

Cyber security skills in the UK labour market 2026

Findings report

Jayesh Shah, Alex Bollen, Jamie Douglas, Sophia Hasapopoulos, Natasha Angus
and Eilidh Roberts (Ipsos)
Sam Donaldson and Jade Rosborough (Perspective Economics)



Contents

Summary.....	1
1 Introduction and methodology.....	3
1.1 About this research.....	3
1.2 Summary of the methodology	3
1.3 Interpretation of the data	4
1.4 Acknowledgements.....	6
2 Mapping the workforce.....	7
2.1 Size of the cyber security workforce	7
2.2 Comparison to Standard Occupational Code (SOC) data	8
2.3 Composition of cyber security teams within the cyber security sector	9
2.4 Staff turnover in the cyber security sector	11
2.5 Awareness of the UK Cyber Security Council and its work.....	11
2.6 Qualitative feedback on attitudes towards chartered professional standards.....	12
3 Diversity in cyber security	14
3.1 Estimates of diversity in the cyber security sector.....	15
3.2 Higher Education student demographic profiles	19
3.3 Engagement with skills and diversity initiatives in the cyber security sector	20
3.4 Engagement with diversity initiatives in recruitment processes	21
4 Demand for cyber security skills	23
4.1 Number of job postings	23
4.2 Geographical differences	27
4.3 The job roles being advertised	29
4.4 Sectoral demand for cyber roles	30
4.5 The skills, experience and qualifications being demanded	31
4.6 Salaries	34
5 Supply of skills	37
5.1 Higher Education data	37
5.2 Apprenticeship data	44
5.3 Retraining and upskilling	46
5.4 The effectiveness of entry-level pathways.....	47
6 Skills gaps and shortages.....	49
6.1 Technical skills gaps within the cyber security sector	50
6.2 Technical skills gaps outside the cyber security sector	51
6.3 Incident response skills.....	54
6.4 Complementary skills	55
6.5 AI skills in cyber security	56
6.6 Qualitative feedback on other future skills needs.....	59
6.7 Governance and compliance skills	60

6.8 Cyber security skills gaps in the wider workforce61

6.9 Outsourcing64

6.10 Hard-to-fill vacancies and skills shortages in the cyber security sector68

7 Conclusions71

8 Annexes.....74

Summary

This is a summary of research into the UK cyber security labour market, carried out by Ipsos and Perspective Economics on behalf of the Department for Science, Innovation and Technology (DSIT). The study involves:

- Representative surveys of cyber security businesses and the wider population of UK organisations (businesses, charities and public sector organisations).
- Qualitative research with cyber security businesses, medium/large private and public sector organisations, training providers and recruitment agents.
- A secondary analysis of cyber security job postings on the Lightcast labour market database and reviewing the supply of cyber security talent through sources such as the Higher Education Statistics Authority (HESA) and Jisc.

This is the eighth iteration of the research, which has been carried out on an annual basis since 2018. This year we asked new questions on awareness and engagement with diversity and cyber skills development initiatives.

Mapping the workforce

Growth in the UK cyber security workforce is slowing. It comprises approximately 145,900 individuals, representing only a slight, 2%, increase compared to the previous year. Recruitment expectations show 53% of cyber firms expect to grow their workforce in 2026, a decline from the 2025 study. However, average core cyber job postings grew 7% compared with 2024.

Geographic distribution of cyber job postings shows Greater London, Manchester, Birmingham, and Bristol holding the top four positions in the UK, with Edinburgh replacing Leeds in fifth position.

Supply of skills

There continues to be an increase in the number of cyber security graduates, with 14% growth recorded between the 2022/23 and 2023/24 academic years to 7,950 graduates. However, there was also a 15% reduction in enrolment in cyber security specific apprenticeships from 2023/24 to 2024/25.

Demand for cyber security skills

Demand may have begun to recover from the lows observed in 2024. There was a 7% increase in core cyber security job postings (jobs where some aspect of cyber security is the main job function) and an increase of 10% for all cyber security job postings (roles that may not formally be labelled or commonly recognised as cyber security jobs but still require cyber security skills).

Diversity in cyber security

The cyber security sector workforce continued to be less diverse compared to the wider digital sectors and the UK workforce as a whole. Only 16% of the cyber security workforce was female compared to 48% of the UK workforce. Just under 1 in 10 (9%) were disabled compared to 18% of the UK workforce. There has been an increase in the proportion of neurodivergent staff reported by employers, from 9% in 2020 to 22% in the 2026 report, though this could reflect improvements in the identification and reporting of neurodiverse conditions.

Skills gaps¹

There continues to be a cyber security skills gap. Over half (57%) of businesses had a basic technical skills gap, an increase from last year (49%).

Almost half of individuals responsible for cyber security in UK businesses and charities (47% each), lacked the confidence to deal with cyber security breaches or attacks, and had not outsourced this function

AI skills

AI skills are becoming increasingly important in the cyber security sector and there is an expectation, highlighted in the qualitative research, that AI and automation will transform the cyber security sector. More cyber security businesses were using AI in cyber security, with 70% reporting that staff were using AI in their day-to-day work, up from 53% last year.

Diversity and skills initiatives

New questions for this year showed that most cyber security firms were involved with diversity or skills initiatives, the most common activities being delivering talks or workshops in schools or colleges and offering work placements

¹ Basic technical skills were a combination of the technical areas covered under the government-endorsed Cyber Essentials scheme and other basic aspects of cyber security. Advanced technical skills may not be required in every organisation but are important for those with more sophisticated cyber security needs.

1 Introduction and methodology

1.1 About this research

The Department for Science, Innovation and Technology (DSIT) commissioned Ipsos and Perspective Economics to conduct the latest in an annual series of studies (since 2018) to improve its understanding of the UK cyber security labour market and skills needs. The research covers UK private sector businesses – both those that form the UK's cyber sector, providing cyber security products and services, and also wider private sector businesses (with 1 or more employees) managing their own cyber security – as well as charities and public sector organisations. It also collected data from cyber security training providers and recruitment agents.

This 2026 report, in line with previous years, covers the data on:

- the size and composition of the cyber security workforce
- staff turnover (within the cyber sector)
- awareness and perceptions of the work of the UK Cyber Security Council – including the Cyber Career Framework and the [Standard for Professional Competence & Commitment](#)
- diversity within cyber security, with quantitative data specifically for the cyber sector
- awareness of diversity and cyber skills initiatives in the cyber security sector
- demand for cyber security skills, based on an analysis of online cyber security job vacancies
- the supply of cyber security skills, based on secondary data covering Higher Education pathways, apprenticeship programmes, and professional retraining and upskilling initiatives
- cyber security skills gaps and skills shortages within and outside the cyber sector
- the use of outsourcing to fill cyber security skills gaps.

This research was conducted alongside a sister study, also for DSIT, which focused specifically on the UK's cyber security sector, covering sector growth and investment – the [Cyber Security Sectoral Analysis 2026](#).

1.2 Summary of the methodology

This section contains a brief outline of the research methodology. Further methodological detail can be found in the accompanying technical report.

The methodology consisted of 4 strands:

- **Quantitative surveys** – Ipsos conducted representative telephone surveys with 4 audiences: UK private sector businesses (outside the cyber sector), public sector organisations, registered charities, and cyber sector businesses (i.e., those providing cyber security products or services). Fieldwork was conducted between 8 August and 27 October 2025. The data for the private sector, public sector and charities has been weighted to be representative of these populations, while the data for the cyber sector is considered representative of that sector, since the entire sector was sampled.
- **Qualitative interviews** – Ipsos conducted 51 in-depth interviews relevant to this labour market research, including 25 with cyber sector businesses (other than training providers), 11 with cyber leads in medium and large private sector businesses and public sector organisations, 5 with

investors in cyber security, 5 with recruitment agents and 5 with cyber security training providers. Our sample was not representative. Therefore the conclusions from qualitative data should not be interpreted as definitive. The interviews explored the challenges organisations faced in addressing skills gaps and shortages, approaches to recruitment, workplace diversity, and factors impacting the development of skills in the cyber security workforce. This fieldwork took place between 15 September and 1 December 2025.

- **Job vacancies analysis** – Perspective Economics analysed cyber security job postings on the Lightcast labour market database, providing details on the number, type and location of job vacancies across the UK. This analysis also covered remuneration, descriptions of job roles and the skills, qualifications and experience being sought by employers. We primarily focused on vacancies across the 2025 calendar year (i.e., January to December 2025).
- **Supply side analysis** – Perspective Economics replicated the methodology used in the previous report to estimate the size of the cyber security recruitment pool. This used the latest published data on graduate enrolments from the Higher Education Statistics Authority (HESA) and Jisc, the HESA Graduate Outcomes survey 2023/24, the latest Department for Education apprenticeship data for England, and wider data on professional retraining and upskilling initiatives. This strand also produced further statistics on the demographic characteristics, educational and occupational backgrounds, and salaries of this pool of labour, as well as outflows from the pool.

1.3 Interpretation of the data

Years of data covered

Throughout this report, when referring to changes over time, we typically reference the publication year (i.e., 2026 for this latest report). However, it is important to note that the primary quantitative and qualitative data was collected in the previous calendar year (i.e., 2025). This is explicitly mentioned in each figure and chart title. To be consistent with previous reports, line charts based on survey data use the report publication year in the x axis, rather than the fieldwork year.

Furthermore, due to the use of multiple methodologies, the report references data from various time periods, summarised below:

- quantitative survey data collected between August and October 2025
- qualitative data collected between September and December 2025
- job vacancies data from January to December 2025
- 2023/24 data on graduate enrolments from HESA and Jisc
- the HESA Graduate Outcomes survey 2023/24 (covering graduates from the 2022/23 academic year, approximately 18 months after their graduation)
- Department for Education apprenticeship data for England (covering the 2024/25 academic year).

