX D: GLOSSARY OF TERMS

ACRONYM	DESCRIPTION
ACE - CSE	Academic Centre in Cyber Security Education
ACE - CSR	Academic Centre in Cyber Security Research
DfE	Department for Education
DiSH MCR	Digital Innovation and Security Hub Manchester
DSIT	Department for Science, Innovation and Technology
DSTL	Defence Science and Technology Laboratory
EPSRC	Engineering and Physical Sciences Research Council
FTE	Full Time Equivalent
GCHQ	Government Communications Headquarters
GM	Greater Manchester
GVA	Gross Value Added
HEI	Higher Education Institution
HESA	Higher Education Statistics Agency
HPC	High Performance Computing
ICS	Industrial Control Systems
IDA	Industrial Digital Acceleration
IP	Intellectual Property
KTN	Knowledge Transfer Network
LCR	Liverpool City Region
LEP	Local Enterprise Partnership
LQ	Location Quotient
MI6	Secret Intelligence Service
MOD	Ministry of Defence
NCF	National Cyber Force
NWCSC	North West Cyber Security Cluster
RAG	Red Amber Green
SCADA	Supervisory Control and Data Acquisition
SCorCH	Secure Code for Capability Hardware
SIC	Standard Industrial Classification
SME	Small and Medium-Sized Enterprise
STFC	Science and Technology Facilities Council
TLC	The Lancashire Colleges
UCLan	University of Central Lancashire
UKRI	UK Research and Innovation
UoM	University of Manchester
UA92	University Academy92

Perspective
Economics