perspective economics

AUTUMN 2025

Lancaster University
North West Cyber Security Ecosystem Mapping

2025 Update

Contents

Executive Summary 4

1. Introduction & Background 8

2. The North West Cyber Corridor 10

2.1 Introduction & Scope 11

2.2 Methodology 12

3. Strategic Context 14

3.1 Introduction 15

3.2 Strategic Update 15

4. North West Cyber Corridor: Updating the Evidence Base 18

4.1 Introduction 19

4.2 Revisiting the Baseline 21

4.3 Cyber Security Businesses in the North West 24

4.4 Wider Cyber Security Assets in the North West 36

5. Demand & Supply of Cyber Security Skills 40

5.1 Introduction 41

5.2 Supply 44

6. Benchmarking the Region 48

6.1 Introduction 48

6.2 Key Markers 49

7. Economic Potential & Growth Ambitions 52

7.1 Introduction 53

7.2 Growth Potential 54

8. Progress & Next Steps 56

Executive Summary

The North West has firmly established itself as one of the UK's leading cyber security hubs, demonstrating significant growth, and strategic leadership since our 2023 baseline assessment. This update reveals a thriving ecosystem that has exceeded initial projections and is a critical region for UK national security and economic resilience. We find that:

- The region now hosts **378 cyber security businesses** (+27% growth), making it home to 18% of all UK registered cyber firms with a regional presence.
- Cyber security related employment has grown to **14,300 FTEs** (+19%), while direct Gross Value Added has reached **£1 billion** (+33%), highlighting growth in scale and productivity.
- For the first time, the North West captured the largest share of UK cyber security investment in 2024, securing **£102 million across 6 deals** (49% of national total).
- The imminent opening of the National Cyber Force headquarters in Samlesbury, alongside GCHQ's expanded Manchester presence, has positioned the region as a national hub for cyber operations and intelligence. This is complemented by over 170 supporting assets across research, innovation, and industry.
- The region demonstrates particular excellence in **threat intelligence and monitoring** (53% vs 44% UK average), **endpoint security** (33% vs 22%), and emerging **AI security capabilities.** Its universities have achieved the UK's highest proportional growth in cyber security course enrolments (+41%) and graduates (+80%), creating a strong talent pipeline.
- Conservative projections suggest the ecosystem will support **25,000 FTEs by 2035,** generating **£2.4 billion in annual GVA** and cumulative economic impact exceeding £19.8 billion over the decade. A stretch target of 30,000 FTEs remains achievable with sustained public investment and continued defence sector growth.
- The region's Cyber Corridor now represents a national asset requiring continued investment in skills, infrastructure, and public-private partnerships. With nearly half of UK civil service cyber vacancies now concentrated in the North West, the ecosystem is well-positioned to support the government's commitment to spend 5% of GDP on national security by 2035.

The North West is one of the UK's leading cyber security hubs.

This update reveals an ecosystem that has exceeded initial projections and is a critical region for UK national security and economic resilience.

378

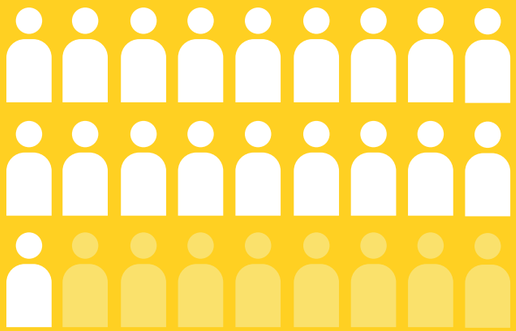
Cyber Security Companies in the North West

27% Growth

Since the 2023 baseline study.

18% of UK cyber firms

Have a regional presence in the North West.



6,700

People employed in the North West cyber security sector *(+34% increase in FTEs).*

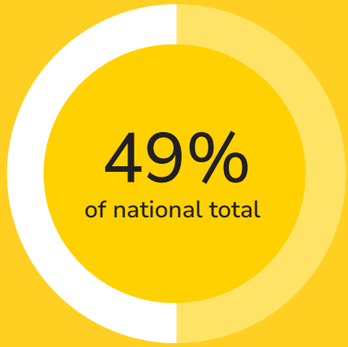
14,300

People employed in the North West cyber security workforce *(+19% across all sectors).*

£102m

Secured in cyber security investment.

For the first time, the North West captured the largest share of UK cyber security investment in 2024.



Areas of Excellence

- Threat intelligence & monitoring
- Endpoint Security
- AI Security Capabilities
- +41% cyber enrolments
- 80% growth in cyber graduates

Economic Projections for 2035

£19.8bn
Cumulative economic impact

£2.4bn
Annual GVA

25,000
FTEs by 2035

1. Introduction & Background

In recent years, the North West has emerged as one of the UK's most active regions for cyber security innovation, investment, and capability. This has been driven by an ecosystem with academic excellence, industry growth, public and private investment, and collaborative leadership.

In 2023, the North West Cyber Corridor Innovation Impact Study, delivered by Perspective Economics in partnership with Lancaster University and Plexal, provided a comprehensive assessment of the region's cyber ecosystem. This research found that the North West hosted almost 300 unique cyber security companies, making it the largest cyber cluster in the UK outside of London and the South East. It also highlighted how cyber capabilities in the region are deeply embedded in, and complementary to, key sectors such as aerospace and defence, energy and nuclear, financial services, and advanced manufacturing.

There is a strong and diverse mix of cyber security businesses represented across the region. Approximately half of the companies are 'pure play' firms focused solely on cyber (e.g. NCC Group and WithSecure), while the other half are 'diversified' firms operating across multiple technology areas. Many of the North West's larger employers—including BAE Systems, BT, Thales, Capgemini, and Deloitte—integrate cyber capabilities within their broader digital and technical portfolios, opening up opportunities to grow cyber capacity through both specialist and generalist pathways.

The ecosystem is underpinned by a rich set of assets and initiatives across the private and public sector, defence, and research institutions. These contribute to the region's cyber capacity—from Smart Cities in the Liverpool City Region, to the Hartree Centre's high-performance computing facilities in Daresbury, and the arrival of the National Cyber Force headquarters in Samlesbury. The region's universities also play a key role through research excellence, innovation partnerships, and building the skills supply —including cyber degree apprenticeships and specialised MBA programmes.

The 2023 baseline report estimated that approximately 12,000 full-time equivalent (FTE) roles are dedicated to cyber security across the North West, generating over £550 million in annual salaries and £760 million in Gross Value Added (GVA) for the regional economy.

This research explores how the North West has developed since the baseline study, and highlights the substantial progress made in the last two years – with 378 cyber security businesses amidst an active ecosystem now supporting over 14,300 FTEs in cyber security and generating over £1bn in annual direct GVA.

2. The North West Cyber Corridor

2.1. INTRODUCTION & SCOPE

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.

The North West of England has a well-established cyber security ecosystem, and following on from the 2023 baseline, this report (2025) provides an updated assessment of the size, scale, and growth potential of the ecosystem.

Within this assessment, we find a growing concentration of cyber security assets, businesses, research institutions, and innovation hubs, and revisit how the cyber security ecosystem is increasingly interconnected with wider technology sectors in the region, such as Artificial Intelligence (AI), defence, and advanced manufacturing. Overall, within this updated analysis, we find substantial growth in cyber related activity, with 378 cyber security companies with a presence in the region (+27% from baseline), and that 18% of UK registered cyber security businesses have at least one office in the North West.

This research builds on the baseline established in the North West Cyber Corridor Impact Study (2023), while adopting an updated approach to mapping the region's cyber and wider technology ecosystem. This includes an enriched evidence base that captures the North West's evolving position across cyber security, but also in key strategic domains such as AI, defence, and deep tech.

This updated report provides:

- An updated review of the businesses and assets in 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 North West, in addition to how the North West can support national security and defence policy, and unlock additional economic growth.
- Undertaking of benchmarking for the region.
- Analysis of the opportunities that the Cyber Corridor has developed in the last two years and could be well placed to take advantage of through 2035.
- Provision of recommendations and strategy for continuing to grow cyber security in the region.

The ecosystem continues to evolve, and there are significant opportunities in the years ahead for the North West, including the upcoming launch of the National Cyber Force in Samlesbury later this year.

2.2. METHODOLOGY

The research team led the baseline North West Cyber Corridor research exercise (2023), and also leads national studies for the Department for Science, Innovation and Technology for sectoral estimates for cyber security, cyber skills, Artificial Intelligence, semiconductors, and more.

As such, the research team has included an assessment of a range of key metrics, including:

- The estimated number of cyber security businesses active in the region, drawing on data from national reports including DSIT Cyber Security Sectoral Analysis (2025) and wider use of web and company data in the region.
- Cyber security workforce estimates, drawing on UK and regional data from the DSIT Cyber Skills in the UK Labour Market (2025) analysis.
- A broader tech ecosystem review, including AI and technology businesses, assets and infrastructure, and key organisations supporting skills, investment and growth in the region.
- The cyber security ecosystem's contribution to regional employment, revenue, and Gross Value Added.
- An analysis of external investment raised, grants secured, and research participation in publicly funded projects by registered cyber security businesses in the region.
- Review of the regional labour market through supply and demand factors. This includes review of higher and further education data, and job postings via the Lightcast platform.
- A review of the baseline projection scenarios to 2035 set out within the North West Cyber Corridor (2023) research.

This enables a time-series analysis of how the ecosystem is evolving, both in terms of economic value and its contribution to the UK's wider cyber and security ambitions.

3. Strategic Context

3.1. INTRODUCTION

The North West's cyber ecosystem is a key asset to the UK's approach to building resilience, economic security, and regional growth. This aligns with the priorities outlined in the National Cyber Strategy (2022–2030), published under the previous government, which sets out a vision to strengthen the UK's cyber ecosystem by investing in regional capabilities and facilitating collaboration across government, academia, and industry.

In May 2025, the Chancellor of the Duchy of Lancaster Pat McFadden MP spoke about the government's focus on using cyber security to drive economic growth at a speech at CYBERUK in Manchester, and announced that the government will publish a new National Cyber Strategy in late 2025. This is expected to focus on better dealing with security threats, including AI-driven and state-actor led attacks, improving defences and national security and defence, and supporting the cyber security sector to grow the UK economy.

The North West's growing concentration of cyber assets (explored in Chapter 4), institutions, and talent (explored in Chapter 5) reflects this ambition and demonstrates how national strategy can be supported through targeted regional activity.

3.2. STRATEGIC UPDATE

Within the baseline ecosystem report, there were a number of strategies identified at a regional and national level with high relevance to the ambitions of the North West Cyber Corridor. These included the National Cyber Strategy (2022), Government Cyber Security Strategy (2022-30), the Integrated Review of Security, Defence, Development and Foreign Policy (2021), in addition to regional local and digital strategies across Greater Manchester, Lancashire, Liverpool City Region, Cheshire and Warrington, and Cumbria.

Since this report, delivery has been ongoing on existing strategies, often through tangible innovation centres and programmes delivered by partners across the North West (see Section 4.4), whilst new strategies, legislation, and codes of practice have also been introduced and supported by national and regional partners. We summarise these below:

- **National Security Strategy (2025):** This commits to spend up to 5% of GDP on national security by 2035 (including 3.5% of GDP on defence and 1.5% on wider security and resilience, including cyber), setting a whole-of-government security framework. The IFS has estimated that 'increasing 'core defence' spending from 2.6% to 3.5% of national income would mean, in real terms, spending around an additional £30 billion a year'.[1] This could result in billions of additional investment in the aerospace, defence and security sectors in the North West over the coming decade, with the MoD currently spending approximately £3.8bn with North West defence suppliers in 2023/24[2].
- **Strategic Defence Review (2025):** This sets out spending 2.5% of GDP on defence by 2027, in addition to new measures to invest in the cyber and electromagnetic (CyberEM) domain, and strengthen defences in Critical National Infrastructure.

[1] https://ifs.org.uk/articles/response-government-commitment-spend-5-gdp-national-security

[2] https://www.gov.uk/government/statistics/mod-regional-expenditure-statistics-with-industry-202324/mod-regional-expenditure-with-industry-202324#mod-expenditure-with-uk-industry-by-region

> "The recent Strategic Defence Review has clearly stated what a vital role regional innovation ecosystems like Lancashire's have to play in strengthening national defence and security, by fostering local-national partnerships, and building critical mass in key technologies such as cyber."
>
> **Nick Miles, Deputy Director of the NCF**

- **Defence Industrial Strategy (2025):** The Ministry of Defence has set out its approach to making the defence industry an 'engine for growth', whereby increased defence spending can support a more 'competitive, integrated, innovative and resilient defence sector'. This strategy highlights the current £28.8 billion in MOD expenditure with UK industry in 2023/24, equivalent to about £420 per person. Of this, an estimated £3.8bn takes place in the North West, the third highest in the UK in absolute terms, and approximately £510 per person in the region (c. 20% higher than the UK per capita estimates). The Strategy also sets out increased targets for MOD expenditure with SMEs, investments in skills through the introduction of Defence Technical Excellence Colleges (DTECs), supporting defence innovation, and the introduction of new Defence Growth Deals to build on strengths in established regions.

- **Cyber Growth Action Plan (2025):** The Cyber Growth Action Plan is an independent research report exploring new areas for UK cyber growth, and will support the upcoming National Cyber Strategy.

- **AI Opportunities Action Plan (2025):** The Government has agreed to adopting all 50 recommendations to boost UK AI, including expansion of public AI compute (AIRR), creating AI Growth Zones, and developing a UK Sovereign AI unit.

- **AI Cyber Security and Software Security Codes of Practice (2025)** to support firms with voluntary baselines for securing AI systems and for software vendors (supply-chain resilience).