Charting of survey results

Where figures in charts do not add to 100%, this is typically due to rounding of percentages that come from weighted data, because the questions allowed more than one response, or because not all responses have been charted for the sake of visual clarity.

Subgroup analysis for businesses

We have undertaken subgroup analysis on the quantitative survey data for businesses, to show how findings differ by business size and sector. There were too few public sector organisations and charities sampled to split out results for these organisations by subgroup.

For businesses, the analysis by size split the population into micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more).

In our sector subgroup analysis, we grouped similar sectors together by SIC 2007 code for higher sample sizes. The groupings are the same ones used in DSIT's [Cyber Security Breaches Survey](#) series. Ultimately, there were relatively few major sector differences to report on, but this is the full list of sector groupings that we looked at in the subgroup analysis:

- administration and real estate (SIC L and N)
- construction (SIC F)
- education (including academies) (SIC P)
- entertainment, service or membership organisations (SIC R and S)
- finance and insurance (SIC K)
- food and hospitality (SIC I)
- health, social care and social work (including NHS organisations) (SIC Q)
- information and communication (SIC J)
- professional, scientific or technical (SIC M)
- retail and wholesale (including vehicle sales and repairs) (SIC G)
- transport and storage (SIC H)
- utilities and production (including manufacturing) (SIC B, C, D and E).

Typically, we compared each sector to the average private sector business. The education sector and health, social care and social work sector include a large mix of private and public sector organisations. We therefore analysed these sectors using a merged sample of private and public sector organisations, specially weighted to represent a merged population profile.

The quantitative survey found few noteworthy or consistent regional subgroup differences. Therefore, we have typically not commented on these across the report. We do, however, have a far more substantial geographic analysis as part of the secondary analysis of job vacancies (covered in Chapter 4).

Statistical significance testing (for subgroups and changes over time)

The survey results are subject to margins of error, which vary with the size of the sample and the percentage figure concerned. We carry out statistical significance tests, which signify whether differences across the results are likely to be real differences in the population, or likely to have occurred by chance.

In this report, where we highlight any subgroup differences by business size or sector, or any other variable, these are statistically significant differences (at the 95% level of confidence) – unless the commentary states otherwise. Similarly, where we indicate that findings have changed since the previous studies, this is indicating a statistically significant change over time unless otherwise stated.

Specifically, this report contains several workforce-level estimates compiled from cyber sector survey data. They estimate the percentage of the cyber sector workforce with certain traits (e.g., the proportion of the cyber sector workforce that is female), unlike most of the reported data for the cyber sector, which represents the percentage of cyber sector businesses. We do not expect to find statistically significant differences over time in these estimates given sample size limitations. Instead, we focus on broad trends and patterns in the data when analysing workforce-level estimates.

Interpretation of the qualitative data

The qualitative findings offer more nuanced insights and case studies into how organisations address their cyber security skills needs, and why they take certain approaches. The findings reported here represent common themes emerging across multiple interviews.

Where we pull out an example, insight or quote from one organisation, this is typically to illustrate findings that emerged more broadly across multiple interviews. As with any qualitative findings, these examples are not intended to be statistically representative of the wider population of UK organisations.

1.4 Acknowledgements

Ipsos and Perspective Economics would like to thank colleagues at DSIT for their project management, support and guidance throughout the study. This research was also endorsed by the National Cyber Security Centre (NCSC), the UK Cyber Security Council (UKCSC), the UK Cyber Cluster Collaboration (UKC3), techUK, teiss and the Security Awareness Special Interest Group (SASIG).

2 Mapping the workforce

This chapter estimates the size of the UK cyber security workforce across the whole economy (accounting for inflows and outflows since the previous study). Within the cyber security sector specifically, it includes survey data on the typical size of cyber teams, staff turnover, and cyber teams' coverage of the specialisms outlined in the UK Cyber Security Council's [Cyber Career Framework](#).

Both the Council's Cyber Career Framework and their [Standard for Professional Competence & Commitment \(UK CSC SPCC\)](#) were also topics for discussion in the qualitative interviews. Businesses, cyber leads and training providers provided broad feedback on the utility of these initiatives, building on the discussion of the Cyber Career Framework in the previous study.

The current picture

There are approximately 145,900 individuals in the cyber security workforce. The longer-term trend shows workforce growth has slowed considerably, increasing by only 2% since last year, compared to 5% growth from 2023 to 2024. This reflects a more challenging labour market.

Within the cyber security sector specifically, small cyber teams continued to dominate, with the median cyber security firm having 3-4 employees and almost a quarter (23%) having just 1 employee in a cyber security role. The top 3 cyber security specialisms were cyber security governance and risk management (45%), cyber security management (37%) and cyber security audit and assurance (37%), following the same pattern seen last year.

What's new since the 2025 report?

Staff turnover showed slight increases, with 14% of cyber security sector employees leaving their roles in the 18 months prior to the survey (compared to 12% in 2025 and 11% in 2024, 2023 and 2022). Recruitment expectations have moderated, with 53% expecting to grow their workforce compared to 67% in 2025, while 46% expected no change versus 30% in 2025.

Awareness of the UK Cyber Security Council reached 74%, up from 69% in the previous study. The qualitative research found that despite some positive developments, there were mixed opinions on the value of chartered professional standards, with concerns about accountability, implementation costs, certification fatigue, and lack of international recognition.

2.1 Size of the cyber security workforce

This chapter explores the size and composition of the UK cyber security workforce across the whole economy.

There are an estimated 145,900 individuals in the cyber security workforce (across employment and self-employed roles) as of December 2025. This is a small increase (+2%, +2,900 individuals) compared to the previous study and reflects wider findings within this study regarding a more challenging labour market compared to previous years.

This represents a slower rate of workforce growth compared to recent years (having grown by 5% from 2023 to 2024) and is a leading indicator of a potentially challenging labour market, particularly for early talent. This comes amidst sustained levels of reduced demand (through advertised vacancies), covered further in Chapter 4.

The workforce size is an experimental estimate undertaken by the Ipsos and Perspective Economics research team. It is informed by economic analysis of employment data within employers in the cyber security sector², and cyber security related roles within the wider labour market. The following sets out the supply and demand estimates for 2026. Previous versions of this study have provided an estimate of the workforce gap in the UK. This has been removed as the estimate inevitably makes various assumptions, which are necessitated by the limitations of the available data, and due to reduced demand for roles. It is also in line with wider research such as the [ISC2 Cybersecurity Workforce Study](#) which has also not included an estimate of the workforce gap for similar reasons.

The current cyber security workforce, as of 2025, is estimated to be around 145,900 individuals.

In 2025, we estimate that approximately 8,600 individuals entered the cyber security workforce through formal education and training pathways (see Chapter 5).

Graduate supply has grown in recent years, particularly driven by universities providing additional cyber security related courses in response to market demand, and increased demand among students.

Further, whilst new supply of talent can help to address market demand, it is worth noting that a percentage of the cyber security workforce will exit each year, due to factors such as retirement or changes in careers. We estimate, based on survey data, that approximately 4% of the workforce may leave in each given year. Applying this rate to the 2025 workforce estimate of 145,900 suggests that approximately 5,800 individuals will leave the cyber security workforce in 2026. It is important to note that this outflow does not capture frictional unemployment such as redundancies, and regional specificity is limited. The expected demand for cyber security professionals in 2026

DSIT's [Cyber Security Sectoral Analysis 2026](#) (the most recent published analysis) estimates that the UK's cyber security sector workforce grew by 3%, from 67,299 in 2024 to 69,589 in 2025. This only accounts for the employees of businesses that sell cyber security products or services, i.e., it does not include cyber security professionals working in other sectors. However, it provides a baseline against which to base an estimate for the growth in demand for cyber security professionals, across all sectors.

Our estimate for the entire cyber security workforce assumes a growth in demand level with the UK cyber security sector (3%). This growth rate reflects this year's data showing a slowing of demand in online job postings for core cyber and wider cyber roles (see Section 4.1). The 3% growth rate suggests a need for approximately 4,400 new people in 2026 to meet new demand, in addition to the 5,800 to replace those exiting the sector, i.e., this suggests a total supply requirement of approximately 10,200 per year for the cyber security workforce in 2026.

2.2 Comparison to Standard Occupational Code (SOC) data

In recent years, the ONS Annual Population Survey has estimated the count of occupations across the UK population by the revised SOC (Standard Occupation Classification) 2020 code³. This includes

² There are an estimated 69,589 Full Time Equivalent (FTEs) working in a cyber security related role across the 2,603 cyber security firms identified in the [Cyber Security Sectoral Analysis 2026](#).

³ SOC2020 classification volumes. Available at:

<https://www.ons.gov.uk/methodology/classificationsandstandards/standardoccupationalclassificationsoc/soc2020>

SOC2135 (Cyber Security Professionals), which the most recent data (January 2025 to December 2025) estimates a total of 80,400 individuals in the profession in the UK.⁴

This is an increase from an estimated 69,900 (+15%) in the previous year. However, this may be subject to annual variance. Firstly, the Annual Population Survey is not an accredited Official Statistic due to a fall in the response rates and, consequently, in the achieved sample sizes. Secondly, respondents may be more likely to self-report as a cyber security professional as a result of overall professionalisation and career pathways supported by initiatives such as the [Cyber Security Council's Chartered Cyber Security Professional title](#). In addition, individuals working in cyber security-related roles may be coded or self-report into another area, such as programming or consultancy, even if their role mainly encompasses cyber security (e.g. a software engineer working for a cyber security firm).

