Cyber Security Labour Market Survey and Sectoral Analysis 2025: Key Findings

Introduction

Nearly half of businesses experienced a cyber breach or attack in the last year!

> *"The threat of breaches are only getting worse. The threats are only becoming more advanced. And I think that the awareness and the understanding of it is going to increase."*
>
> Medium cyber sector business (2025 report)

In the past 12 months, many businesses and charities have experienced a cyber breach or attack

43% of businesses

67% of medium businesses

74% of large business

30% of charities

Source: Cyber Security Breaches Survey 2025

The cost and impact of a cyber breach can extend beyond short-term disruption and damage growth prospects and reputation in the longer-term.

There are a range of tools and guidance offered – from the DSIT Cyber Governance Code of Practice to the NCSC Cyber Security Toolkit for Boards – to help organisations strengthen their cyber resilience. However, the Cyber Security Breaches Survey 2025 suggests:

- Only around three in ten businesses (27%) and charities (30%) have board-level responsibility for cyber security—rising to 66% among large businesses.
- This is a concerning downward trend, down from 38% of businesses in 2021.

Despite these risks, the Cyber Security Breaches Survey 2025 found most businesses and charities were not insuring themselves against cyber attacks, and only around 1 in 5 businesses (19%) and charities (21%) had provided staff training on cyber security within the 12 months prior to the study.

IMPLICATIONS

Preparing for a cyber attack requires strong governance for agile response, skilled teams to defend and react, smart investment in cyber solutions, and assurance that defences are effective. These elements are vital not only for organisational resilience but also for the growth of the UK economy, supported by a thriving cyber sector and a skilled workforce.

Perspective Economics

Ipsos

Growth of the UK Cyber Security Sector

The UK cyber security sector continued its impressive growth trajectory in 2024, solidifying its position as a global leader and a vital contributor to the UK economy:

2,165 cyber security companies active in the UK

67,300 employed in cyber security roles (up 11%)

£13.2 billion in revenue (up 12%)

£7.8 billion in Gross Value Added (GVA) (up 21%)

Venture capital investment in dedicated cyber security businesses attracted **£206 million** in 2024, reflecting a broader tech sector reset driven by macroeconomic conditions and rising interest rates. Notably, the North West led regional investment for the first time, securing 49% of all UK cyber investment (£102 million) across six deals, driven by firms such as PortSwigger.

UK cyber exports also rose to **£7.2 billion** in 2023[1], reflecting strong international demand alongside domestic growth. In the qualitative research, investors continue to back the sector, citing digitalisation, evolving threats, regulation, and emerging tech like AI and quantum computing as key drivers.

> *"We're very bullish on the growth for cyber security. Cyber security is not going away. More and more things are being done online, everything is becoming digital. AI is starting to change the world and that's going to lead to security issues and the need for security around all of that new infrastructure. We think that there's going to be a huge number of very attractive companies to continue to invest in for years to come."*
>
> **Venture capital investor (2025 report)**

Investors valued the government's role in supporting the cyber security ecosystem through incubators and accelerators, enabling connections with early-stage startups and other investors.

1 UK cyber exports statistic from https://www.gov.uk/government/statistics/uk-security-export-statistics-2023/uk-security-export-statistics-2023

IMPLICATIONS

The challenge is to ensure that businesses can access the right investment and skills to support growth, particularly in emerging technologies. Sustained demand and support for the early-stage pipeline will be crucial for growth.

The Regional Picture

Where are the UK's cyber companies?

38% of firms are still registered in Greater London, **17%** in the South East, but **almost half (45%) now sit elsewhere** – with dense clusters in Manchester, Bristol-Bath, Cheltenham, Belfast and Glasgow.

Money follows talent

In 2024, the **North West captured 49% of UK cyber venture capital (£102 million)** – the first time any region has out-raised the capital. London and the South East delivered 51% of all deals yet only 35% of deal value, signalling a healthier spread of growth capital.

Jobs are becoming less London-centric

One in four cyber vacancies were advertised as remote/UK-wide last year, and the London salary premium has narrowed to **£11,000** compared to the UK average (London £69,800 vs £58,800 across regions).

IMPLICATIONS

There is a need to look beyond aggregate national statistics and take a regional perspective on growth, skills gaps and challenges. Schemes such as Cyber Runway and new capital funds for seed investment in UK cyber firms such as Osney Capital's cyber fund can help unlock capital across the regions. Public procurement can help channel more defence and critical infrastructure spend into high-growth clusters.