- **Upcoming National Cyber Strategy, and Defence Investment Plan:** The Government has signalled a new National Cyber Strategy focused on resilience and growth is set to be published later in 2025.

- **Greater Manchester's Cyber Strategy (2023–2028):** In August 2023, Greater Manchester Combined Authority published its Cyber Strategy setting out five pillars for collaboration, innovation and investment, increasing access into cyber careers, increasing diversity, and promoting the region's cyber capabilities globally.

- **Lancashire Cyber Partnership:** In 2023, Lancashire County Council (LCC); the Lancashire Enterprise Partnership (LEP); the University of Central Lancashire (UCLan); Lancaster University; BAE Systems; and the National Cyber Force (NCF) announced the formation of the Lancashire Cyber Partnership to 'to implement initiatives and strategies which will facilitate and boost cyber-led economic growth across the County's digital industries, technology supply chains, and broader disciplines'.

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

[4] A response to government commitment to spend 5 % of GDP on national security (2025), Institute for Fiscal Studies, https://ifs.org.uk/articles/response-government-commitment-spend-5-gdp-national-security

- **North West Regional Defence and Security Cluster (NWRDSC):** In late 2024, the North West Regional Defence and Security Cluster (NWRDSC) was formally launched is part of a nationwide network of defence and security clusters, supported by the Ministry of Defence (MoD) and the government's Defence and Security Accelerator (DASA).

- In May, Manchester hosted CYBERUK 2025, the UK's flagship cyber security conference, further reflecting the national and international regard for the region's capabilities.

Case Study: The North West as a Strategic Asset to National Defence & Security

The UK's **National Security Strategy 2025** makes clear that strengthening the country's industrial base and economic resilience is not just an economic goal but a strategic imperative for national defence[3]. The government explicitly frames **economic security as national security**, envisioning a "defence dividend" where increased investment in defence revitalises industrial communities across the country.
With this, the UK is targeting to spend 5% of GDP on defence by 2035, with 3.5% on 'core defence' and 1.5% on resilience and security. Both segments of this budget provide opportunities for the cyber sector, with the IFS estimating this could generate an additional spend of £30 billion annually by 2035[4], providing an opportunity for billions of additional spend and procurement in the North West.

The North West has long played a central role in UK national security and defence, with BAE Systems' Barrow-in-Furness shipyard building nuclear submarines for the AUKUS alliance, while the Warton and Samlesbury sites lead development of the Tempest future combat air system[5]. With the National Cyber Force's new headquarters in Samlesbury, this further solidifies the link between traditional defence manufacturing and cyber operations.

In November 2024, the region's leaders launched the North West Regional Defence and Security Cluster (NWRDSC), marking a strategic effort to unify and promote the North West's defence and cyber security strengths[6]. Backed by the Ministry of Defence's accelerator programme, the NWRDSC is part of a UK-wide network of clusters aimed at boosting innovation and investment in security sectors.

The NWRDSC's mission is to **strengthen the North West's profile in defence and cyber, promoting collaboration across industry, academia and government.** Key objectives include sharing intelligence and best practices among firms, accelerating commercialisation of R&D (particularly in dual-use technologies), and developing a skilled workforce pipeline to sustain long-term growth.

As global threats evolve, the North West's integrated strengths across defence, cyber, and advanced manufacturing position it as a cornerstone of the UK's long-term resilience.

[5] North West comes together to bolster its defence (2024), Lancashire Business View, https://www.lancashirebusinessview.co.uk/latest-news-and-features/north-west-comes-together-to-bolster-its-defence

[6] North West Regional Defence and Security Cluster (NWRDSC), https://northwestrdsc.co.uk/

4. The North West Cyber Corridor: Updating the Evidence Base

4.1. INTRODUCTION

In 2023, Lancaster University and Perspective Economics published the first 'North West Cyber Corridor Innovation Impact Study', providing an evidence base and a baseline for the North West's cyber security ecosystem. This included an analysis of cyber security businesses in the region, the workforce supply and demand, and wider factors such as investment, research, and innovation activity.

This evidence base was developed through tailored regional engagement, as well as a deep-dive of regional data gathered by Perspective Economics through national studies such as the DSIT Cyber Security Sectoral Analysis and Cyber Skills in the UK Labour Market research.

The North West Cyber Corridor Evidence Base (2023) also set out a series of potential targets for the region with respect to cyber security ecosystem growth. We explore the progress made to date against these ambitions.

This chapter explores how the landscape has changed in the past two years in the region, against the wider national and international context.

We find encouraging progress in the region, with increased productivity and employment, and several new regional startups securing customers and investment on the global stage. We also find shifts in business models, driven not only by increased AI adoption in the last two years, but also through a sustained focus among businesses in the region to enhance public and private partnerships, expand their service offering, and both embrace and secure new technologies.

Since the baseline, there has been significant activity across the North West cyber ecosystem from a range of partners on areas such as national security and defence, new infrastructure, skills development, novel research and innovation initiatives, start-up engagement, and more.

UPDATING THE NORTH WEST CYBER ECOSYSTEM

2018
Lancaster University, Manchester Met, University of Manchester, and University of Salford collaborate on the £6m Cyber Foundry project to help protect regional businesses.

2019
GCHQ opens a hub in Manchester, at Heron House, setting up collaborations with local high-tech start-up companies.

Lancaster University is designated University Enterprise Zone status from Research England in Secure Digitalisation.

2020
Building on the success of GM Cyber Foundry, the £2.1 million Lancashire Cyber Foundry launches to support regional SMEs.

2021
The North West Cyber Security Cluster (NWCSC) relaunches and has since hosted over 30 events and talks.

UKG announced the Integrated Review, committing to the development of the North West Cyber Corridor.

North West Partnership for Security and Trust launched with Lancaster University, University of Manchester, Manchester Met, University of Salford & GCHQ.

National Cyber Force announces plans to build HQ in Samlesbury, bringing over 3,000 jobs to the North West.

2022
The DSHIH (Digital Security Innovation Hub) opens – a £10m cyber innovation centre, collocated at Heron House with GCHQ, led by Barclays Eagle Labs, Plexal, Lancaster University, and the University of Manchester.

Launch of Lancashire Cyber Alliance to maximise the opportunities from the Cyber Corridor.

Lancaster University reveals 'once-in-a-generation' investment in data, cyber security, and protection science (worth over £19m and 60 jobs).

Lancaster University announces new multi-million pound teaching facilities to educate the next generation of computer science and cyber security students.

2023
Lancaster University launches the first Executive Cyber MBA and University Academy 92 (UA92) launches a BSc in Cyber Security.

Launch of North West Cyber Security Connect for Commercialisation (NW CyberCom).

Nebuaca, a Manchester-based cyber security business, secures a £4.4m investment to support continued growth.

Lancashire Cyber Festival & Lancashire Cyber Partnership announced.

GMCA launches the Greater Manchester Cyber Strategy 2023–2028.

Lancaster University and Plexal publish the North West Cyber Corridor Impact Study.

2024
Lancaster University and IN4 Group sign contract to develop tech talent through establishment of 24 CyberFirst Gold Hubs in each of the North West's Local Authority areas.

MIT joins the NW CyberCom to bring world-leading expertise into the development of place-based innovation ecosystems.

University of Manchester announces a £4.7 million investment in AI and trust capability to enhance research and teaching in humanities.

UCLan announces funding for new degree apprenticeships in cyber security and engineering.

Fhunded Live, Lancashire's new digital industries conference, brings over 100 business leaders together in Lancaster.

Lancaster University spinout company Mindgard wins 'UK's Most Innovative Cyber SME 2024' award at Infosecurity Europe 2024.

Cheshire-based PortSwigger secures £8bn in investment. Manchester-based Cultural raises £8m to support 'break-out growth', and Manchester-based Esportsfield raises £2.8m to help enterprises maximise ROI on security investment.

Lancaster invests £1m from the Regional Innovation Fund to develop a vibrant co-working and collaboration space for cyber security-related businesses and government organisations in Lancaster, as well as a shared Environment for New Security (LENS), and develops a new Decision Theatre and Digital Training Labs supported by a £4m grant from the Office for Students (OfS).

CyberFocus project launched with £4.9m in UKRI funding aimed at strengthening emerging and existing research and innovation clusters to kickstart economic growth and address regional needs.

2025
Lancaster University opens one of the largest educational facilities in the country to help train the next generation of computer science and cyber security students.

Lancaster University hosts cyber security training to equip nuclear industry professionals in line with the UK Government's Civil Nuclear Cyber Security Strategy.

Manchester hosts CYBERUK 2025, the UK's flagship cyber security conference.

Lancashire Cyber Festival hosts more than 200 businesses, investors, policymakers, and academics from across the UK to become a global leader in cyber-enabled defence and security.

The National Cyber Force will establish its HQ in Samlesbury, bringing over 3,000 jobs and new growth into the region's cyber ecosystem.

4.2. REVISITING THE BASELINE

The research team has reviewed the state of the North West Cyber Corridor ecosystem as of July 2025 across a number of key metrics set out in the baseline report. This review has included an assessment of:

- The estimated number of cyber security businesses active in the region, drawing on data from the DSIT Cyber Security Sectoral Analysis (2025) and wider use of web and company data in the region.
- Cyber security workforce estimates, drawing on UK and regional data from the DSIT Cyber Skills in the UK Labour Market (2025) analysis.
- A place-based review of the broader tech ecosystem in the North West, including AI and technology businesses, assets and infrastructure, and key organisations supporting skills, investment and growth
- The ecosystem's contribution to regional employment, revenue, and Gross Value Added modelled by Perspective Economics
- Review of external investment raised, grants secured, and research participation in publicly funded projects by registered cyber security businesses in the region
- Review of labour market supply and demand factors, including graduate and apprenticeship supply, and demand through advertised job vacancies
- Review of the baseline projection scenarios to 2035 set out within the North West Cyber Corridor (2023) research

Collectively, this provides a basis to consider how the cyber security ecosystem has developed in the last two years in the region, with benchmarking to other regions and the wider UK as appropriate.

Overall, we find positive evidence of growth within the North West cyber ecosystem across the majority of metrics baselined within the 2023 analysis. In the last two years, we find that the number of cyber security businesses in the region has grown by 27% to 378 unique firms. This has been particularly driven by new regional startups, supported by initiatives such as DiSH. Further, we estimate the region's cyber security related workforce has also grown by 19% to over 14,300 individuals in the last two years. The North West was also cited in the most recent UK Cyber Security Sectoral Analysis as the leading region for external investment in 2024, as launched at the CYBERUK 2025 in Manchester.

In turn, this is creating economic growth in the North West, with the ecosystem now generating in excess of £1bn per annum in direct Gross Value Added (up 33% from the 2023 baseline estimate of £760m).

The region is well positioned to continue to grow, with its growing skills base and investment in new infrastructure to support the cyber security ecosystem. However, some reduction in headcount and new job vacancies among providers may place some downward pressures upon growth, and we explore and revise growth scenarios accordingly, in addition to exploring where growth is most evident within the ecosystem at present and in future.

We set out some of the key figures in the following table, and how these have been compiled subsequently.

TABLE 4.1: SUMMARY TABLE

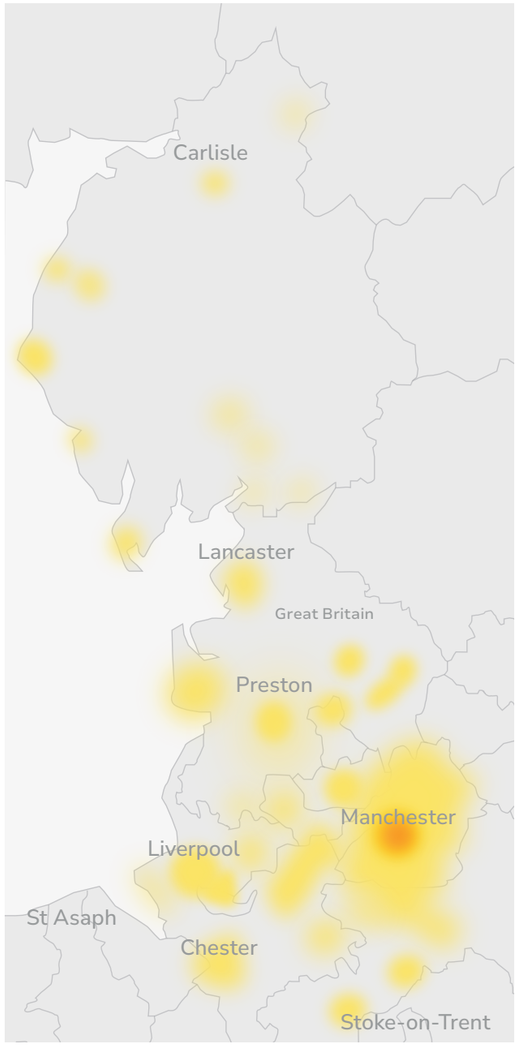
Key Stats	2023	2025 Estimate	Change
Number of Cyber Security Businesses Active in the North West **(Registered and Trading)**	298	378	+ 81 (+27%)
Number of Registered Cyber Security Businesses in the North West **(Registered only)**	144	226	+ 82 (+58%)
Number Employed in the Cyber Security Sector **(Estimated, FTEs)**	5,000	6,700	+ 1,700 (+34%)
Estimated Cyber Security Workforce **(across all sectors)**	12,000	14,000	+ 2,300 (+19%)
Estimated Cyber Security Workforce **(across all sectors)**	£760m	£1,010m (£1bn)	+ £250m (+33%)
External Investment (VC) raised by registered pure-play cyber security firms in the North West	£38.1m (6 deals) (13% of UK value) (2022 full year) 3rd Highest in UK	£102m (6 deals) (49% of UK value) (2024 full year) 1st in UK	+£64.1m (+168%)
Number of unique Cyber Security Job Postings in the North West **(Lightcast)**	4,563 (2022)	2,620 (2024)	-1,943 (-43%)
Mean Advertised Salary for Cyber Security Professionals **(North West)**	Mean: £56,800	Mean: £56,800	Nominal: No Change
Number of Graduates in Cyber Security and Computer Science **(North West)**	3,680	4,560	+ 882 (+24%)
Number of Cyber Security Graduates **(North West)**	350	640	+ 290 (+80%)

4.3 CYBER SECURITY BUSINESSES IN THE NORTH WEST

The DSIT UK Cyber Security Sectoral Analysis (2025) identifies 2,165 businesses within the UK that offer cyber security products or services. These businesses have an estimated 3,132 offices across the UK. In 2025, the UK's cyber security sector employed an estimated c. 67,300 Full-Time Equivalents (FTEs) (an increase of 11% since the previous year), with cyber security related revenue and Gross Value Added reaching £13.2bn and £7.8bn respectively.