As such, our estimate of 145,900 individuals in the cyber security workforce is considered a broader estimate of all cyber security related roles across all sectors and pathways.

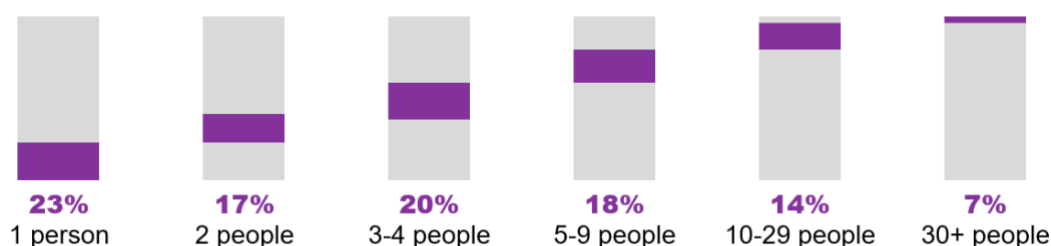
2.3 Composition of cyber security teams within the cyber security sector

This section specifically focuses on survey data for the cyber security sector.

The latest [Cyber Security Sectoral Analysis 2026](#) highlights that 58% of cyber security businesses were micro in size, employing less than 10 people and with a turnover of less than £1 million. As such, it is expected that most cyber security team sizes across the sector will be at the smaller end. In the latest Cyber Security Skills Survey, around a quarter (23%) had 1 employee in a cyber security role, while the average cyber security firm had 3 to 4 employees.⁵

The overall composition, shown in Figure 2.1, was similar to the last 3 waves. The median cyber security team size in the last 3 waves was 3 to 4 employees, compared to 5 to 9 employees in the 2023 and 2022 studies.

Figure 2.1: Percentage of UK cyber security businesses by the number of people working in cyber security roles



Base: 230 cyber security businesses

⁴ Office for National Statistics (2025). Annual Population Survey - Occupation (SOC2020) by sex, employment status and full/part-time. [January 2025–December 2025]. Available at: <https://www.nomisweb.co.uk/datasets/aps218/reports/employment-by-status-and-occupation?compare=K02000001>

⁵ The mean was 9 employees, however this higher mean was driven by 3 large cyber security firms being included in our sample in the current study, rather than reflecting a true shift across the cyber security sector. The mean in the previous year's wave was 7 employees.

Cyber security sector recruitment expectations

Just over half (53%) of cyber security businesses expected to grow their workforce and just under half (46%) expected no change. Compared to the previous study, there was a marked decline in those expecting to increase their workforce (67% in 2025) and more employers expecting their workforce not to change (30% in 2025 vs. 46% in 2026). This aligns with the wider data in this study, with cyber security employment within the UK cyber security sector growing by only 3% in the most recent sectoral report (2025), and Lightcast job posting data suggesting that demand for core cyber roles remains at lower levels in 2024 and 2025 when compared with previous years (this is explored in detail in Chapter 4).

Specialisms of cyber teams within the cyber security sector

Cyber security businesses were asked whether their organisation employed staff in any of the 15 specialisms set out in the [Cyber Career Framework](#) (see Figure 2.2).

The top 3 specialisms were cyber security governance and risk management (45%), cyber security management (37%) and cyber security audit and assurance (37%). At the other end, digital forensics (10%) and cryptography and communications security (12%) were least commonly reported.

Figure 2.2: Percentage of UK cyber security businesses that employ people in cyber security roles covering each of the following Cyber Career Framework specialisms



Base: 230 cyber security businesses

This study saw an increase in cyber security firms employing people in network monitoring and intrusion detection roles, rising from 15% last year to 23% in this wave.

2.4 Staff turnover in the cyber security sector

In the 18 months prior to the survey (i.e., since around January 2024), an estimated 14% of employees working in the cyber security sector reported leaving their role. This includes 9% who left voluntarily, 3% leaving for redundancy, and 1% each leaving for dismissal and retirement. The turnover rate has risen slightly when reflecting over a longer period (14% in 2026, 12% in 2025, and 11% in 2024, 2023 and 2022). Although these changes are not statistically significant, they can be taken as an indication that staff turnover may be starting to gain momentum.

The above estimates should be interpreted as lower bounds. In calculating the size of the workforce, we assume that all staff who left during the period were already in post 18 months earlier. This excludes individuals who both joined and left within the 18-month window, potentially leading to an underestimation of true staff turnover.

In previous studies, the wider business population was also surveyed, as well as charities and public sector organisations on the size of their cyber teams. However, this question has not been included since the 2024 study to improve survey design.

In the qualitative research, there continued to be a perception that employees were staying in their jobs because demand for cyber security professionals had slowed. One recruitment agent commented that this was limiting the progression of people in mid-level roles.

“There’s nowhere for them to go. But then there’s people coming up behind them who are 45 to 55, and there’s nowhere for them to go because the market got into this vacuum.”

Recruitment agent

2.5 Awareness of the UK Cyber Security Council and its work

There is a high level of awareness built up since the UK Cyber Security Council (UKCSC) was created in 2021, with 74% of cyber security businesses having heard of it. This indicates a rise in awareness of the Council compared to the previous study (69%), although this change is not statistically significant given the low base size.

As has been the case in the qualitative feedback from previous studies, the UKCSC’s Cyber Career Framework was praised for its value in providing entry-level career guidance and demonstrating the breadth of cyber security roles.

“I do think this looks good. It’s a positive way forward. It helps to articulate and communicate because it can be quite overwhelming and complex when you’re talking about cyber because there are so many different areas. Having something like this that explains in a digestible format what all of those roles mean, what day to day is, what it looks like and what qualifications beginners intermediate experts need to obtain to pursue. I think that’s useful.”

Large public sector

However, it appeared that initial awareness of the framework did not always translate into sustained engagement. Several participants who were introduced to the framework in the qualitative research in the previous study were unable to spontaneously recall it, suggesting a need for further sustained promotion.

"I just thought this hasn't really been packaged for explaining the story to the people it affects."

Large cyber security sector business

Similar concerns to the previous studies were raised regarding the framework's practical implementation. Some participants questioned how overlapping specialisms translated into real-world roles, where responsibilities would often be combined and span several specialisms.

"How do you then bring some of these together for a job that's in the real world? Because in lots of organisations the subjects are joined together."

Large non-cyber security (private sector) business

One employer also queried whether the framework created unrealistic expectations about current job availability, particularly for entry-level applicants.

2.6 Qualitative feedback on attitudes towards chartered professional standards

In 2025, the UKCSC continued to roll out chartered professional standards for the 15 cyber security specialisms in the Cyber Career Framework. At the time of the qualitative fieldwork (September to December 2025), it was possible to obtain professional registration in 8 specialisms. A few instances were identified of cyber security firms considering or securing registration to comply with requirements attached to certain contracts or schemes (e.g., the National Cyber Security Centre's CHECK assurance scheme for penetration testing).

Consistent with the previous studies, there were mixed views on the value of chartered professional standards. As these standards were rolled out, there was more feedback on implementation challenges. Some participants raised concerns about regulatory backing and governance and the need for proper accountability mechanisms.

"I think it will be worth it when people are held to account. If we take things like chartered accountants, for example, there are very clear ramifications if you do not keep up with the ethics and the code that you sign up to. The same thing should happen with this."

Micro cyber security sector business

Two other implementation challenges were mentioned. Recruitment agents reported a sense of 'certification fatigue' among cyber security professionals due to the proliferation of paid certifications. The lack of international recognition of the professional standards was a concern for globally operating organisations.

Training providers raised concerns about the cost barriers of achieving relevant charterships, noting the burden on small and medium-sized enterprises (SMEs) that relied on multi-skilled practitioners who worked across multiple specialisms. It was thought that this would mean that a single employee would need to obtain multiple charterships to cover all areas of their work. Cyber security sector businesses echoed this, suggesting that smaller businesses would not have the scale or complexity to necessarily "tick all the boxes" or silo skills in an environment where more generalist roles were desired.

"We're asking to be chartered in all those different things, which takes lots and lots of time, lots of CPD [continuing professional development] effort and is very expensive for small companies."

Training provider

3 Diversity in cyber security

This chapter explores diversity within the cyber security workforce, covering sex, age, state school backgrounds, ethnicity, disability and neurodiversity.⁶ It includes workforce diversity estimates from the quantitative survey, secondary data covering diversity in the Higher Education recruitment pool, and qualitative findings.

As in the previous studies, survey questions on diversity were only asked of cyber security businesses and not the wider business population. This is because cyber security businesses are the primary recruiters and employers of cyber security-related positions. Chapter 2 highlights that the UK cyber security sector workforce employs an estimated 69,589 people. This represents a substantial share of the broader cyber security talent base, estimated at around 145,900 individuals, which includes both those currently working in cyber security roles, and those in the wider recruitment pool. Moreover, most private sector businesses have employees undertaking cyber security roles informally. Therefore, including these businesses would give an inaccurate view of diversity in the cyber security professional workforce. The qualitative findings do nevertheless include the perspectives of non-cyber security firms, recruitment agents and training providers.

Data from the Annual Population Survey (APS) indicates that in 2025, just 14% of those in full-time SOC 2135 roles were women.⁷ However, as mentioned in the previous chapter, the APS is not an accredited Official Statistic due to declining response rates and sample sizes. While some APS respondents may self-report as cyber security professionals as the sector professionalises, and some individuals in cyber security roles may still be coded under adjacent occupations such as programming or consultancy.