Cyber Security Skills and Labour Market

UK businesses continue to face cyber security skills shortages, leaving many organisations and supply chains vulnerable to common cyber threats.

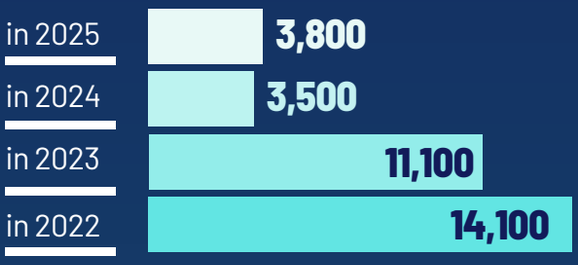
49% of businesses have a **basic** technical skills gap including setting up firewalls, managing personal data securely and detecting malware

30% of businesses have an **advanced** technical skills gap including forensic analysis, interpreting malicious code, and penetration testing

28% of cyber businesses report a lack of technical skills among their existing employees

While these challenges persist, there are signs of progress: the overall supply of cyber security skills in the UK economy is improving—suggesting that businesses now have greater opportunities to invest in upskilling their workforce and closing these critical gaps.

The cyber security workforce gap – the shortfall between people *needed* in the workforce and the people *entering* the workforce – fell sharply after the post-pandemic boom and has since stabilised.



This reduction reflects both increased **supply** through graduates and apprenticeships, and a slowdown in **demand** for cyber security professionals.

Supply

An estimated 9,100 new individuals entered the cyber security labour market in 2024:

- 6,000 new graduates (up 20% in the past academic year)
- 2,500 individuals via retraining and upskilling initiatives
- 600 new apprenticeships

Demand

Demand for cyber security and entry-level professionals has slowed for two consecutive years:

- Core cyber job postings declined by 33% in 2024
- The wage premium for cyber jobs over general IT jobs has continued to shrink from 33% in 2022 to 12% in 2024
- Demand for entry-level candidates has fallen from 25% in 2022 to 17% in 2024

IMPLICATIONS

The cyber skills challenge is shifting from growing the workforce to better aligning talent with demand, requiring regional and technical focus. In the UK, this means addressing regional gaps through targeted training, remote work, and emerging tech initiatives, while also developing advanced skills in areas like cryptography and AI.

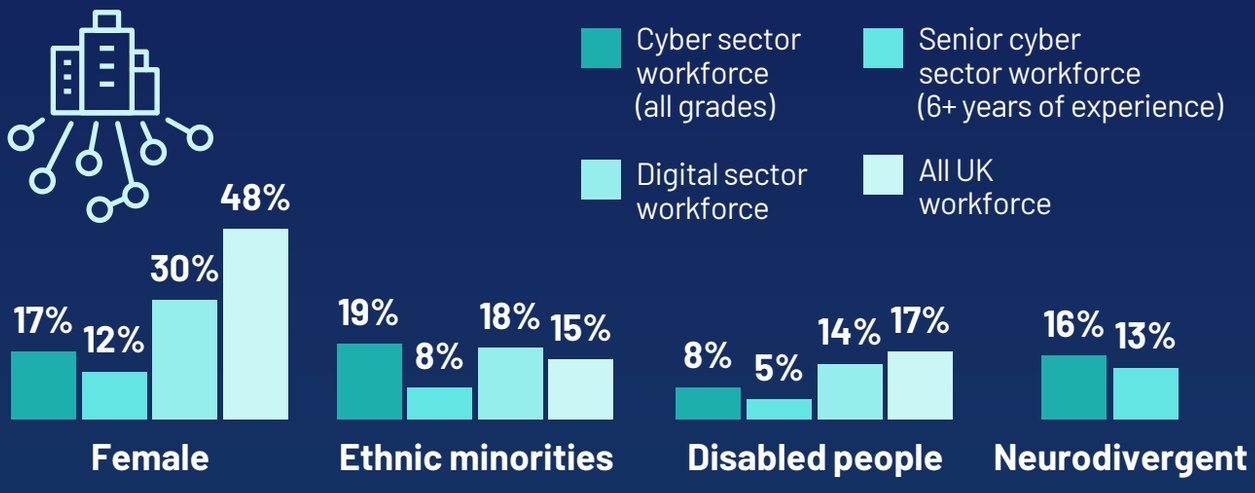
Perspective Economics

Ipsos

Diversity of the Labour Market

The diversity of the cyber sector workforce continues to be a challenge, although there have also been some encouraging developments.