Review of the DSIT UK Cyber Security Sectoral Analysis (2025), in addition to further review by the research team, suggests that the North West is home to:

- 378 cyber security companies, with 442 cyber security offices. Of these 226 are registered in the region (i.e. headquartered), and a further 152 are registered in other regions but have a physical office presence in the North West.
- The region is home to approximately 10% of the UK's cyber security sector (in terms of registered office count), and that almost one in five (18%) of UK registered cyber security businesses have at least one office in the North West.
- This data continues to highlight that the North West is the UK's largest cyber security ecosystem outside of London and South East.
- The majority (61%) of cyber security offices are based in Greater Manchester, followed by Cheshire and Warrington (16%), Lancashire (10%) and Cumbria (4%). Manchester has the second highest number of cyber security offices in the UK (269).
- There remains 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, and advanced manufacturing – all of which have concentrated cyber security expertise.



4.3.1. SIZE AND STRENGTHS

- Of the cyber security businesses with an active office in the region, 26% (97) are large, 19% (70) are medium, 12% (45) are small, and 44% (166) are micro.
- Compared to the 2023 baseline, this is encouraging as it suggests a growing and maturing ecosystem in the North West, with:
  - An absolute increase in the number of large firms active in the region (from 68 to 97), and medium firms (from 37 to 70). This includes where larger firms have established a presence in the North West, as well as growth among SMEs to 'medium' size, driven by both organic growth and merger activity.
  - The number of 'small' firms has reduced from 71 to 45; however, this also reflects growth and acquisition activity.
  - Further, the number of micro firms active in the region has increased from 122 to 166, reflecting new registrations and start-ups.
- This also highlights that there is increased potential to engage with a growing start-up and scale-up base across the North West, not only within the cyber security ecosystem, but across wider technology rollout and adoption in the region. The data highlights over 40 newly registered cyber security firms in the region since 2022, supported by initiatives such as DiSH.
- 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 52% of firms are 'dedicated' and 48% of firms are 'diversified' in the North West.

As highlighted in the baseline report, review of the company level data highlights regional excellence in:

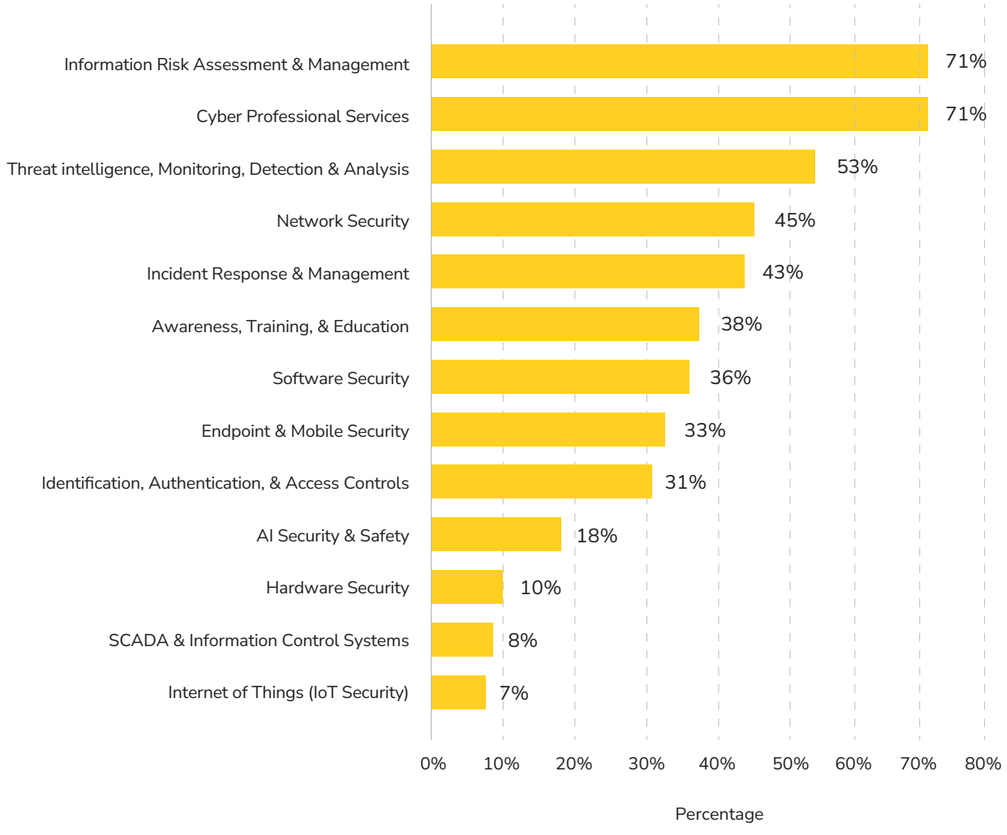
- Attracting large multinational businesses to the region with active presence in cyber security (e.g. Cisco, BT, BAE Systems, IBM, Darktrace, Deloitte, PwC, KPMG, EY, Capgemini, Microsoft, Ericsson, QinetiQ, and Thales all have an active presence). However, review of FDI Markets data suggests that the number and value of cyber security FDI projects in the UK (i.e. where international firms establish a UK presence) may be diminishing in 2024/25 compared to 2021/22 levels (e.g. 74 cyber security FDI projects in the UK in 2021 and 2022 combined compared to 40 in 2023 and 2024 combined). As such, working to grow established firms in the region, attract FDI amidst a more challenging landscape, and scale local firms will all be required for growth.
- 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). The DSIT AI and Software Market Analysis highlights the North West as a burgeoning area for AI security in particular.

4.3.2. PRODUCTS AND SERVICES

The DSIT Cyber Sectoral Analysis (2025) provides a market taxonomy covering key areas of product and service provision by the cyber security sector. Within this study, we have matched company descriptions (in their own words through website analysis) with the key terms within each taxonomy category, followed by use of additional natural language processing to assign companies to one (or more) taxonomy categories with respect to their product and service provision.

Within the North West, we find the following percentage of companies appear to offer products or services aligned to the following areas.

FIGURE 4.1: SERVICE OFFERING OF NW CYBER SECURITY COMPANIES



Source: Perspective Economics analysis of company data (n = 378)

When compared to the UK data, this suggests the North West has relative strengths in the following domains:

- **Threat Intelligence, Monitoring, Detection and Analysis:** The North West outperforms the UK average (53% vs 44%[7]), suggesting regional specialism in proactive threat hunting, SOC, and intelligence capabilities.
- **Endpoint and Mobile Security:** 33% of firms in the North West offer endpoint and mobile security compared to 22% nationally, indicating the region has applied expertise in securing devices and mobile infrastructure, with overlap into areas such as managed security services and securing telecommunications infrastructure.
- **Incident Response and Management:** The North West shows stronger representation (43% vs 36%), demonstrating regional capability in incident and breach response.
- **SCADA and Information Control Systems:** Whilst small in absolute terms, the North West has a slightly higher proportion than the national average (8% vs 6%), possibly reflecting industrial and manufacturing presence requiring operational technology (OT) security support.
- **AI Security and Safety:** The North West also appears to have emerging strengths in AI security and wider AI safety, assurance and governance capabilities, driven by firms such as Mindgard, Fuzzy Labs, and Zally.

Fuzzy Labs: Open-Source Machine Learning Operations with a Security Mindset

Manchester-based Fuzzy Labs (founded by engineers with DevOps backgrounds) has carved a niche in open-source Machine Learning Operations (MLOps), helping organisations take AI models from concept to production in a secure and scalable way. Fuzzy Labs has been operating since 2019, building AI solutions with security that is incorporated through the entirety of the ML.

"Security is fundamental to everything Fuzzy Labs delivers – not an afterthought"

Co-Founder Matt Squire

By using open-source tools and collaborating closely with clients, the Fuzzy Labs team ensures transparency and upskills organisations in MLOps best practices[8].

In **early 2025, Fuzzy Labs was selected for LASR Validate, the UK's first accelerator programme for AI security innovation** (a public-private initiative to boost national AI resilience). During this programme, Fuzzy Labs and other startups tackled real-world challenges in sectors like finance, defence, and telecoms, and integrating cyber security into AI solutions. The company's focus was advancing open-source MLOps to streamline AI deployment while addressing emerging threats. The team has explored tools for "purple teaming" large language models, combining offensive and defensive techniques to evaluate LLMs' code-generation security.

[7] https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2025/cyber-security-sectoral-analysis-2025#profile-of-the-uk-cyber-security-sector

[8] Fuzzy Labs: Engineering AI for the real world with strong principles (2025), Plexal, https://www.plexal.com/news/fuzzy-labs-engineering-ai-real-world/

4.3.3. ESTIMATED REVENUE AND EMPLOYMENT

The DSIT Cyber Security Sectoral Analysis (2025) also tracks core metrics for the cyber security sector including estimated cyber related revenue, Gross Value Added, and employment.

These figures are identified at a national level (i.e. estimated for UK related activity). They can be segmented at a regional level based upon registered location; however, this is likely to underestimate the actual activity at a regional level. For example, a firm may be registered in London but employ a security team in Manchester. As such, these figures should be treated with caution, and indicative only. Further, we estimate the 'regional' ecosystem, using these figures in addition to wider use of workforce, web, and demand data to estimate the economic contribution of the cyber security ecosystem in the North West more overall in Section 7.

The UK Cyber Security Sectoral Analysis estimated that the sector generated £13.2bn in the most recent year (2024). Of this, the 175 firms identified as registered in the North West generated an estimated £732m in cyber security related revenue, £542m in cyber security related GVA, and employed an estimated 4,633 cyber security FTEs.

However, the study also estimates that the North West is home to approximately 10% of the UK's cyber security sectoral workforce (i.e. up to 6,700 people) – highlighting the need to capture regional employment within registered and trading offices. Compared to the 2023 North West Cyber Corridor baseline, the regional data for the North West is encouraging, as it highlights how firms registered in the region have increased their combined cyber related revenues from £493m to £732m (+48% in two years) and employment from 3,700 cyber security FTEs to 4,633 (+25% in two years).

This compares favourably to the national growth of the UK cyber security sector, where revenue has grown by 26% in the last two years (from £10.5bn to £13.2bn) and employment has grown by 16% (from 58,000 to 67,300 FTEs).

4.3.4. UPDATED ESTIMATES FOR THE NORTH WEST CYBER CORRIDOR ECOSYSTEM

Estimating the size and scale of the North West Cyber Corridor ecosystem requires the use of national datapoints, such as the DSIT Cyber Sectoral and Skills research, in addition to further use of web and company data to explore the extent of the offering within the North West.

As such, this section sets out revised estimates for the North West Cyber Corridor ecosystem (compiled in July 2025) and compares these to the baseline estimates included within the 2023 baseline.

Firstly, we explore cyber security related employment within the North West. This provides the basis for estimating wider values such as regional revenue and Gross Value Added, in line with wider data available, and helps to capture activity within the region.

There are multiple data points available to help inform this estimation:

- DSIT Cyber Security Sectoral Analysis (2025, Registered only): 4,633 FTEs across 175 registered firms in the North West. This is considered a conservative estimate as it only captures registered firms.
- DSIT Cyber Skills in the UK Labour Market Estimate: 10% of the UK sector, based on review of workforce profiles, sectoral data, and vacancies = 6,700 FTEs in the North West. This is a regional estimate as set out within a national study.
- Automated Review of Workforce Data, Accounts, and Web Review: c. 6,100 FTEs and profiles identified in the North West (against the 378 active businesses identified in the region) as part of this research review. All 378 firms have been reviewed to identify relevant profiles within the North West. This is likely to be accurate on a firm-by-firm basis but may underestimate where there is insufficient web coverage.

This data suggests that the estimate of 6,700 FTEs in the North West cyber security sector (as of 2025) is appropriate for current regional employment. This represents an increase of up to 1,700 FTEs since the 2023 baseline report (+34%).

Further, as noted within the baseline, the cyber security sector is only one component of cyber security employment in the region. It does not include public sector, research and education, or cyber security roles within other private sector employers. As such, the DSIT Cyber Skills in the UK Labour Market (2025) research estimates that there are 143,000 individuals employed in the overall cyber security workforce across the UK.

Review of this workforce data and applying the proportional estimate of 10% for the North West, suggests that the region's cyber security workforce could be in the region of **14,300 individuals** (an increase of 2,300 FTEs, or 19% from the 2023 baseline estimate of 12,000 FTEs). This is also in line with the projected forecast for 2024 (14,100 FTEs) set out in the baseline report.