The current picture

The UK cyber security sector workforce continues to display less diversity in terms of sex and disability compared to the wider digital sectors and overall UK workforce. Women make up 16% and disabled staff 9% of the cyber security workforce, maintaining the previous year's patterns. However, the sector shows improved diversity in ethnicity and neurodiversity: neurodiversity has increased to 22% from 9% in a 2020 study, and ethnic minority representation aligns with the wider digital workforce.

As has been the case in previous years, in the qualitative interviews the sector was still regarded as male-dominated, despite efforts to improve diversity. Ethnic diversity was thought to be less of an issue. Participants felt that the sector is increasingly recognising and encouraging neurodiversity. A lack of diversity in the talent pool was again considered the main barrier to diverse recruitment.

What's new since the 2025 report?

New questions for this year showed that cyber security firms had a high level of engagement with diversity or skills initiatives. In the last year, 68% of firms engaged with at least one such initiatives. Almost two-thirds of firms were aware of CyberFirst, whilst just under a third were aware of TechFirst.

⁶ For this study (e.g., in question wording) neurodiversity was defined as the inclusion of people with "conditions or learning disorders, such as autism spectrum disorder (ASD), dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD)".

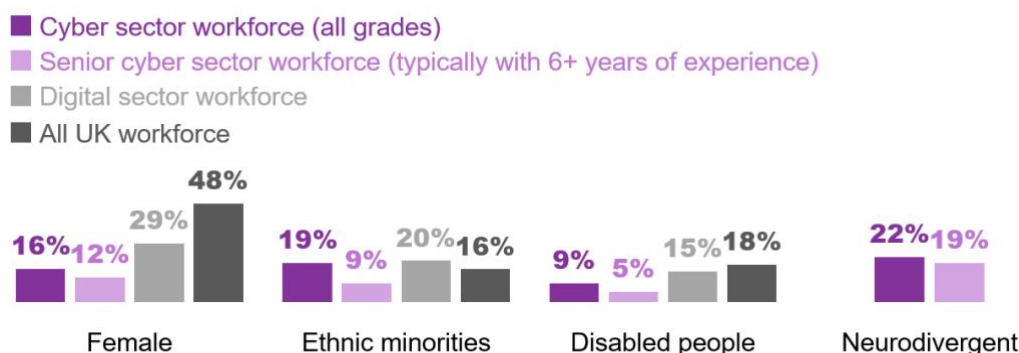
⁷ Office for National Statistics (2025). Annual Population Survey - Occupation (SOC2020) by sex, employment status and full/part-time. [January 2025–December 2025]. Available at: <https://www.nomisweb.co.uk/datasets/aps218/reports/employment-by-status-and-occupation?compare=K02000001>

The qualitative research this year specifically explored diversity at senior levels. Participants felt there was less diversity at senior levels for women and neurodiverse people but hardly mentioned ethnicity. Lack of diversity of women at a senior level was attributed to historical hiring gaps, a reluctance to hire women for senior roles, and perceptions that women undervalue their skills. There was an assumption, held by some participants themselves, that neurodiverse people were not suited to leadership roles.

3.1 Estimates of diversity in the cyber security sector

Figure 3.1 shows that the UK cyber security sector workforce was less diverse than the wider digital sectors and the UK workforce overall in terms of sex and disability. However, the statistics were more in line for ethnicity. The senior workforce – defined as those who have 6 or more years of experience – was less diverse across all groupings. This matched the patterns seen in previous studies.⁸

Figure 3.1: Percentage of the UK cyber security sector workforce estimated to belong to each of the following diversity groups



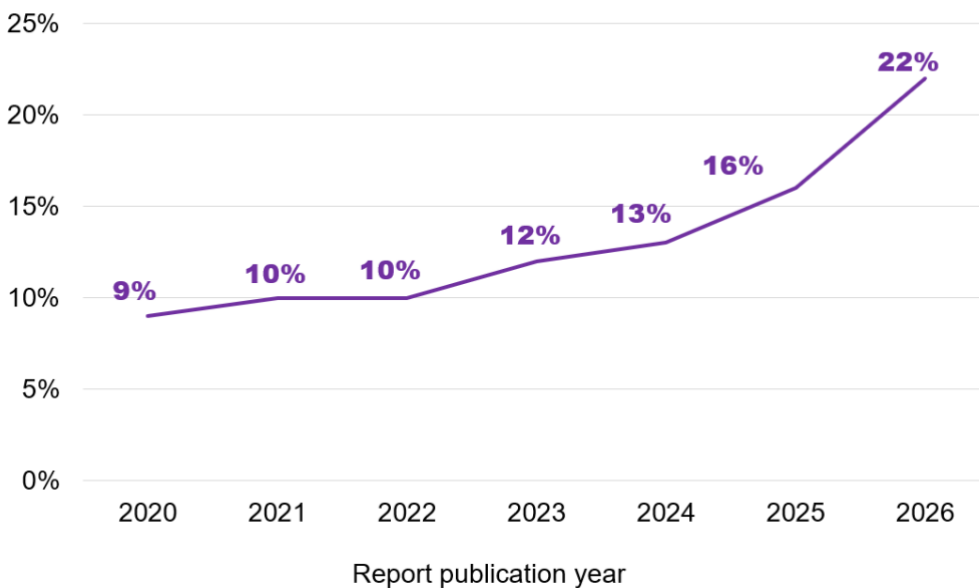
Bases: 204-224 cyber security businesses for whole cyber security sector workforce estimates, 202-218 for senior workforce estimates (in each case excluding those that were not able to answer or refused these questions)

N.B. sex, ethnicity and disability comparison data for the whole UK workforce and digital sectors sourced from DSIT [Economic Estimates](#) (specifically, the January 2024 to December 2024 data). We use 'ethnic minorities' to refer to all ethnic groups except the White British group. Ethnic minorities include White minorities, such as Gypsy, Roma and Irish Traveller groups.

Figure 3.2 shows how the data for the neurodivergent proportion of the whole cyber security sector workforce has changed over time. The data suggest that the proportion of the workforce who are neurodivergent has risen since this measure was first taken, from 9% in the 2020 study to 22% in 2026. It is important to note that this increase could simply reflect an increasing awareness of neurodiversity across employers, leading to greater identification or reporting, rather than a genuine increase in the number of neurodivergent employees.

⁸ These workforce-level estimates are derived from survey responses from cyber security sector employers (i.e., these employers tell us how many of their staff are, for example, neurodivergent). As per the previous studies, these estimates can be very variable, so sudden year-to-year shifts should be treated with caution. Moreover, the results are susceptible to outliers in the data. For instance, in this study's data, there were 2 cyber security businesses that reported having 30 or more employees who were neurodivergent. If these 2 were excluded from the base, the neurodivergent statistic would decrease from 22% to 18%. There were no other notable outliers in the data for this study.

Figure 3.2: Percentage of the whole UK cyber security sector workforce estimated to be neurodivergent



Bases: c.200 cyber security businesses each year

For consistency with previous reports, the x axis refers to the report publication year, which is one year on from the fieldwork year.

Qualitative findings on diversity in the cyber security sector

Qualitative findings on diversity were largely consistent with the previous studies. There was general agreement that the cyber security sector remained male-dominated, despite efforts to improve diversity.

“It’s getting better, we are getting a higher number of female students but we’re still not there yet. We’re not equal.”

Training provider

As also found in the previous studies, ethnic diversity was felt to be less of an issue than sex. However, recruitment agents noted that changes in visa requirements for international candidates could make it harder to recruit more diverse ethnic groups.

“I think I’m probably getting about 40% of people who require some sort of visa sponsorship and clients not knowing if they’re going to be able to support that because of constant changes in regulation.”

Recruitment agent

This study also saw further praise for the neurodiversity of the sector. As was the case in the previous studies, participants shared examples of employers making accommodations for neurodiverse employees such as flexible working hours. However, as discussed in the senior diversity section below, participants identified barriers to neurodiverse employees progressing to senior roles.

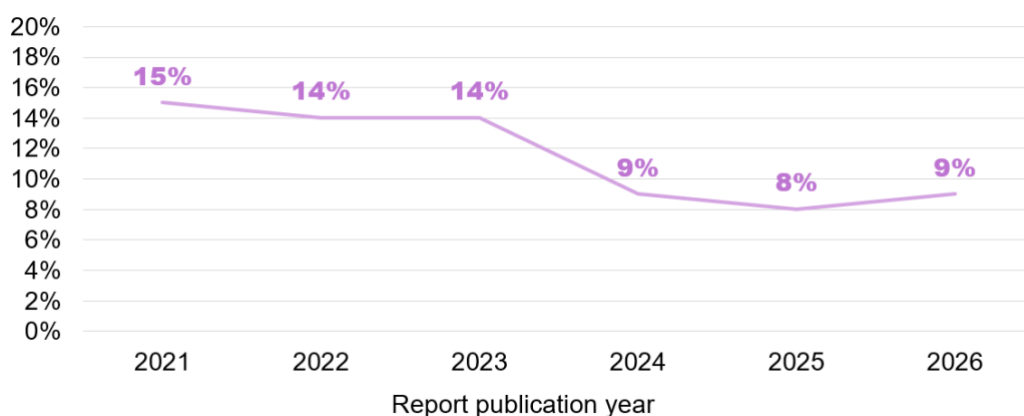
“Cyber security is the most neurodiverse sector I have ever seen, and I think personally it’s celebrated, especially internally within the sector.”

Small cyber security sector business

Senior workforce diversity statistics

Within the senior workforce, the proportion from ethnic minorities remained consistent with the 2024 and 2025 studies, and lower than in the studies from 2021 to 2023, as Figure 3.3 highlights.