The cyber sector workforce remained less diverse than the wider digital sector and the UK workforce as a whole, particularly within the senior cyber workforce (those with 6+ years experience).



Increase in neurodivergent staff reported by employers

from **9%** in 2020

to **16%** in 2025

Continuous incremental improvement in women enrolled on postgraduate cyber courses

from **21%** in 2020/21

to **27%** in 2022/23

The most common actions cyber sector employers have been taking to diversify their recruitment practices were hiring through non-degree routes (63%) and outreach activities in schools and colleges (41%). Recruitment agents often played an important role in educating employers on how to achieve diversity when hiring.

"I wish there was more support in this area. You can observe that the pool is not as diverse as it needs to be. But I'm not necessarily educated enough to see how to solve that problem."
Micro cyber sector business (2025 report)

As in previous years, the qualitative research highlighted persistent challenges to improving diversity in the cyber sector:

- Perceived limited diversity in the talent pool
- Financial costs associated with degrees and qualifications
- Negative stereotypes of the sector

IMPLICATIONS

More action is needed to increase the diversity of the cyber workforce, including identifying where and how to attract candidates from diverse backgrounds into the sector, encouraging employers to be part of diverse networks and improving senior progression and representation.

AI and Cyber Security

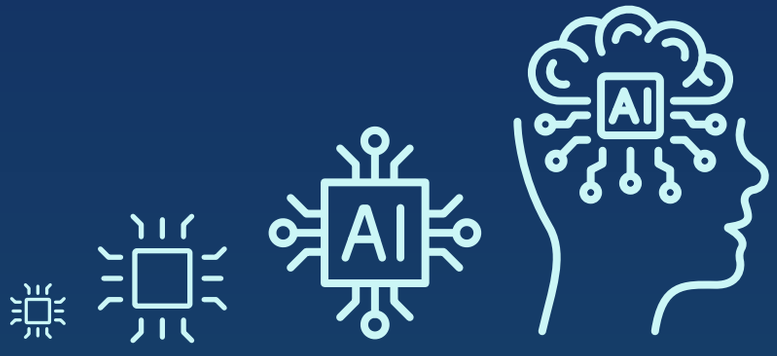
The DSIT AI and Software Security Market Analysis (March 2025) identifies just 66 UK firms specialising in AI security. That number is expected to climb quickly as demand for guardrails, assurance, ethics, explainability and secure-by-design tooling accelerates. A robust AI security ecosystem is critical to the UK economy.

53% of cyber sector businesses said their staff were using AI in their day-to-day work

but only

42% Reported that any of their staff had received training on AI concepts or algorithms

Of those cyber sector businesses that had tried to recruit in the 18 months prior to the survey, only 15% had recruited anyone with AI skills into a cyber security role. However, with 2 in 3 cyber sector businesses (65%) expecting their need for AI skills among employees to increase over the next 12 months, the demand for AI talent is likely to increase.



65% of cyber sector businesses expected their need for AI skills to grow in the next 12 months

In the qualitative research, employers expressed concern about current and future shortages of technical skills in relation to AI within cyber security. We heard that the rapid pace of AI advancements makes it challenging for training and certifications to keep up with the latest developments.

> *"You could easily have a training module written on a Monday, and it would be out of date by Friday in terms of the pace of change and growth in AI."*
>
> Medium cyber sector business (2025 report)

IMPLICATIONS

Upskilling the cyber security workforce in AI is required to close the skills gap in a rapidly evolving area. AI concepts and use cases need to be integrated into cyber training pathways. It is also key to support cyber security professionals and the wider sector with knowledge dissemination and support in areas such as AI and supply-chain risk, through guidance such as the DSIT AI Cyber Security Code of Practice.

Cyber Security Labour Market Survey and Sectoral Analysis Research Design:

- Representative surveys of cyber sector businesses (209 respondents) and the wider population of UK organisations: businesses (1,061 respondents), charities (197 respondents) and public sector organisations (111 respondents).
- Qualitative interviews with cyber sector businesses, private and public sector organisations, investors, training providers, and recruitment agents (50 interviews total).
- Secondary analysis of cyber security job postings on the Lightcast labour market database, as well as reviewing the supply of cyber security talent through sources such as the Higher Education Statistics Authority (HESA) and DfE, and VC investments via Beauhurst.
- This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252.

Research reports:

Cyber Security Sectoral Analysis 2025:
https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2025

Cyber Security Labour Market Analysis 2025:
https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2025

Perspective Economics

Ipsos