4.3.5. ESTIMATING CYBER SECURITY RELATED GROSS VALUE ADDED (GVA)

Gross Value Added (GVA) is a metric that can help to capture the economic contribution and productivity of a sectoral ecosystem. It combines firm-level profitability and workforce remuneration, in addition to wider amortisation and depreciation. Within the baseline report, the estimated GVA (2022) for the North West was £760m. This estimated GVA on a per employee basis, for those employed in the cyber security sector (based on the DSIT Sectoral Analysis), and using average estimated remuneration for those within the wider ecosystem.

- Within this update, we estimate GVA within the most recent year at £1,010m (£1bn). We have reviewed the most recent available data for GVA and remuneration, and use the following assumptions to estimate the regional ecosystem GVA:
- The DSIT Cyber Security Sectoral Analysis (2025) estimates that GVA per employee within the UK sector is approximately £116,200. This typically consists of salary / remuneration and firm level profitability. This is 8% higher than the figure used in the 2023 baseline report.
- As with the baseline, within the North West, we estimate that GVA per cyber security role is approximately 90% of UK levels[9](c. £104,600 per cyber sector employee).
- Further, we also estimate that average North West cyber security related salaries (outside of the cyber security sector) are approximately £40,700[10].
- **As a conservative estimate, we calculate updated (2024) direct GVA for the NW cyber security ecosystem at £1,010m[11].**

We explore future ecosystem growth and review and revise baseline scenarios until 2035 in Section 7.

[9] This uses the broader cyber security vacancy average remuneration within the Cyber Skills in the UK Labour Market research (2022-25) and applies a 90% weighting

[10] Lightcast estimate for cyber security roles outside of the core sector

[11]Calculated using the (c. 6,700 FTEs in cyber security sector * £104,600) + (7,600 wider roles x salary only, £40,700) = £1,010m.

4.3.6. EXTERNAL INVESTMENT RAISED

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).

The most recent report (2025) estimates that the UK cyber security sector raised approximately £206 million raised across 59 deals within dedicated cyber security firms in 2024. However, this is considerably lower than levels seen in 2019 – 2021, where external investment in dedicated cyber security companies reached record figures, particularly in 2020 and 2021, with £814m raised and £1,013m raised respectively. However, these high levels were arguably due to wider macroeconomic conditions such as low interest rates, and high demand for investment into technology sectors such as cyber security and AI.

The 2024 data highlights that, for the first time, the highest proportion of external investment was in the North West (49%) with six deals to the value of £102m. This is largely due to the c. £88m raised by Cheshire-based web application security firm PortSwigger, as well as firms such as CultureAI, Cytix, CloudGuard, and Zally. This is followed by the South East (21%), and London (14%).

As of August 2025, we have revisited these estimates (which can be revised as firms announce retrospective investments). This is based upon updated regional data and retains firms active in the North West that have had a registered address in the North West at any time since 2020. This increases the estimated investment raised by firms in the North West to £114m across eleven deals in 2024.

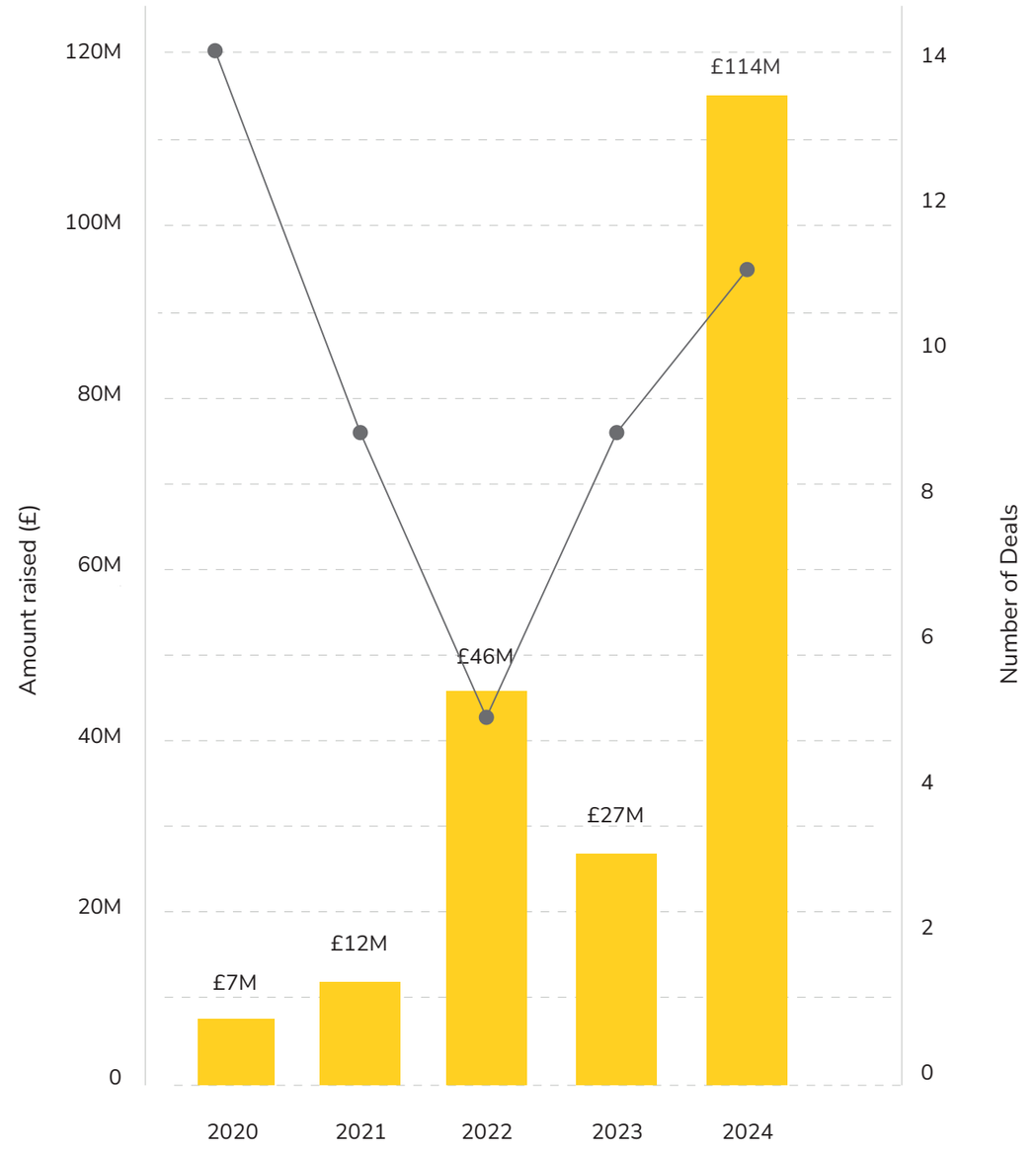
This is a substantial increase since the baseline report (then estimated at £38m in 2022, revised to £46m), more than doubling within the two-year period.

However, investment data can be subject to significant annual variation, particularly when a small number of high-growth companies raise significant investment rounds. We also note that the strong PortSwigger raise of £88m in 2024 is a statistical outlier. If we remove this deal from the set, investment in the North West would be broadly comparable in 2024 (£26m) as with 2023 levels (£27m).

Whilst reflective of a relatively small number of deals, the previous five years of investment data within the North West provides some interesting insight into investor activity. The region saw a sharp decline in deal activity from 14 deals in 2020 to just 5 in 2022 (- 64%), mirroring the broader tech and cyber security landscape. However, the number of deals has broadly rebound in the last two years.

Further, there is evidence of significant maturity within the North West's cyber ecosystem from a few years prior. For example, in 2020, the North West raised £7m across 14 deals (average deal size of £500k), representing less than 1% of all UK cyber investment (£814m) that year. In 2024, even excluding PortSwigger, the average deal size has increased fivefold to over £2.6m suggesting that the North West is increasingly becoming an early-stage to Series A level area of interest to investors, and a maturing ecosystem with increasing 'deal flow'. Total cyber security investment in the UK cyber security sector has fallen consecutively year on year since 2021; however, the North West has countered this trend twice in 2022 and 2024.

FIGURE 4.2: CYBER SECURITY VC INVESTMENT IN THE NORTH WEST (2020-2024)



Source: Regional analysis of UK Cyber Security Sectoral Analysis (Perspective Economics), Beauhurst

PortSwigger: Global Application Security Leader

PortSwigger, headquartered in Cheshire, is a North West–grown cyber security leader with global reach. Founded in 2008 by ethical hacker Dafydd Stuttard, the company was established in 2003 when Stuttard created the first version of Burp. Over the following years, Burp Suite evolved from a niche proxy tool into the industry-standard platform for web application security testing, now used by over 16,000 organisations in 160 countries, including Microsoft, Amazon, and NASA, and supported by over one million learners on its free Web Security Academy[12]. Key milestones for the company include:

- the launch of the Burp Scanner in 2007;
- entry into the Gartner Magic Quadrant for Application Security Testing in 2014;
- the creation of the BApp Store for community extensions in 2015;
- the 2019 release of Burp Suite Enterprise Edition enabling large-scale DevSecOps adoption;
- the Web Security Academy hit its million-user milestone within a year of launch, underscoring the company's role in global security education.

In 2024, **PortSwigger secured its first external investment of £88m** from U.S. based growth fund Brighton Park Capital, to accelerate product development, enhance Burp Suite for enterprise needs, and expand its research and community initiatives. A new U.S. office in Atlanta now supports a North American customer base that makes up over half of its users.[13]

CultureAI: Managing the Human Factor in Cyber Risk

Manchester's CultureAI is using AI to deeply understand human behaviour to detect risks and threats affecting employees across the human perimeter in real-time, and intervene to mitigate them as they arise. Founded by James Moore, CultureAI has developed a "Human Risk Management" platform that helps companies detect risky employee actions (such as falling for phishing, using weak passwords, or mishandling data) and coach staff in real time to prevent breaches.

CultureAI's innovative vision has attracted notable customers and investors. After raising £4 million in 2021 and £5 million in 2023 (seed rounds), the company saw rapid adoption of its platform by clients like Revolut, Marie Curie, RAC, Wickes, Delivery Hero and others.[14] In July 2024, CultureAI closed a $10 million Series A funding round co-led by Mercia Ventures and Smedvig, **bringing its total funding to over $19 million.** This inflow of capital is fuelling a scale-up, with the company planning to double its headcount in 12 months and expand its presence in the U.S. market. The company is positioning itself as a leader in emerging human risk security management platforms.

[12] PortSwigger — a web security company on a mission to enable the world to secure the web (2025), PortSwigger, https://portswigger.net/about

[13] Bootstrapped PortSwigger secures £88 M in first external investment (2024), UK Tech News, https://www.uktech.news/cybersecurity/portswigger-brighton-park-capital-funding-20240701

[14] Culture AI raises $10 million in Series A funding to evolve how organisations manage human risk (2024), CultureAI, https://www.culture.ai/resources/blog/cultureai-raises-10-million-in-series-a-funding

4.3.7. RESEARCH AND INNOVATION:

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

- The University of Lancashire
- The University of Lancaster
- Liverpool Hope University
- Liverpool John Moores University
- The Manchester Metropolitan University
- The University of Greater Manchester
- The University of Liverpool
- The University of Manchester
- The University of Salford
- University of Chester
- University of Cumbria
- Edge Hill University

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 revisits 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 to identify cyber security related projects. The research team has utilised over two hundred relevant keywords matched against over 160,000 research projects (since 2006), followed by LLM review to identify 'cyber security' related research projects.

In total, we find over 1,300 publicly funded cyber security research projects across the UK between 2020 and 2025 (to date).

TABLE 4.2: PUBLICLY FUNDED CYBER SECURITY RESEARCH PROJECTS (2020-2025)

	Projects led by organisations	Percentage	Value	Percentage
North West	80	7%[15]	£52,808,524	8%[16]
UK	1,346		£717,134,595	

Source: Perspective Economics analysis of UKRI Gateway to Research (2020 to 2025)

[15] We have identified 80 cyber security projects led by organisations from the North West. There are 1,103 projects across the UK with a known region.

[16] NW = £52.8m divided by £661.3m across known regions

Over the past three years, the North West has seen numerous **cyber security** and **digital trust** research projects and innovation initiatives. These range from large multi-institution programmes to targeted translational projects, funded by UK Research and Innovation (UKRI) councils (EPSRC, Innovate UK, Research England), government agencies and industry partnerships. They involve universities partnering across the region – including Lancaster, Manchester, Liverpool, Salford, Manchester Metropolitan (MMU), Central Lancashire (UCLan) – in collaboration with industry, government, and startups.

We summarise some of the key initiatives (2022–2025) below.

- **North West Cyber Security Connect for Commercialisation (NW CyberCom)** (£1.2m, announced October 2023), is led by Lancaster University with support from Universities of Liverpool, Salford, Manchester Metropolitan, Manchester, UCLan, alongside Plexal, MIT REAP and CRSI. This initiative focuses on commercialising cyber security research from universities, providing training for researchers on commercialisation opportunities, and creating an innovation ecosystem. The programme aims to create new products, services and policy to better protect consumers, businesses and UK infrastructure.

- **CyberFocus** (£4.9m, announced November 2024), is a consortium of seven North West universities led by Lancaster, Liverpool, Salford, Manchester Metropolitan, Manchester, UCLan and Cumbria. This programme acts as a catalyst for cyber knowledge exchange to transform research ideas and innovations into solutions, products and services. The initiative aims to create 85 collaborative partnerships, develop 400 new products and services, secure £40 million in additional funding, and train 300 individuals in cyber innovation skills.
- **North West Partnership for Security and Trust** (NWPST) (launched October 2021), is a partnership between GCHQ and four universities: Lancaster, Salford, Manchester Metropolitan and Manchester. This partnership fosters collaboration across research, innovation, skills development, and public engagement to produce new knowledge to benefit national prosperity and societal understanding of issues relevant to national security. This represents the first time the intelligence services will publish research jointly with universities.