Figure 3.3: Percentage of the senior UK cyber security sector workforce estimated to be from ethnic minorities



Bases: c.200 cyber security businesses each year

For consistency with previous reports, the x axis refers to the report publication year, which is one year on from the fieldwork year.

Qualitative findings on senior workforce diversity

The qualitative research for this study specifically explored diversity in the senior workforce. There was a common perception among participants that diversity was lower at more senior levels. This was particularly thought to be the case for sex. There was less discussion of neurodiversity, although neurodiverse people were also thought to be under-represented at senior level. Ethnicity was hardly mentioned and was not generally felt to be an issue, despite the quantitative findings suggesting ethnic diversity at senior levels has remained lower than in the 2021 to 2023 studies.

Barriers to senior workforce diversity

Some employers attributed the lack of male/female diversity at a senior level primarily to a historical shortage of women in the cyber security sector. This was believed to limit the current talent pool. However, the thinking was that as more women had entered the industry at junior level in recent years, the senior workforce would become more diverse in the future.

“It’s certainly less diverse the higher up you go because of the historical [gap]. It takes a while to get up to those roles there.”

Large non-cyber security (private sector) business

Some participants felt that there were other factors at play and these would continue to impede male/female diversity at a senior level. Some argued that employers could be reluctant to hire women into leadership roles because of concerns that they might leave to start a family. Some employers

believed that leadership roles with long hours and high levels of stress would not appeal to women with families.

“When I’ve spoken to a business and said to them ‘why don’t you hire a more diverse workforce?’ You’ll get the normal common ones of ‘well if we hire a female, she’ll get pregnant, she’ll be off for 12 months’, which isn’t right.”

Recruitment agent

Other barriers to career progression raised by participants were assumptions that women did not have technical skills or interests, and perceptions of cyber security as an ‘old boys’ club’. This tied into a broader finding that stereotypes about women not being interested in cyber security continued to persist. A cyber security firm noted that during a career talk on cyber security, a group of girls walked out of the talk, and the careers teacher reinforced the perception that the sector did not appeal to women.

“I went to the careers lady ‘what was the story with the five girls that left?’ And she went ‘oh, cyber security is not really a girl’s job’.”

Small cyber security sector business

Women undervaluing their skills was another barrier identified by participants. Women were thought to be more reluctant than men to put themselves forward for senior roles if they did not have all the skills specified in a job description. A recruitment agent commented that women in senior positions could have lower salary expectations, inadvertently signalling to potential employers that they were less qualified, despite their actual experience.

Turning to neurodiverse people, participants raised one key barrier to progression into senior positions. This was the assumption, held by some participants themselves, that neurodiverse people lacked complementary or “soft” skills, such as communication (see also Section 6.6), and were not suited to certain aspects of leadership.

“They’re more than capable of doing a leadership role. It’s just they might not be soft skilled enough to deal with difficult teams, difficult conversations. But to be honest, I’ve seen some fantastic people who are neurodiverse in leadership roles.”

Small cyber security sector business

Suggested support for improving senior workforce diversity

Participants in the qualitative research were asked what steps, if any, organisations could take to support the progression of diverse groups into senior cyber security roles. Most commonly, participants did not offer any concrete suggestions for enabling the progression of staff from diverse backgrounds into senior cyber security positions. Some employers stated that career development was open to everyone and was based on merit.

“The goal that an individual has to achieve to obtain the next level up of job title and pay grade and benefits are very, very clearly mapped out and they are open. All support, all resources are available to all staff.”

Small cyber security sector business

A few large private sector businesses had company-wide schemes and mentorship programmes to aid the career progression of diverse employees. In addition, one large cyber security employer set quotas

for women in senior cyber security leadership roles and was using head-hunters to find senior female candidates.

“We have a plethora of those things, as most big organisations do. We’ve got future seeds leaders programme, and part of that is a mentoring process, coaching as well. So all of the things are there but you’ve got to show you’re hungry for future development.”

Large non-cyber security (private sector) business

Two other suggestions from participants to enhance diversity in senior roles were recruiting candidates from other tech and business areas and creating targeted developmental pathways for women and minority groups.

3.2 Higher Education student demographic profiles

This section provides the breakdown of students in cyber security and computer science courses for the latest available academic year (2023/24), in terms of sex, ethnicity, age, and entry from state schools. This is taken from HESA and Jisc secondary data on Higher Education. The pipeline of new entrants shows gradual improvement in female participation, particularly at postgraduate level, though male/female disparities remain significant.

- **Female participation** in cyber security courses remained low, with only 14% of undergraduate and 28% of postgraduate students identifying as female. These levels were lower than for computer science courses (21% and 37% respectively). However, the postgraduate cyber security figure showed continued improvement, rising from 21% in 2020/21 to 24% in 2021/22, 27% in 2022/23, and 28% in 2023/24 (i.e., rising 7 percentage points between 2020/21 and 2022/23). These courses continue to attract a lower proportion of female students when compared across all Higher Education student enrolments (56% female student enrolment in 2023/24)⁹.
- **Ethnicity data** showed that at least 18% of all cyber security students and 14% of computer science students were from ethnic minority backgrounds. Asian students represented the largest ethnic minority group (9% for cyber security, 7% for computing). However, a high proportion of students had undisclosed ethnicity (55% for cyber security, 63% for computing), limiting interpretation of these figures.
- **Age diversity** remained strong, particularly in cyber security. Mature students in cyber security (aged 30+) continue to show a strong preference for part-time study, with 41% taking this option compared to lower rates among younger age groups.
- **State school background:** At least 70% of UK-domiciled cyber security students came from state schools, consistent with 72% for computer science students. These figures likely underestimate the true proportions, as students with unknown schooling backgrounds (28% of cyber security students, 24% of computer science students) were most likely to have been state-educated. Only 2% of cyber security students and 4% of computer science students came from privately funded schools.

The full data for this section is provided in Annex B.

⁹ HE Student Data (2026) HESA <https://www.hesa.ac.uk/data-and-analysis/students/whos-in-he#characteristics>

3.3 Engagement with skills and diversity initiatives in the cyber security sector

For this study, new questions were asked about the diversity and skills-development initiatives that cyber security firms had taken part in or offered in the 12 months prior to the survey.

A majority of cyber security firms had engaged with diversity and skills-development initiatives. Almost 7 in 10 (68%) had undertaken at least one of the 8 activities or initiatives asked about in the survey (shown in Figure 3.4). The most common activities or initiatives were delivering talks or workshops in schools or colleges (32%) and offering work placements (30%). Findings also showed that firms offered apprenticeships more than graduate programmes: although 28% of cyber security firms offered apprenticeships, fewer than 1 in 5 cyber security firms offered graduate schemes (17%).

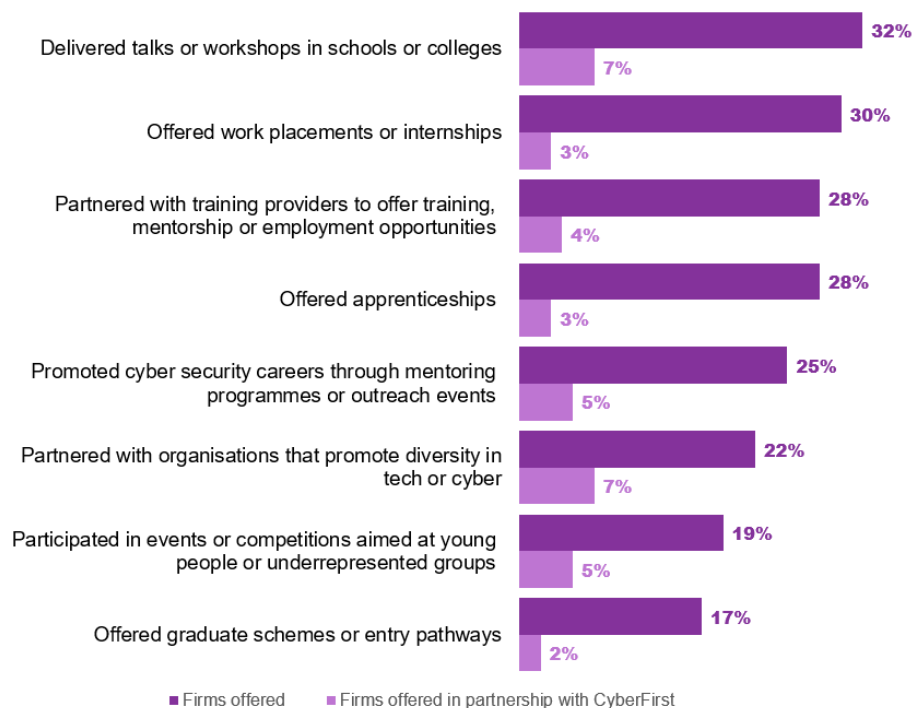
Awareness of and engagement with CyberFirst and TechFirst

For this study cyber security firms were also asked about their awareness of [CyberFirst](#)¹⁰ and [TechFirst](#)¹¹, and whether delivery of initiatives was in collaboration with CyberFirst. Almost two-thirds of cyber security firms were aware of the CyberFirst initiative (64%), while 30% were aware of TechFirst. One third of cyber security businesses (33%) said they were not aware of either of these initiatives.

As Figure 3.4 shows, the most common activities or initiatives done in collaboration with CyberFirst were delivering talks or workshops in schools or colleges (7%) and partnering with organisations that promote diversity in technology and cyber security (7%). Partnering with organisations that promote diversity in technology and cyber security was ranked 6 out of 8 in the activities undertaken overall but ranked 2 out of 8 when collaborating with CyberFirst. This may suggest the key role CyberFirst can play in addressing diversity gaps in the cyber security sector (see Section 3.1).

¹⁰ [CyberFirst](#) is a government-backed outreach and education programme designed to create opportunities for talented young people in future-focused tech careers

¹¹ [TechFirst](#) is the government's flagship tech skills programme opening pathways into the UK's fast-growing tech sector.

Figure 3.4: Initiatives which firms have offered in the last 12 months

Base: 230 cyber security firms, data for 'Firms offered in partnership with CyberFirst' has been rebased to all cyber security firms

Although not covered explicitly in the qualitative research, some training providers spontaneously praised the government's CyberFirst initiative for bringing together educational establishments and industry to attract young people into the sector.

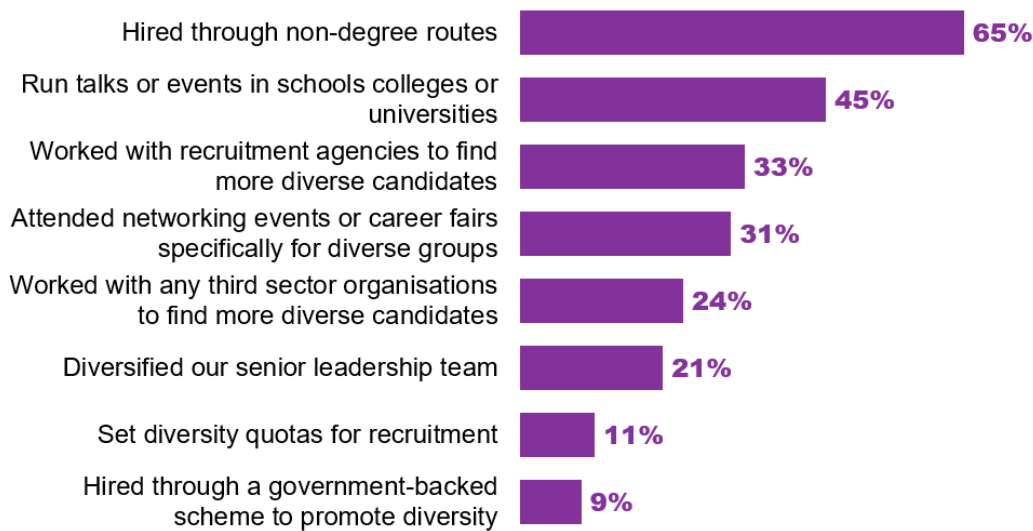
"There's this CyberFirst initiative ... it's aiming to bring together schools, higher education institutions and industry to come together to put [out] programmes to develop skills within the area. And I think it's a perfect example of how it should be done".

Training provider

3.4 Engagement with diversity initiatives in recruitment processes

Cyber security businesses that had been recruiting since the start of 2024 reported a range of measures they had taken to encourage job applications from diverse groups. As Figure 3.5 shows, a majority said they had hired through non-degree routes (65%). Another relatively common action, undertaken by 45% of employers when hiring, involved running events in schools or colleges. This is similar to the actions taken among cyber security firms overall, as seen above in Figure 3.4, where running events in schools or colleges was the most common initiative. Comparatively few businesses had set diversity quotas (11%) or hired through government-backed diversity schemes (9%). These findings are broadly similar to the previous study.

Figure 3.5: Actions taken to encourage job applications from diverse groups in the UK cyber security sector



Base: 118 cyber security businesses that had any job vacancies since January 2024

Qualitative findings on diversity in the recruitment process

As consistently found in this research series, participants in the qualitative research felt that a lack of diversity in the talent pool was the key barrier to diverse recruitment. Employers also did not often have any specific strategies in place to recruit more diverse candidates.

"Our practice is really simple. If you can do the job, you get the job."

Micro cyber security sector business

Where employers were taking steps, requesting diverse shortlists from recruiters was most commonly mentioned. Other strategies were networking events, blind CVs, skills-led interviewing and adapting recruitment processes to accommodate neurodiverse applicants (e.g. not requiring them to do tests).

For this study, mode of working was also explored, with most of the employers who took part in the qualitative research offering the option of remote or hybrid work arrangements.

Some employers commented that remote or hybrid working provides access to a broader and more diverse talent pool. Remote or hybrid employment could also support diverse groups, notably by enabling flexible working hours for employees with caring responsibilities and allowing neurodiverse employees to work in the environment best suited to their needs.

However, for some roles and organisations, remote work was not a possibility, for instance due to the sensitive nature of their client work, or because of on-site infrastructure or client environments that required employees to be on site.

4 Demand for cyber security skills

This chapter explores UK employer demand for cyber security skills. It considers the volume of relevant online job postings, including an assessment of the roles, skills, qualifications, and experience levels in demand, geographic and sectoral demand, and typical levels of advertised remuneration. The data for this report focuses mainly on the 2025 calendar year (January to December 2025). This is based on our analysis of online job vacancy data using the [Lightcast](#) Analyst labour market database, which tracks millions of global job postings.

Some of the analysis across this chapter continues, as in previous waves, to split out **core cyber roles** (where some aspect of cyber security is the main job function) and **cyber-enabled roles** (which require cyber security skills but may not formally be labelled or commonly recognised as cyber security jobs). The charts therefore have separate data for core roles and “all cyber roles” (which sums core and cyber-enabled job postings). Further detail on the definition of core and cyber-enabled roles is set out in Annex C.

The current picture

In 2025 (the latest data covered in this 2026 report), there was an average of 2,911 core cyber security job postings every month, and a further 2,669 in wider cyber job postings. This marks an increase of 7% in core cyber security job postings since 2024, though 2024 levels were considerably lower than previous years. This suggests that demand may have begun to recover modestly from the lows observed in 2024.

In the qualitative interviews, some employers reported receiving a high volume of AI-generated CVs and applications from candidates overclaiming skills. Some felt that unrealistic expectations about salaries could encourage candidates to apply for cyber security jobs they did not have the skills for. Despite the strength of the employment market for cyber security employers, employers said that there continued to be intense competition for strong candidates with the right skillsets.

What's new since the 2025 report?

Cyber security job postings appear to be somewhat stabilising in volume. Demand increased by 7% for core cyber roles and 10% for all cyber roles in 2025, though this may represent market stabilisation rather than a return to the levels of high demand experienced in the early 2020s.

Remote working postings have plateaued. After peaking at 28% in 2022, they have declined to 16% in 2025.

Automation skills continue to grow in demand (rising to 15% in 2025 from 11% in 2024), and there has been a notable increase in job postings requesting AI skills (9% in 2025 up from 4% in 2024).

4.1 Number of job postings

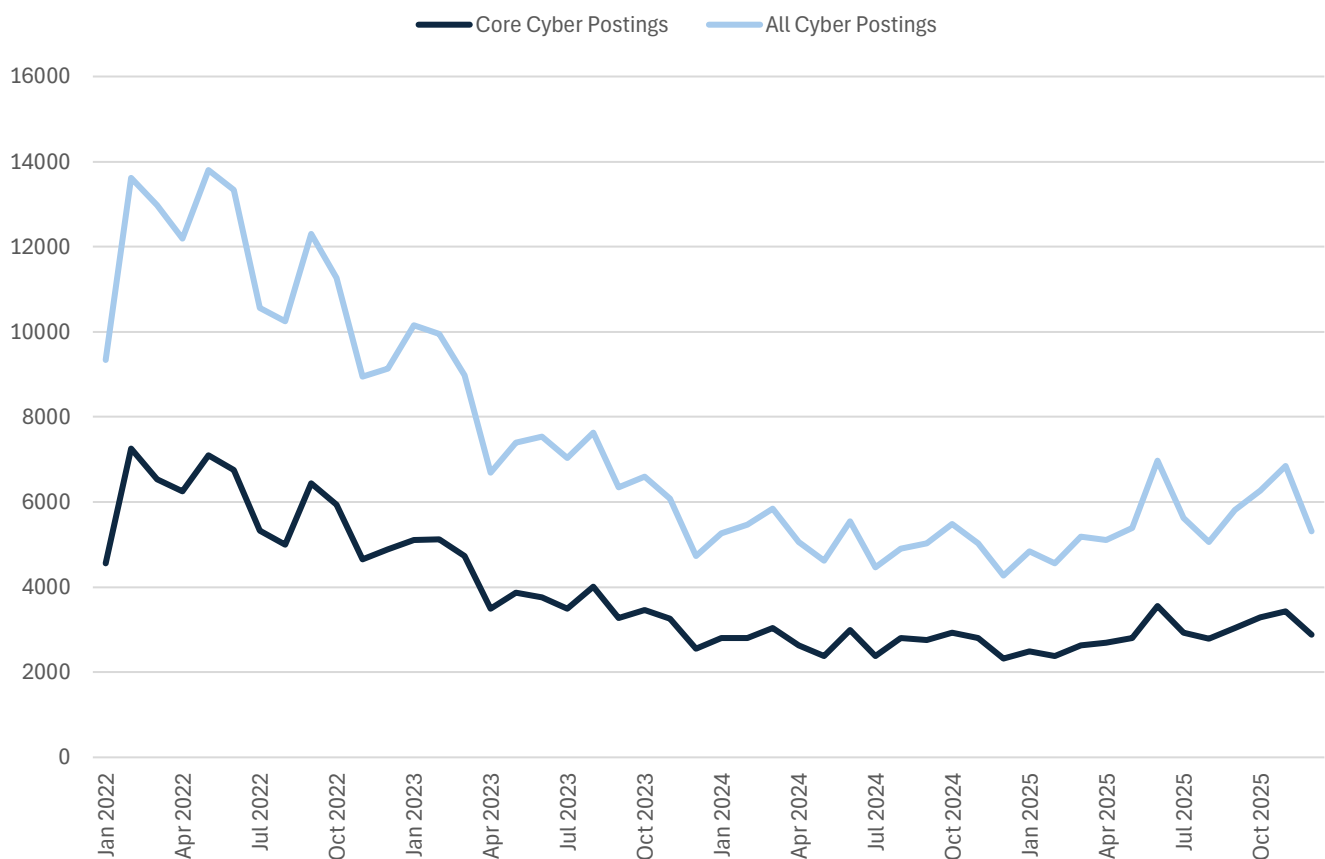
In 2025, there were 66,964 relevant job postings covering all cyber roles. This includes 34,932 job postings across core cyber roles (averaging 2,911 per month) and 32,032 other cyber-enabled job postings requesting cyber security skills (averaging 2,669 per month).