- **Greater Manchester Digital Security Hub (DiSH)** (£10m, launched June 2022), is led by Barclays Eagle Labs Plexal with Lancaster and Manchester universities. The hub comprises an 11,000 square foot state-of-the-art space in Heron House, aiming to support 500 start-ups and create over 1000 jobs in Greater Manchester. The facility offers access to mentors and coaching, dedicated growth programmes through Barclays Eagle Labs and a new industry accelerator created by Plexal.

- **Greater Manchester Cyber Foundry (GMCF)** (£6m, 2018-2022), was a collaboration between Lancaster, Salford, Manchester Metropolitan and Manchester, funded by ERDF. The programme engaged with 55 SMEs in Greater Manchester through business strategy workshops and knowledge sessions, with 14 receiving further technical support. This initiative aimed to combat £860m annual cyber attack risk to region's businesses by combining expertise and research in cyber security to create new products and services for SMEs.

- **Lancashire Cyber Foundry (LCF)** (£2.1m, 2019-2022), was led by Lancaster University with ERDF funding. The programme aimed to engage with 320 SMEs through a blend of face-to-face workshops, online modules, and software development. This three-part programme supported SMEs in Lancashire to defend, innovate and grow, including business strategy programmes and fully funded R&D services.

- **SPRITE+ NetworkPlus** (£4m total: £1.4m initial + £2.6m follow-on, launched September 2019, extended 2023-2027), is led by The University of Manchester under EPSRC Digital Economy theme. This is the UK's national NetworkPlus for Trust, Identity, Privacy and Security (TIPS), fostering engagement between academic and non-academic communities and providing a platform for building interdisciplinary collaborations. The network funds studies and pilot projects, holds workshops and facilitates internships and staff exchanges.

- **TAS Node in Security** (£3m, launched November 2020-2025), is led by Lancaster University under EPSRC Strategic Priorities Fund. This forms part of the £33m UKRI Trustworthy Autonomous Systems programme, developing fundamental security techniques to provide practical and scientifically rigorous principles for secure Autonomous Systems. The initiative brings together a cross-disciplinary team of security experts from Distributed Systems, Communications, Controls, AI, Sociology and Law, working with Cranfield University.

- **Centre for Digital Innovation** (£4.1m, launched 2023), is a partnership between Manchester Metropolitan, Manchester, Lancaster, Salford and Greater Manchester Colleges under UK Innovation Accelerator pilot. This centre focuses on four technology strands – artificial intelligence (AI), cyber, industrial digitalisation (ID) and immersive technology (IT). The programme works on R&D, skills development, business models for SMEs, and community outreach to create a supercluster for digital innovation, expertise and skills development.

Case Study: CyberFocus: Research-Led Impact Partnerships

CyberFocus brings together a consortium of universities and industry partners with £4.9 million UK Research and Innovation (UKRI) fund for place-based impact funding to turbocharge the North West's cyber sector.

This includes:

- Lancaster University
- University of Lancashire
- University of Cumbria
- University of Liverpool
- University of Salford
- Manchester Metropolitan University
- The University of Manchester
- 18 civic, government and industrial partners.

CyberFocus invests in trusted academia-industry partnerships and innovation support to translate research into cutting-edge cyber solutions. It explicitly targets growth outcomes for the regional cyber ecosystem. CyberFocus sets out to:

- Build 85 new collaborative R&D partnerships between universities and businesses
- Develop 400 new cyber products or services via innovation support
- Attract £40 million of additional funding into the North West cyber sector
- Train 300 people in cyber innovation skills to expand the talent pipeline

Early project activity involves "Team Barrow" (Westmorland and Furness Council with BAE Systems in Barrow) and other civic partners aligning cyber innovation with local strengths such as maritime and defence engineering. By integrating expertise from different sectors, CyberFocus is expected to **create new high-skilled jobs, stimulate inward investment, and boost the region's overall cyber resilience.**

4.4. WIDER CYBER SECURITY ASSETS IN THE NORTH WEST

This research highlights how the North West's cyber ecosystem has developed since the baseline study. In addition to a larger core of specialist cyber firms, there is also a broader system of assets such as public bodies, primes, R&D infrastructure, universities, co-working / innovation hubs and adjacent-sector anchors that collectively strengthen the region's cyber ecosystem. This section explores:

- The role of over 170 unique **wider public, private and research assets** relevant to cyber across the Corridor (see Appendix for full list provided for this update).
- The role of adjacent sectors where the region has distinctive strengths, aerospace & defence, advanced manufacturing, professional services, creative / digital and telecoms, and which are increasingly cyber-intensive.

The region has seen an increase in activity from defence and public sector bodies since the baseline study.

- **The National Cyber Force (NCF):** With NCF's permanent base at Samlesbury set to open later in 2025, this will employ several hundreds of personnel in year one and grow thereafter. The NCF is designed to catalyse partnerships with local industry and universities and is already prompting further investment activity (e.g., a proposed £13.2m Innovation Hub at Samlesbury Enterprise Zone).
- **GCHQ presence:** GCHQ's Manchester office continues to anchor skills and innovation activity in the city region.

The region continues to boost a unique range of research and development assets, including:

- **STFC Hartree Centre:** The STFC Hartree Centre at Daresbury puts national capability in AI and high-performance computing at the heart of the region. For example, its Industrial Digitalisation Accelerator with Siemens and Atos helped manufacturers adopt Industry 4.0 and secure OT/IT systems, an important enabler for cyber across supply chains.
- **AMRC North West:** Supports digital manufacturing adoption and productivity growth among Lancashire firms, complementing emerging NCF activity.
- **Oxford Road Corridor:** One of Europe's largest clinical-academic campuses anchored by MFT and The University of Manchester, with Manchester Science Park hosting over 150 businesses. The Citylabs cluster now includes Citylabs 4.0[17], officially opened in March 2025 strengthening the health innovation footprint on the Corridor.
- **Sister (formerly ID Manchester):** A £1.7bn science and technology district on the former 'North Campus' site. Sister is a joint venture between The University of Manchester and Bruntwood SciTech, and will be delivered over the next 15 years. Sister is predicted to generate over 10,000 on-site full-time jobs and contribute around £1.5 billion to the economy every year in Manchester.

The following section explores the role of adjacent industries and sectors, such as AI, defence and national security, and semiconductors. The region also has a strong presence of primes and professional services, such as:

- **Defence and national security:** The North West is a significant asset for wider defence and national security, with activity spanning primes, test and evaluation, and public bodies generates

[17] Citylabs 4.0 officially opens, further strengthening Manchester's life sciences ecosystem (2025), Manchester University NHS Foundation Trust, https://www.mft.nhs.uk/2025/03/27/citylabs-4-0-officially-opens-further-strengthening-manchesters-life-sciences-ecosystem/

[18] House of Commons Library, 'The contribution of the defence industry to UK regions,' Research Briefing CBP-

sustained demand for high-assurance systems, OT/ICS security and cleared personnel, providing an anchor market for regional suppliers.

In 2023/24, the Ministry of Defence spent c. £3.8 billion with industry in the North West, making it the third-highest recipient of MOD expenditure nationally, behind only the South East (£7.1bn) and South West (£6.9bn). This substantial investment translates into approximately 23,200 MOD-related jobs across industry, civilian, and military roles.[18] It is estimated that when the broader defence ecosystem is considered, employment increases to c. 45,000 roles, with almost half (20,000) based in Lancashire, according to Innovate Lancashire research (2025).

The Joint Economic Data Hub (JEDHub) 2024 report on the UK's defence sector also highlighted the North West as an 'epicentre for defence employment,' with '31.5% of the surveyed UK defence workforce located within the region'.[19]

- **Aerospace & manufacturing:** The manufacturing, defence and aerospace footprint in the region creates a constant requirement for secure-by-design engineering and OT/ICS security. In May 2025, MBDA confirmed a £200 million expansion in Bolton, with 700 additional roles and expanding the regional supply chain.[20] QinetiQ's MOD Eskmeals range specialises in testing systems in Cumbria, while Thales' Cheadle Heath team in Stockport contributes sonar systems to the Royal Navy's Dreadnought programme.

BAE Systems' Barrow-in-Furness shipyard represents the UK's sole nuclear submarine construction facility and one of only a small number globally. The site employs approximately 14,500 people—nearly one-third of the town's working-age population—with plans to grow to around 17,000[21] at peak to support the Astute, Dreadnought, and SSN-AUKUS programmes, underpinned by £4bn of defence contracts.

It is estimated that each submarine built at Barrow represents a national industrial endeavour. On average, over 11,600 UK suppliers contribute components and services to every vessel, expected to generate total supply-chain expenditure of approximately £7.5 billion across 1,500 companies over the life of the Dreadnought programme.[23]

The North West Aerospace Alliance represents ~25% of UK aerospace with over 240 members and supports common standards and supplier development.[24] These assets translate directly into cyber needs around classified networks, secure data handling and industrial resilience.

- **Professional services & telecoms:** The North West has a strong concentration of professional services and network engineering with links to the cyber ecosystem. The region is home to the Big-four (PwC, KPMG, Deloitte, EY), and other major consultancies, which rely on strong cyber security, and have cyber and advanced tech focuses internally. BT in Manchester and TalkTalk's headquarters in Salford embed key network and security operations within the region.

[19] HM Government (2024) Defence sector continues contributing significantly to UK economy https://www.gov.uk/government/news/defence-sector-continues-contributing-significantly-to-uk-economy.

[20] UK Business Secretary visits MBDA site as planned investment and recruitment announced (2025), MBDA UK, https://www.mbda-systems.com/uk-business-secretary-visits-mbda-site-planned-investment-and-recruitment-announced.

[21] https://www.pesmedia.com/bae-systems-selected-to-build-aukus-nuclear-submarines

[22] https://www.gov.uk/government/news/4-billion-uk-contracts-progresses-aukus-submarine-design

[23] https://www.asd-europe.org/news-media/news-events/get-inspired/how-submarine-building-is-powering-jobs-and-skills-in-barrow/

- **AI and automation:** We estimate, based on the DSIT AI Sectoral Analysis, that the region is home to more than 400 of the UK's registered AI firms. This substantial base across applied AI, machine learning and automation is driving requirements for secure data engineering, AI assurance and privacy-preserving analytics, while broadening the pool of data and software talent relevant to cyber within the region.

- **Semiconductors and ElecTech:** The region also has emergent strengths in design, materials and embedded systems support hardware security and supply-chain assurance, complementing the wider software-led cyber capabilities.

Case Study: CyberFocus: Research-Led Impact Partnerships

Mindgard is an AI cyber security startup founded in 2022 at Lancaster University that specialises in securing Artificial Intelligence systems. The company has rapidly gained national recognition for its cutting-edge AI Red Teaming platform.

In June 2024, Mindgard was crowned the "UK's Most Innovative Cyber SME 2024" at the Infosecurity Europe conference, emerging the winner among 14 finalists[25]. This award highlighted Mindgard's contributions to identifying and mitigating vulnerabilities in AI, GenAI, and LLMs. Mindgard recently launched their flagship AI Security Labs, a platform (free to use) enabling enterprises to continuously pen-test their AI, GenAI, and LLM models for vulnerabilities. As businesses increase their use of AI, Mindgard's tools help uncover threats like prompt injections, data leakage, and model evasion attacks that traditional security tools often miss.

Mindgard's growth has been supported by significant investment. After an initial $4 million seed raise in 2023, the startup secured an $8 million funding round in late 2024 to accelerate the business' goals[26]. This round of funding, led by U.S. and European venture firms, is helping Mindgard to scale up, including appointing new senior executives, and expand into North America.

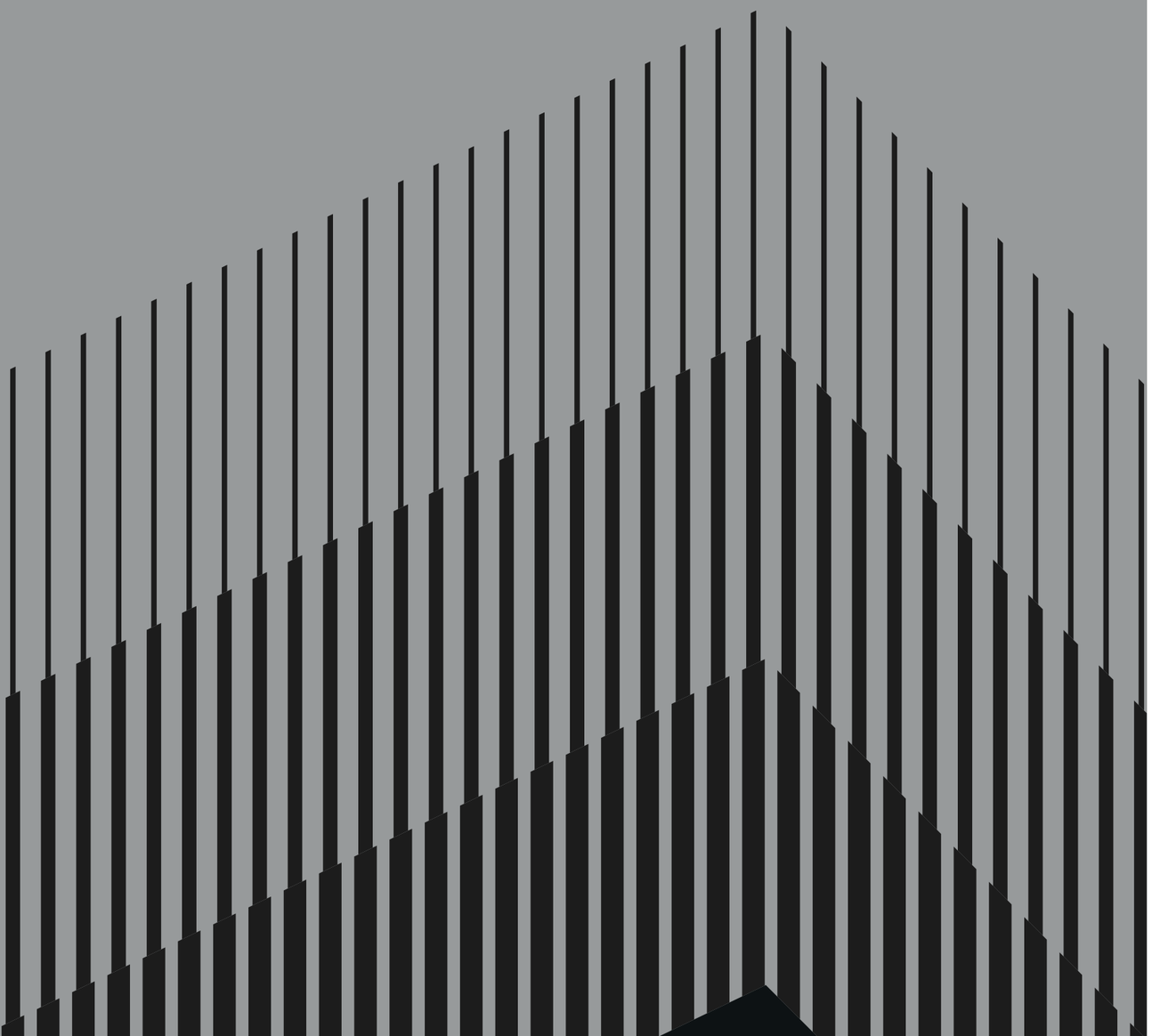
The progression of Mindgard as a Lancaster University research project to an award-winning AI security venture exemplifies the North West's ability to build and support nationally important cyber innovations. Its success underscores the UK's growing focus on AI security, with Mindgard now "leading the charge toward creating a safer, more secure future for AI" in enterprise.

[24] North West Aerospace Alliance (2025), North West Aerospace Alliance, https://www.aerospace.co.uk/

[25] Mindgard Recognized as UK's Most Innovative Cyber SME 2024 at Infosecurity Europe (2025), Mindgard, https://mindgard.ai/resources/mindgard-recognized-as-uks-most-innovative-cyber-sme-2024-at-infosecurity-europe

[26] Mindgard secures $8 M to tackle emerging AI security risks (2024), Tech.eu, https://tech.eu/2024/12/23/mindgard-secures-8m-to-tackle-emerging-ai-security-risks/

5. Demand & Supply of Cyber Security Skills



5.1. DEMAND

The DSIT Cyber Security Skills in the UK Labour Market (2025) research highlights that:

In 2024 across the UK, there were an average of 2,698 core cyber job postings every month, and a further 2,399 in cyber-enabled job roles.

Approximately 11% of these vacancies were posted in the North West region.

In line with the baseline research, the region has the third highest demand for cyber security professions behind London and the South East.

Building on the UK-wide research, this section explores demand for cyber security skills across the North West. Recent analysis using the Lightcast job postings database (covering between January 2024 to June 2025) reveals some shifts in employer demand for cyber-related roles.

This data explores trends in the volume of postings, the types of roles advertised, and the specific skills, qualifications, and levels of experience employers are seeking in cyber security.

It also explores demand for cyber security roles across sectors and geography, and remuneration in the North West compared with the rest of the UK.

This data focuses on demand for core cyber postings, which are roles formally labelled or commonly recognised as cyber security jobs (see UK report for full definition). These postings include roles with demand for skillsets directly related to cyber security, such as information systems, cryptography, information assurance, network scanners, and security operations. These are job roles where some aspect of cyber security is the main job function. This would typically include job titles such as Cyber Security Architect, Cyber Security Engineer, Cyber Security Consultant, Security Operations Centre (SOC) Analyst and Penetration Tester.

5.1.1. NUMBER OF JOB POSTINGS

Within the previous baseline report, we found there had been a sharp increase in demand for cyber security professionals between 2020 – 2022 in the North West (consistent with wider UK trends). Our analysis suggests there 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.

However, as shown in the recent national research, job postings in cyber security (and the wider tech ecosystem) have been reduced between 2023 and present (2025) driven by multiple technological and macroeconomic factors.

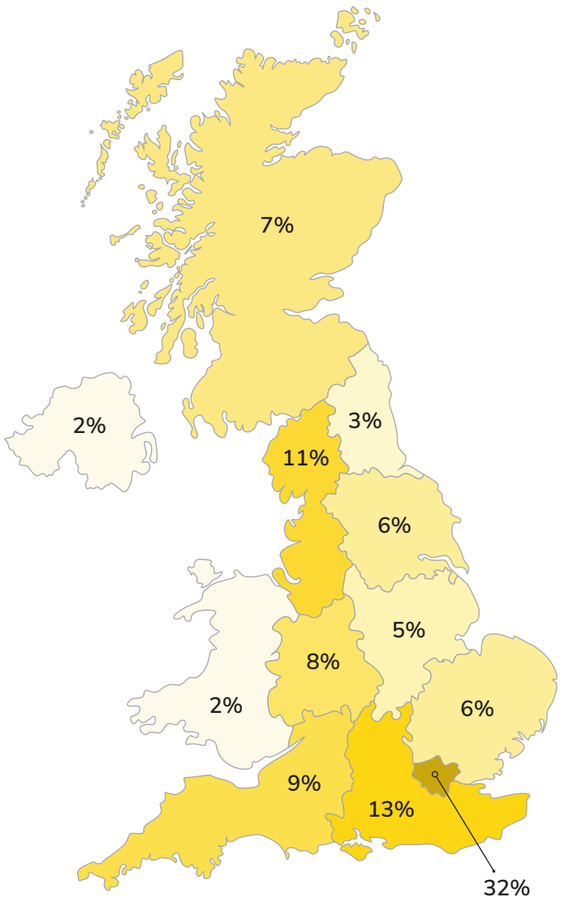
In 2024, there were approximately 32,400 unique job postings in UK cyber security, a 33% reduction from the previous year (c. 48,500 in 2023). Approximately 11% of these vacancies with a known location were in the North West.

5.1.2. UK-WIDE TRENDS

While overall demand decreased in 2024, the geographical distribution of cyber security roles has remained relatively stable. London continues to account for the largest share of core cyber job postings (32%), followed by the South East (13%) and the North West (11%).

FIGURE 5.1: PERCENTAGE OF CORE CYBER JOB POSTINGS FROM EACH UK REGION (WHERE LOCATION IS KNOWN) (2024)

1. London (32%)
2. South East (13%)
3. North West (11%)
4. South West (9%)
5. West Midlands (8%)
6. Yorkshire and The Humber (6%)
7. Scotland (7%)
8. East of England (5%)
9. East Midlands (3%)
10. North East (3%)
11. Wales (2%)
12. Northern Ireland (2%)

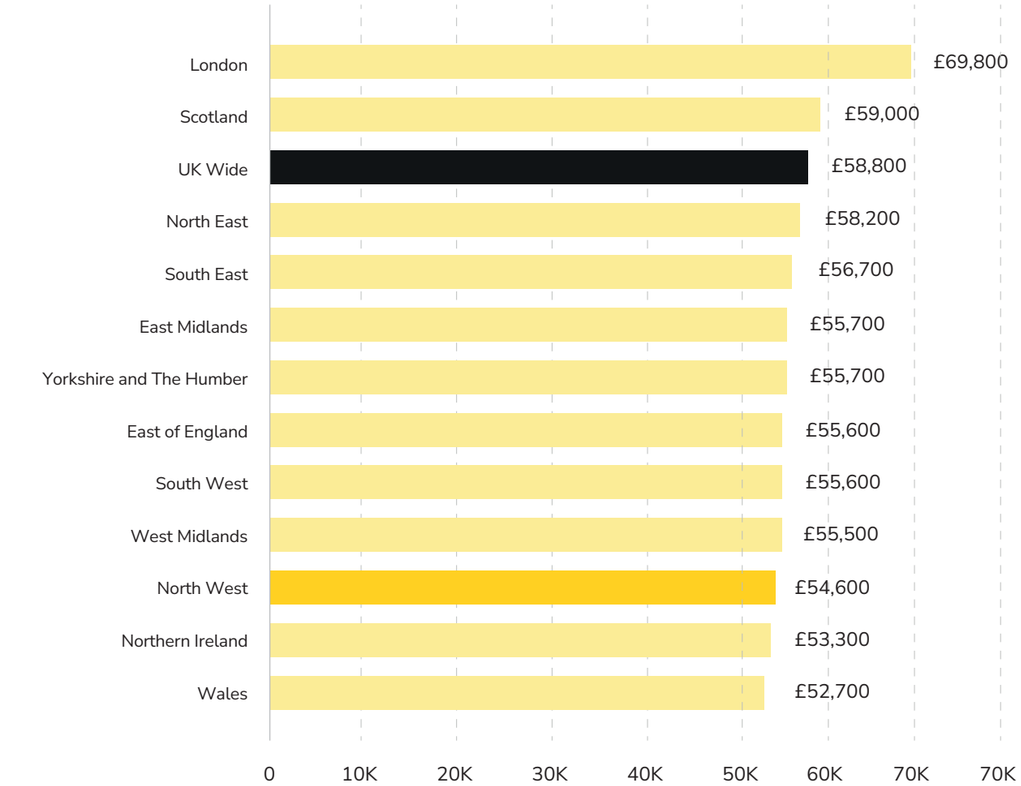


Source: Lightcast
Base: 24,085 online job postings with location data in 2024

Despite wider contraction, the North West has remained as one of the top three regions in terms of cyber job demand since 2020.

In 2024, the average UK advertised salary was £58,800 for core cyber job postings, with a median value of £55,000. In the North West, the average advertised salary was £54,600. This is the same in nominal terms as the salaries set out in the baseline report, which may suggest some real-term decline in advertised salary or may be where job postings are either tailored towards more junior and mid-level talent, or where individuals may be remuneration with basic salary plus wider benefits in areas such as the public sector.

FIGURE 5.2: MEAN SALARY OFFERS FOR CORE CYBER JOB POSTINGS, BY REGION (WHERE THE SALARY OR SALARY RANGE IS ADVERTISED) (2024)



Source: Lightcast

As explored in the following section, the proportion of roles available at entry level is higher in the North West than across the UK average (24% North West compared to 17% UK wide). This may signal an opportune market for recruitment; medium and large employers are well placed to develop sustained pipelines of cyber security professionals via entry-level hiring in the North West.

5.1.3. IN-DEMAND ROLES & QUALIFICATIONS

A review of the cyber security job postings in the region highlights that demand is highest for security analysts, security engineers, and security managers. This is in line with the baseline research. Analysis of job postings between January 2024 and June 2025 suggests that in the North West cyber sector (where stated):

- 24% of postings require <1 years' experience (compared to 17% at the UK level), suggesting an improved climate for graduate recruitment;
- 35% of postings require 1-3 years' experience, with the remaining 40% of postings looking for more than 4 years' experience from applicants.

5.1.4. REGIONAL BREAKDOWN

Between January 2024 and June 2025 there were 3,770 core cyber job postings across c. 1,070 different employers in the region. For roles with a known location, we find that just over half of advertised cyber roles are in Greater Manchester (55%), followed by Merseyside (Liverpool City Region) (16%), Cheshire (14%), Lancashire (10%) and Cumbria (3%). The top recruiters included a mix of large employers and specialists including BAE Systems, Unilever, Virgin Money, the NHS, Barclays, and NCC Group.

Previous research highlighted the North West's position as a crucial centre of demand for cyber security talent, driven by developments in government, industry, and academia. The establishment of the National Cyber Force (NCF) headquarters in Lancashire, alongside the growing presence of GCHQ in Manchester, has increased demand for skilled professionals across the region.

These strategic government investments have positioned the North West as a national hub for cyber operations, intelligence, and advanced technological expertise.

Reflecting this increase in demand, at the time of writing, recruitment data for early 2025 indicates that nearly half of all UK civil service cyber-related vacancies are now concentrated in the North West, with roles spanning key locations such as Manchester, Lancashire, Wilmslow, and Preston. Both GCHQ and the NCF have been actively recruiting in the region, signalling growth in cyber career opportunities and a commitment to building local talent pools. The expanding cyber ecosystem in the North West has created opportunities to sustain demand for cyber security talent.

5.2. SUPPLY

The DSIT Cyber Skills in the UK Labour Market Report (2025) suggests that the UK cyber security workforce has c.143,000 individuals. Of these, an estimated 10% (14,300 people) are based in the North West. Our analysis suggests that approximately 6,700 FTEs work in the region's cyber security sector and a further 7,600 FTEs work in wider cyber security related roles in other industries and the public sector.

The following sub-sections explore the provision of cyber security skills in the region, including university course provision and further education. This section draws on bespoke data from the Higher Education Statistics Authority (HESA) and Jisc. The data provides an insight to the considerable range of courses in cyber security and computer science at both undergraduate and postgraduate level in the UK.