There has been an increase in the number of job postings across core cyber and wider cyber-enabled roles between 2024 and 2025 (see Figure 4.1).

Core cyber job postings have increased by 7% (from 32,671 in 2024), after falling by 33% the previous year (from 48,492 in 2023). Demand for all cyber roles increased by 10% (from 60,992 in 2024), after dropping the previous year by 41%.

Despite this growth, the longer-term trend shows a more challenging labour market. However, signs of demand stabilisation are encouraging compared to previous year-on-year declines. This is consistent with the 2025 ISC2 Cybersecurity Workforce Study, where global cyber security recruitment teams had suggested that recruitment freezes and layoffs may show some signs of stabilisation and levelling in 2025.¹²

Figure 4.1: Monthly number of core and all online cyber job postings in the UK (January 2022 to December 2025)



Source: Lightcast

Bases: 354,786 online job postings across all cyber roles from January 2022 to December 2025 (of which 66,964 were in 2025); 184,434 for core cyber roles (34,932 in 2025)

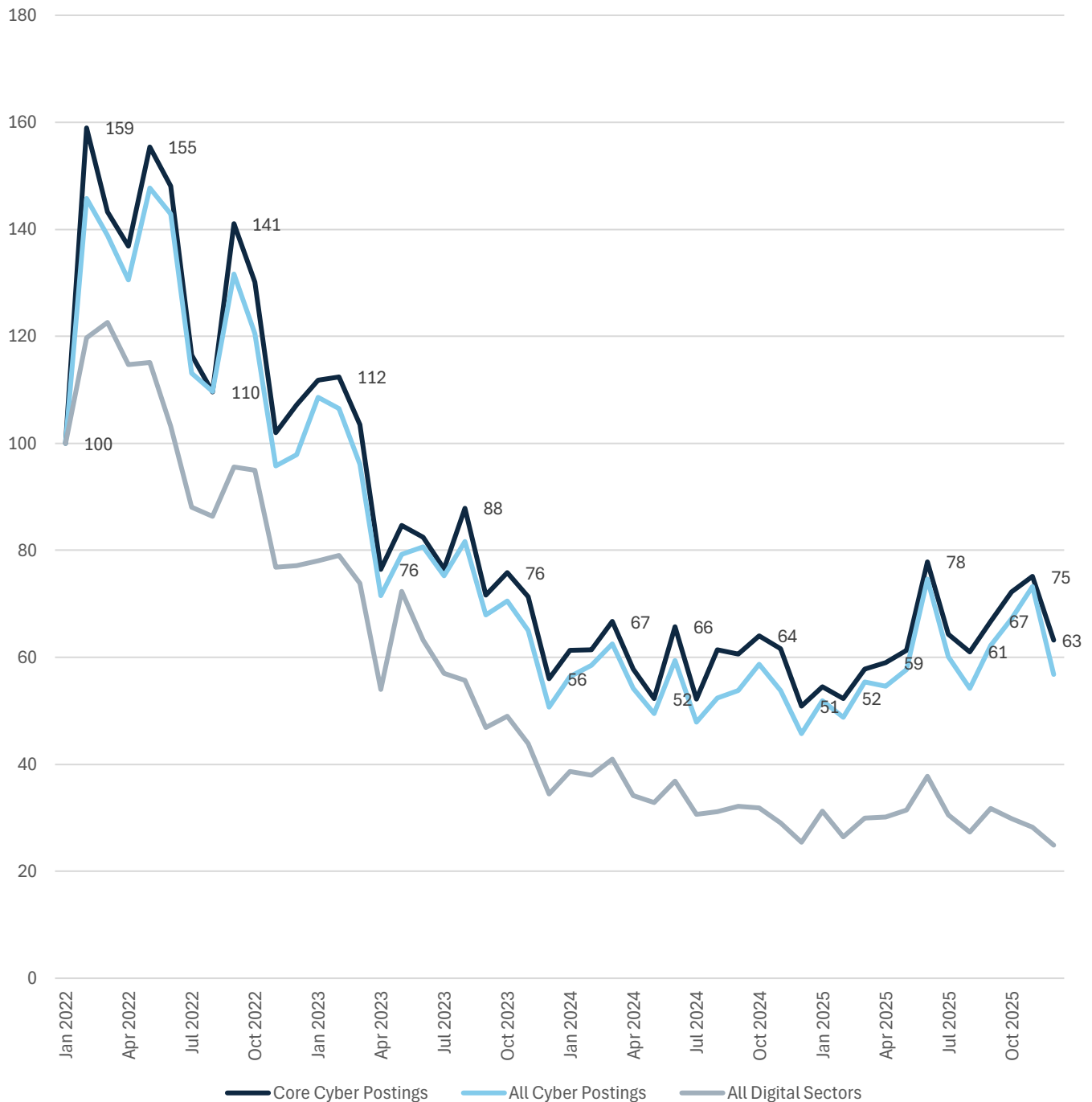
Figure 4.2a sets out how the volume of cyber security job postings has changed since January 2022, compared to job postings across all digital sectors. The job postings for each subsequent month are indexed against January 2022 (i.e., January 2022 postings = 100).

¹² [2025 ISC2 Cybersecurity Workforce Study](#)

Between January 2022 and March 2023, there was particularly strong growth in cyber job postings. However, across cyber security and wider digital roles, levels of demand fell from April 2023 and continued throughout 2024.

In 2025, demand may have levelled out compared to 2024. This suggests either an ongoing softening in demand in cyber security roles amidst a tightening labour market, or a plateauing of cyber security demand.

Figure 4.2a: Index of online cyber job postings in the UK (January 2022 to December 2025, January 2022 = 100)



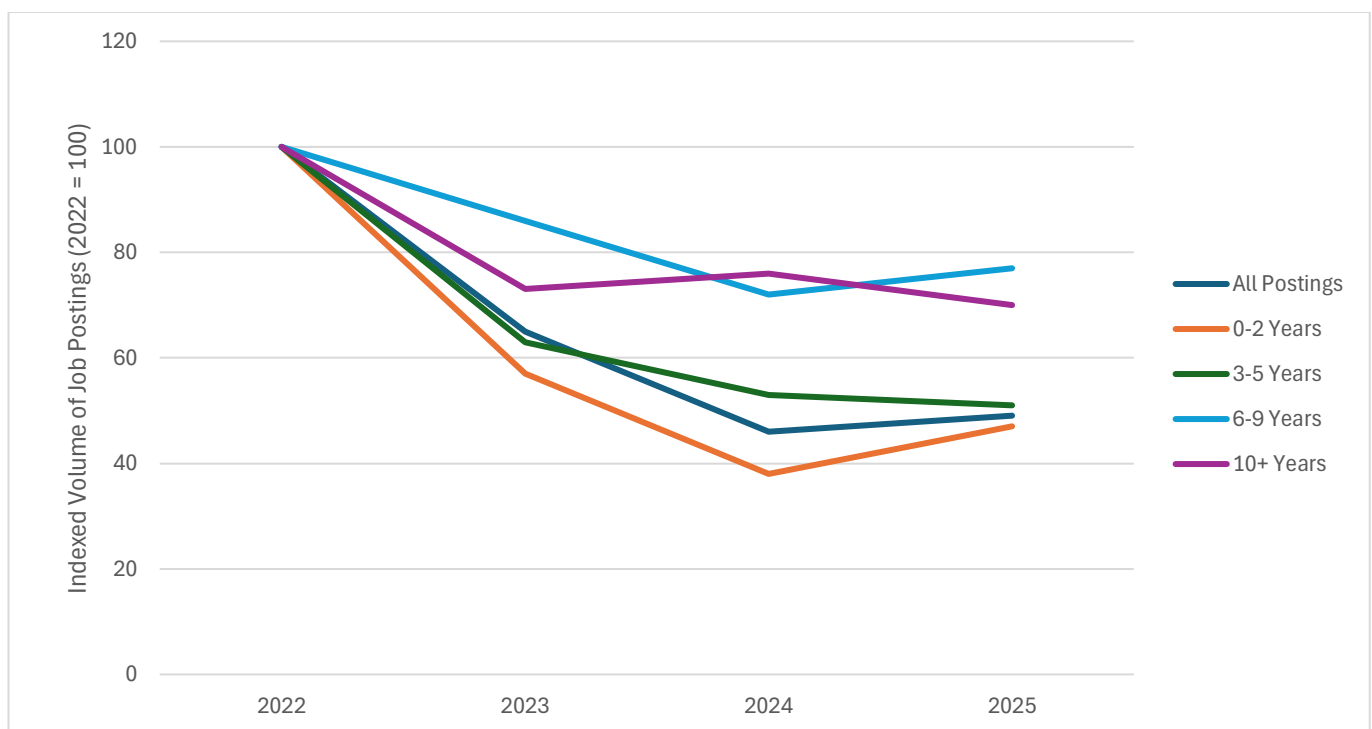
Source: Lightcast

Bases: 354,786 online job postings across all cyber roles from January 2022 to December 2025 (of which 66,964 were in 2025); 3,110,892 across all digital sectors (420,221 in 2025)

Figure 4.2b explores demand for the full years between 2022 and 2025 (indexed to the full year 2022). This highlights that whilst the overall number of core cyber security job postings has fallen by 51% between 2022 and 2025, this is primarily driven by a reduction in entry and early-stage roles (with the volume of roles requesting less than two years' experience falling by 53%, and three to five years' experience by 49%). This compares to a 23% reduction in roles requesting six to nine years' experience, and 30% for those with more than ten years' experience.