We explore enrolments, graduate outcomes, and regional comparisons for cyber and computer science courses up to the academic year 2022/23. This explores talent coming through universities, where graduates go on to work, and how the North West compares to other parts of the UK.

5.2.1. UNDERSTANDING THE CURRENT HIGHER EDUCATION PROVISION LANDSCAPE

The North West is home to a significant share of the UK's university-level provision in cyber security and computer science education. In the 2022/23 academic year, 10% of the UK's Higher Education Institutions offering cyber security or computing-related courses were based in the region. This reflects the region's strengths in digital and technical education and reinforces the potential for the North West to serve as a key source of talent for the UK's cyber workforce, particularly considering the arrival of the National Cyber Force in Samlesbury and the wider ambitions around the North West Cyber Corridor.

TABLE 5.1: HIGHER EDUCATION PROVIDERS OF CYBER BY REGION

Region	Cyber Course Providers	Cyber Course Providers
London	16 (16%)	27 (19%)
South East	14 (14%)	19 (13%)
Scotland	13 (13%)	16 (11%)
North West	10 (10%)	13 (9%)
West Midlands	9 (9%)	12 (8%)
Wales	8 (8%)	11 (8%)
East of England	7 (7%)	11 (8%)
Yorkshire & the Humber	7 (7%)	11 (8%)
South West	7 (7%)	9 (6%)
East Midlands	5 (5%)	8 (6%)
North East	4 (4%)	5 (3%)
Northern Ireland	2 (2%)	3 (2%)
UK Total	**102**	**144**

Source: Perspective Economics analysis of HESA (Jisc) 2022/23

5.2.2. ENROLMENTS & GRADUATES

Analysis of enrolments and graduations from cyber security and computer science courses have been steadily increasing, as discussed in the previous report. Between the 2020/21 and 2022/23 academic years, enrolments in cyber security courses across North West universities increased by 41%, rising from 1,390 to 1,950.

This is the highest proportional growth of enrolments in cyber security courses across the UK, highlighting how universities have responded to market demand.

Computer science courses have also grown by 13% from 11,230 in 2020/21 to 12,710 in 2022/23.

TABLE 5.2: BREAKDOWN OF STUDENT ENROLMENT AND QUALIFIERS IN CYBER SECURITY AND COMPUTER SCIENCE COURSES IN UK HIGHER EDUCATION INSTITUTIONS (HEIS, 2020/21- 2022/23 ACADEMIC YEARS)

	Enrolments			Graduates		
Year	2020/21	2021/22	2022/23	2020/21	2021/22	2022/23
North West	12,620	13,340	14,660	3,680	4,350	4,560
UK	164,680	177, 480	189,510	42,820	54,410	60,910

Source: Perspective Economics analysis of HESA (Jisc) 2021/22 - 2022/23. Note: numbers are rounded.

A more significant increase is shown in the number of graduates from these programmes.

Over the same period (2020/21 to 2022/23), the number of students graduating from cyber security courses in the region rose by 80%, from 350 to 640. This is higher than the UK-wide average increase of 61% in cyber security graduates, highlighting that the North West is expanding its contribution to the national cyber talent pool at a faster rate than many other regions.

The increases in both enrolments and graduates highlights how the region's universities are enhancing their cyber specific pathways in response to market needs. It also suggests that the region is well positioned to meet employer demand for cyber skills across sectors.

5.2.3. GRADUATE OUTCOMES

The most recent HESA data on graduate outcomes covers the 2021/22 academic year, based on responses to the Graduate Outcomes Survey. This survey captures graduates' activities around 15 months after completing their studies, meaning the data reflects activity between December 2022 and September 2023.

Across the UK, 66% of cyber security and computer science graduates reported being in full-time employment 15 months after graduation. This figure rises slightly to 68% for graduates from universities in the North West. However, these graduates may be employed in any sector, either within the UK or abroad.

Looking at the broader UK context, 8% of all cyber security and computer science graduates reported working in the North West (n= 1,200 graduates employed in the North West). While the majority of those working in the North West graduated from North West based universities, there is notable inflow of skilled graduates from adjacent regions such as Yorkshire and the Humber and the West Midlands.

Within the Graduate Outcomes Survey, we find that among those studying relevant courses in the North West who enter a cyber related role (SIC213) just over half (51%) stay in the region, with 34% moving to other UK regions, and 15% international or other locations for work. However, we also find that of those currently working in a cyber related role in the North West, 46% of these came from other UK universities outside of the North West.

This suggests that for every employed graduate produced by a NW university, the effective combined retention and attraction rate is 0.94 (i.e., the GO Survey highlights 630 graduates created by the North West and 590 working in regional roles), meaning that the region is attractive to graduates from across the North of England. This means that the region benefits from inflows from nearby regions to meet demand in the labour market.

5.2.4. FURTHER EDUCATION

In addition to Higher Education, there remains an important role for a wider range of skills providers in the region. The supply of cyber skills and talent in the North West is boosted by further education courses focused on cyber security and wider tech. Some initiatives are aimed at training and educating young students, whilst others target adults who may desire to retrain or upskill in cyber. Some key examples include:

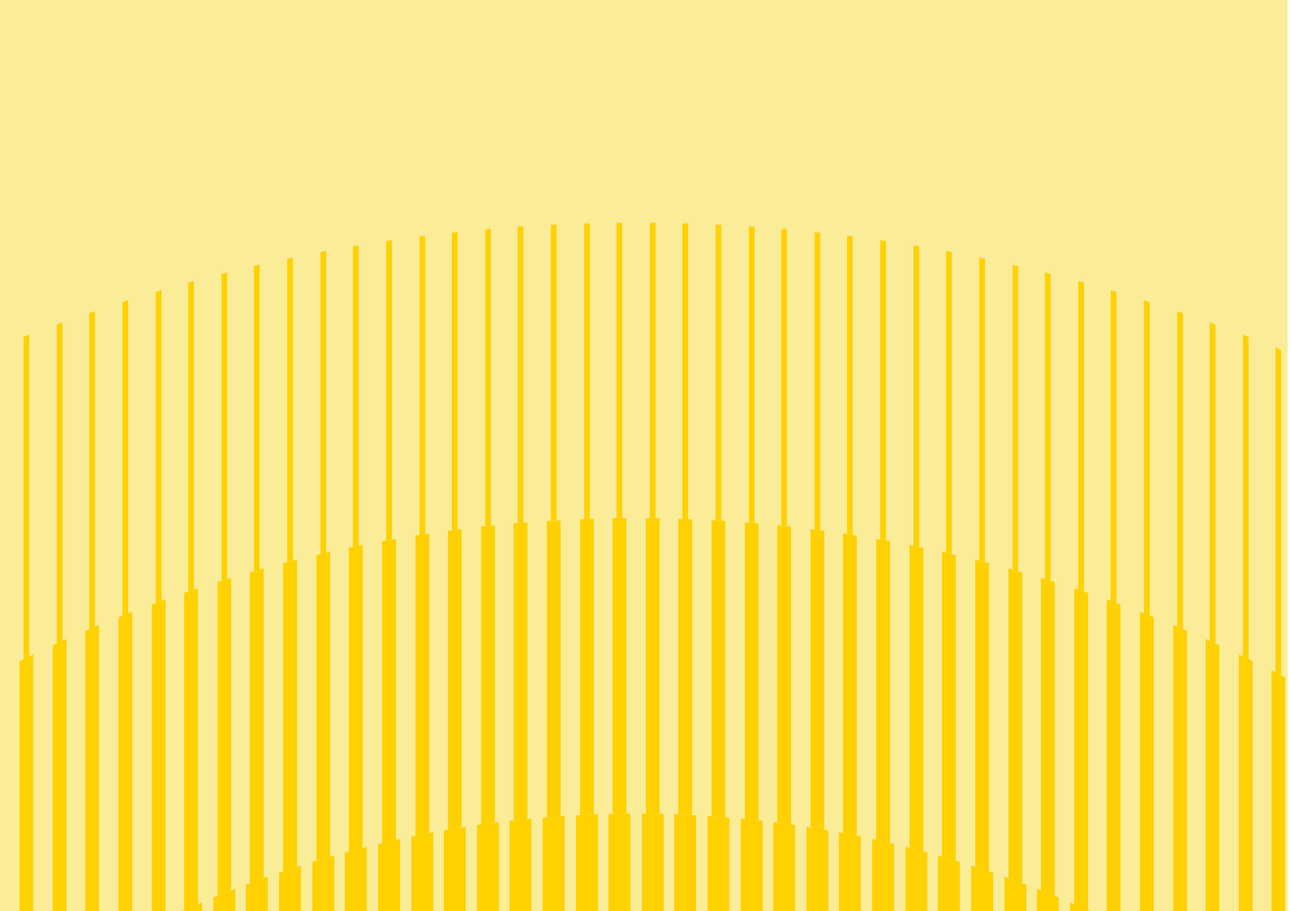
- Blackpool and the Fylde College offer L3 – L6 courses in network engineering, cyber security, and digital support.
- The City of Liverpool College offers an L3 NCFE Certificate in Cyber Security Practices
- Tameside College offers a L4 Higher Technical Qualification in Computing (Cyber Security Pathway)
- Nelson & Colne College University Centre offers a Foundation Degree in Cyber Security and Networking
- The University Academy 92 also offers a Cert HE in Cyber Security, leading to a full BSc (Hons) degree.

6. Benchmarking the Region

6.1. INTRODUCTION

The previous sections updated the 2023 evidence base, highlighting the sustained growth and increasing strength of the North West's cyber security ecosystem. With an expanding role in advanced technologies and manufacturing, defence and national security, supported by a strong network of assets, the region's status as a leading UK hub for cyber security has been further reinforced.

This section updates the key metrics and measures from the baseline evaluation, used to track progress and benchmark the North West against other regions and nationally. We apply a Red-Amber-Green (RAG) rating across business, asset, investment, research, and skills indicators, assessing how the region's performance has evolved in comparison to previous estimates.



6.2. KEY MARKERS

Measure	RAG	Comment
Cyber Security Ecosystem		
Number of Cyber Security Businesses		• 378 cyber security businesses active in the North West (+27% from baseline). • 227 UK registered cyber security businesses have at least one office in the North West (+58% from baseline). • The North West remains the UK's largest cyber security ecosystem outside of London and South East.
Number of Cyber Security Employees		• We estimate that the cyber security workforce in the North West has grown by 19% since the baseline research, from 12,000 to 14,300. • Of these, approximately 6,700 FTEs work in the region's cyber security sector (+34% from 5,000 FTEs). • A further 7,600 FTEs work in wider cyber security related roles in other industries and the public sector.
Evidence of Aligned Industries & Assets		• There are over 172 relevant assets in the North West (+8% from baseline), including c. 20 major players in defence and national security. • There are more than 400 UK registered Artificial Intelligence firms with a North West presence, including c.320 registered offices within the region.
External Investment Raised by Cyber Security Sector		• Cyber security businesses raised £104m in external VC investment in 2024, making the North West the top region in the UK. • This is an increase of 168% (£64.1m) from 2022 (baseline full year). • However, there were still just 6 deals, with one deal amounting to 85% of the region's total cyber security investment (PortSwigger secured £88m in external investment).

Measure	RAG	Comment
Cyber Security Ecosystem		
R&D Activity: Volume & Value of Cyber Security Research Projects		• There are more than 1,300 publicly funded cyber security research projects across the UK between 2020 and 2025. • Of this, there were 80 projects led by organisations from the North West (7% of the count of projects). • The value of these projects amounted to 8% of the UK total, £52.8m of £717m.
Evidence of Support Infrastructure (e.g., accelerators, initiatives)		• The region continues to support businesses through more than 20 high quality co-working and incubation spaces with a digital and cyber security focus. • This includes Manchester's Digital Security Hub (DiSH) which since 2022 has supported 223 businesses, hosted more than 330 events, secured over £40m in funding and helped to upskill c.5.6k people in digital security. • North West Universities partnered in 2024 for the ongoing £4.9m CyberFocus project to create trusted research-led partnerships and boost the region's cyber potential.
Skills & Access to Talent		
Number of Universities (Cyber Security & Related Courses)		• The region continues to support businesses through more than 20 high quality co-working and incubation spaces with a digital and cyber security focus. • This includes Manchester's Digital Security Hub (DiSH) which since 2022 has supported 223 businesses, hosted more than 330 events, secured over £40m in funding and helped to upskill c.5.6k people in digital security. • North West Universities partnered in 2024 for the ongoing £4.9m CyberFocus project to create trusted research-led partnerships and boost the region's cyber potential.

Measure	RAG	Comment
Skills & Access to Talent		
Number of Cyber Security & Computer Science Graduates		• In the most recent academic year for data collection (2022/23), there were 14,660 students enrolled at all levels in cyber security and computer science courses in the North West. • Between 2020/21 and 2022/23 the North West has seen a proportionally higher increase in enrolments across these courses (16% increase), compared to the UK average increase of 15%. • There was a notable proportionally higher increase in the number enrolled in cyber security courses of 41%. • The region also produced 4,560 graduates in cyber security and computer science courses in 2022/23. • The number of cyber security graduates in the region rose by 80% between 2020/21 and 2022/23, higher than the UK wide increase of 61%.
Education Outcomes of Cyber Security & Computer Science		• In the UK, 66% of cyber security and computer science graduates reported being in full-time employment (2021/22 academic year). This rises to 68% for cyber security and computer science graduates from North West universities. • Of those who reported being in full-time employment from North West universities, 58% were working in the North West (+4% from baseline).
Evidence of Wider Skills & Retraining Initiatives		• As part of the CyberFocus project, the consortium will train 300 people in advanced cyber innovation skills to expand the talent pipeline. • The North West Cyber Resilience Centre provides businesses within the region with cyber security skills and knowledge. Funded support is available in Merseyside, Cheshire and Lancashire. • The University of Central Lancashire is now offering Degree Apprenticeships in Cyber Security. • Lancaster University and IN4 Group have partnered to establish CyberFirst Gold Hubs. These hubs will work with education and corporate partners, including IBM, Northrop Grumman, KPMG UK, QinetiQ, and BT, to deliver skills and drive employment through degree apprenticeships and degree courses. • From September 2025 a range of Greater Manchester colleges are planning to offer the Digital T Level (Cyber Security Pathway).

7. Economic Potential & Growth Ambitions

7.1. INTRODUCTION

The previous sections set out how the region's cyber security ecosystem has grown in the last two years since the baseline report.

The ecosystem has grown in line with projections set out within the baseline, and the growth to date continues to suggest there is considerable opportunity to grow the ecosystem further, particularly as new partners such as the National Cyber Force open later in 2025.

As set out within the baseline, 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.

Initiatives such as NWCyberCom and CyberFocus are starting to maximise the infrastructural investments made by the private sector, academia, and organisations such as the NCF and GCHQ – and help to develop a shared ambition and leadership for the region.

Overall, we find that the ecosystem has performed well in the last two years since the baseline, with employment growing at approximately 9% per annum to 14,300 FTEs, and Gross Value Added now exceeding £1bn per annum, growing 15% per annum in the last two years.

The previous baseline report explored sectoral and ecosystem employment growth between 2017-2022 and assumed that the ecosystem could support up to 30,000 FTEs by 2035.

However, as set out within Section 5, whilst the ecosystem supports significant employment, there is some evidence of a tightening labour market, which could potentially reduce opportunities for new talent and investment into new roles. We therefore estimate that under a softened growth forecast (c. 5% per annum), in line with national study estimates, the cyber security ecosystem workforce appears on track to reach approximately 25,000 FTEs by 2035, but additional job creation (such as public investment in defence and increased regional investment) may be required to achieve the 30,000 target.

We summarise this position below, with further analysis in the next subsection.

TABLE 7.1: ECONOMIC PROJECTIONS

	Baseline (2022)	Update (2024)	Revised Mid Target (2035)	Target
Employment	12,000 FTEs in the wider cyber ecosystem	14,300 FTEs	25,000 FTEs	30,000 FTEs
Gross Value Added	£760m	£1,010m	£2.4bn	£2.7bn

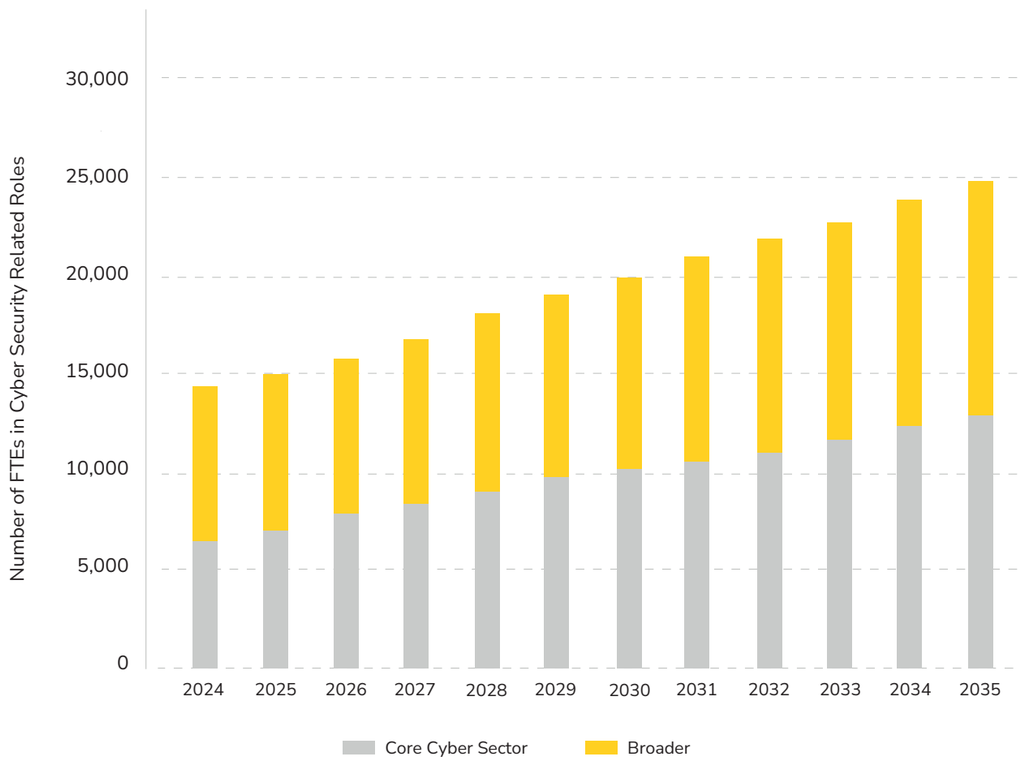
7.2. GROWTH POTENTIAL

Based on the growth to date, we set out potential growth scenarios to 2035 (updated from the baseline). We anticipate potentially softened employment growth to 2035 (as reflected by reducing vacancies), macroeconomic conditions, and tightened conditions in the UK labour market. However, the North West may benefit from crowding-in of public investments as bodies such as the National Cyber Force continue to recruit, and growth from areas such as AI security becomes more embedded.

We estimate the region should reach c. 25,000 FTEs by 2035, with the initial 30,000 figure estimated in 2023 now serving as a 'stretch target' for the region. This assumes:

- 8% Compound Annual Growth Rate (CAGR) in employment in the cyber security sector from 2024 to 2030, reducing to 5% from 2030 to 2025.
- 4% CAGR across all roles in the wider ecosystem, driven by modest public sector and defence growth.

FIGURE 7.1: FORECAST CYBER SECURITY RELATED EMPLOYMENT (FULL ECOSYSTEM)



Source: Perspective Economics forecast

GVA Potential

As set out previously, cyber security is a high-value sector for the North West economy, and this is reflected in employer demand, salaries, and Gross Value Added.

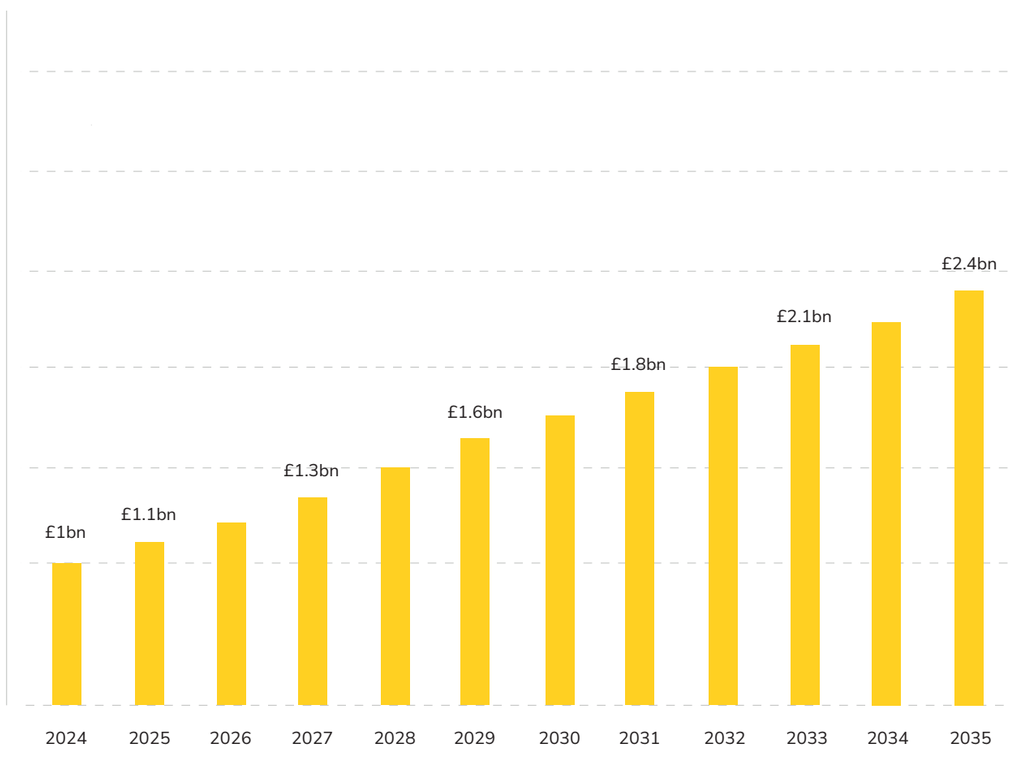
Within the baseline report, the estimated GVA (2022) for the North West was £760m. This estimated GVA on a per employee basis, for those employed in the cyber security sector (based on the DSIT Sectoral Analysis), and using average estimated remuneration for those within the wider ecosystem.

Within this update, we estimate GVA within the most recent year at £1,010m (£1bn).

In line with the baseline forecasts, assuming a 2.5% salary increase for the cyber security sector, and 2% elsewhere, and assuming employment grows in line with the scenario set out – **we estimate that direct GVA from the region's cyber security ecosystem could reach c. £2.4bn per annum by 2035.**

Over the period from 2025 – 2035, this could generate cumulative GVA in excess of £19.8bn for the region.

FIGURE 7.2: FORECAST CYBER SECURITY RELATED GROSS VALUE ADDED (FULL ECOSYSTEM)



Source: Perspective Economics forecast

8. Progress & Next Steps

8.1. INTRODUCTION

This report provides an update to the baseline for the North West Cyber Corridor. Some recommendations were made in the baseline research to help develop the Corridor initiative.

The following table summarises progress against these recommendations and sets out suggested actions to sustain and grow the North West cyber security ecosystem.

Baseline Recommendation	Progress (RAG)	Updated Recommendation
1. Develop an agreed governance structure and strategy for the North West Cyber Corridor		Steering and advisory structures have been formed since the baseline through a range of collaborative programmes that connect the private and public sectors with academia. A website for the North West Cyber Corridor has also been established. The region should continue to progress this partnership towards a formalised governance structure endorsed by and with representation from all sub-regions.
2. Build a coalition of cyber security ecosystem partners		The region has successfully built upon its coalition of partners in the last two years. We note that cross-regional and institutional collaboration has expanded, driven by initiatives such as NW CyberCom, Cyber Focus,
3. Develop a Growth Strategy		Whilst several regional and place-based strategies across the region point to cyber as a growth driver, we note the sustained need to build upon a shared strategic plan to continue to build momentum and buy-in amidst
4. Brand, Identity, and Vision		The region has positioned itself as ‘the heartland of UK defence and security. This brand should be built on by the launch of the NCF and success of regional programmes, leveraging the existing cyber expertise.
5. Resourcing		The region has secured a range of funding for initiatives such as NW CyberCom, fhunded and Cyber Focus, attracting significant public investment in the region’s cyber capabilities. There remains a need for longer-term resource funding and support to enable participation, collaboration, and events across all sub-regions and partners.

In addition, we recommend the following actions should be undertaken to further embed and grow the cyber security and wider ecosystem in the region:

01

Formalising governance and strategy for the North West cyber security ecosystem with full backing and resourcing, including agreed formal governance, membership, and sub-regional collaboration.

02

Furthering regional defence and cyber growth partnerships, with a co-ordinated regional and sub-regional response to anticipated increases in national security and defence spending to 2035. This research highlights that the North West is well placed to participate and maximise opportunities with respect to defence spend, increasing the skills and education pipeline, and attracting early-stage and external investment.

03

Sustained investment in the cyber security skills pipeline. This study notes an increase in the cyber security workforce in the last two years, amidst a significant reduction in active new job postings. As such, the region should ensure sufficient investment in applied skills initiatives (such as Digital Skills for Defence (D4SD), investing in apprenticeships and funded work experience, and undertaking interventions to ensure a competitive workforce e.g. ensuring a supply of highly talented security-cleared employees.

04

Identify opportunities for a regional investment fund for cyber security, working with VCs and investment partners to ensure patient capital is in place.

05

Develop a regional proposition for cyber security strengths in the North West, potentially focuses on secure digitisation within wider national security and defence, and building on the region's emerging strengths in AI Security, potentially exploring opportunities for a regional AI Security Centre of Excellence, and target the region as a leader in AI red-teaming and LLM security testing by 2030, aligned with Government's AI Opportunities Action Plan and defence AI security requirements.

06

Identify opportunities for a Defence Supply Chain Analysis and Assurance initiative. This study has noted that whilst the region is home to almost 400 cyber security firms, there is a much wider defence and supply chain ecosystem, with thousands of wider suppliers. This reflects a dual opportunity for the North West – firstly, to potentially undertake a wider defence ecosystem mapping study exploring wider strengths and supply chain opportunities; but also increasing cyber resilience among the supply chain.

07

Developing international partnerships and gateway opportunities. The North West should seek to formalise partnerships with an agreed number of international cyber clusters (e.g. US, Australia, Singapore, Estonia etc) to promote knowledge transfer, shared R&D, and market access. This should be undertaken with a focus on supporting scale-ups to export and attracting FDI into the region.

08

Commercialising academic IP and bridging the gap: The region has invested heavily in initiatives such as DISH, NW CyberCom, and Cyber Focus to help develop a new pipeline of cyber startups. These have proven successful in increasing the cyber security pipeline. Ongoing support should be provided for firms to secure recurrent revenue, focusing on sales, procurement and working with

perspective economics

2025

Get in touch

Perspective Economics
Pearl Assurance House
1 Donegall Square East
Belfast
BT1 5HB

perspectiveeconomics.com