It should be noted that over 70% of postings do not contain sufficient text regarding levels of experience requested. Furthermore, some employers may also have changed their routes to securing levels of talent in recent years (e.g., use of external recruitment). As such, this data is considered indicative of wider labour market trends, but further interpretation may be required to explore the extent of opportunities and demand across experience levels.

Figure 4.2b: Index of core cyber job postings in the UK by minimum experience required (2022 to 2025, 2022 = 100)



Source: Lightcast

Bases: 184,432 online job postings across all cyber roles from January 2022 to December 2025, of which 53,023 roles included a requested minimum level of experience.

4.2 Geographical differences

The remainder of this chapter focuses on only the 34,932 core cyber job postings from January to December 2025.

Figure 4.3 shows the proportion of these job postings from each UK region (where region has been provided in the job listing) for 2025. On the heatmap, a darker colour indicates a higher density of cyber jobs in that region.

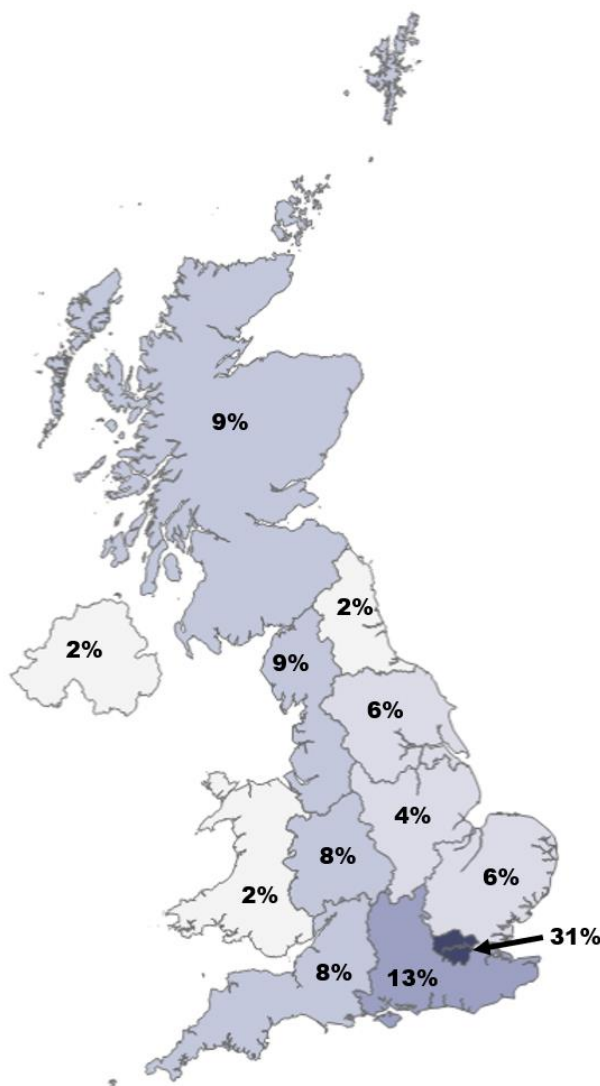
In line with last year's report, the highest concentration of job posts fell within Greater London and the South East. While the proportion of roles within Scotland appears to have risen slightly (7% in 2024 to 9% in 2025), the regional spread of core cyber job postings across the UK remains relatively consistent.

Notably, 16% of job postings had no regional location listed, i.e., the roles are assumed to be remote or UK-wide. This represents a substantial decline from 2024 (26%) and suggests a reversal of prior trends, suggesting that remote working offerings have now plateaued or begun to decline. Remote job postings had risen between 2020 and 2022, peaking at 28%, and this continued through 2023 and 2024 with remote job postings remaining over 20%.

Figure 4.3: Percentage of core cyber job postings from each UK region (where location is known, January to December 2025)

Ranking

1. Greater London (31%)
2. South East (13%)
3. North West (9%)
4. Scotland (9%)
5. South West (8%)
6. West Midlands (8%)
7. East of England (6%)
8. Yorkshire and the Humber (6%)
9. East Midlands (4%)
10. Wales (2%)
11. North East (2%)
12. Northern Ireland (2%)



Source: Lightcast

Base: 29,411 online job postings with location data from January to December 2025

Figure 4.4 sets out the UK Local Authorities with the highest number of job postings, alongside the top 15 Local Authorities in terms of Location Quotient rankings. Location Quotients measure how concentrated labour market demand is in a local labour market relative to its concentration nationally. The average demand is set at 1.0. A Location Quotient of 1.2, for example, indicates that the demand for core cyber security employees is 20% higher than the UK average.

Greater London, Manchester, Birmingham and Bristol have consistently held the top four positions for job postings since 2021, while Edinburgh has replaced Leeds in fifth place in 2025. In terms of Location Quotient rankings, Reading continues as a leading location for cyber security job postings (since 2023), while some of the wider highest demand areas (relative to local labour market size) include Cheltenham, Rushmoor, Bristol, and Manchester. In 2025, there also continues to be strong relative demand for cyber talent in areas such as Cambridge, Southampton, Gloucester, Basingstoke, and Edinburgh.

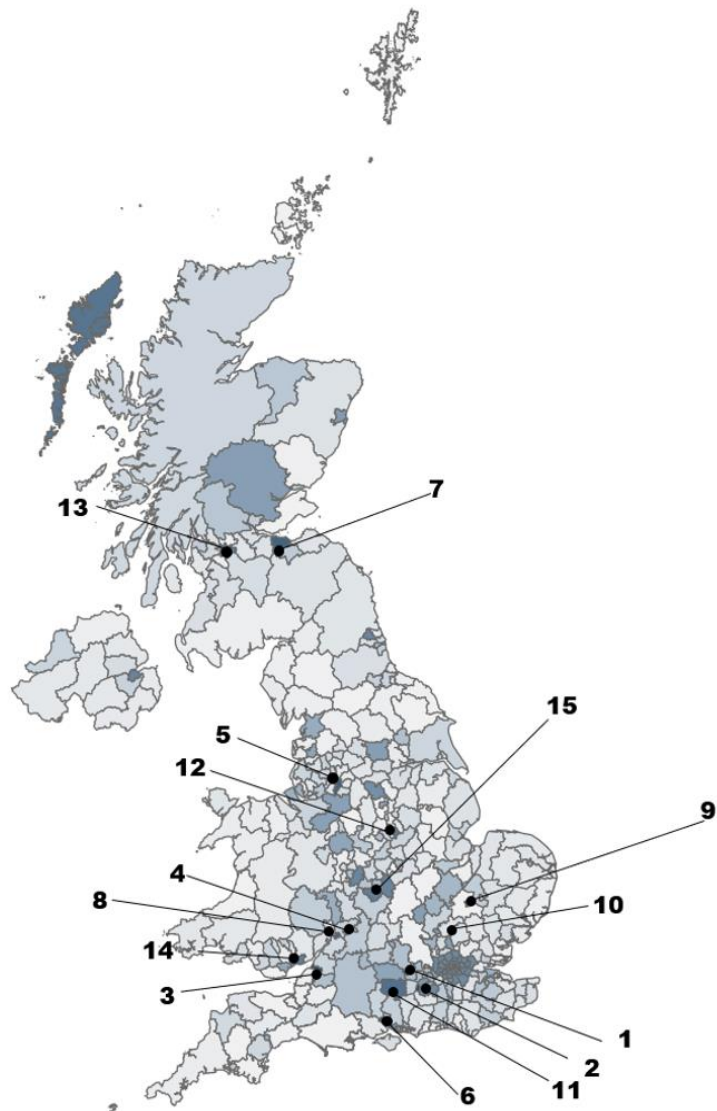
Figure 4.4: Top 15 UK Local Authorities by number of core cyber job postings and Location Quotients (January to December 2025)

Top 15 in terms of absolute number of job postings (number in brackets)

- i. Greater London (9,262)
- ii. Manchester (1,079)
- iii. Birmingham (930)
- iv. Bristol (886)
- v. Edinburgh (845)
- vi. Glasgow (804)
- vii. Leeds (621)
- viii. Reading (413)
- ix. Belfast (406)
- x. Nottingham (397)
- xi. Sheffield (395)
- xii. Newcastle upon Tyne (326)
- xiii. Liverpool (272)
- xiv. Southampton (269)
- xv. Cambridge (265)

Top 15 in terms of Location Quotient (shown in brackets) with ranking labelled on map

1. Reading (4.71)
2. Rushmoor (4.17)
3. Bristol (3.89)
4. Cheltenham (3.43)
5. Manchester (3.27)
6. Southampton (3.24)
7. Edinburgh (3.14)
8. Gloucester (3.06)
9. Cambridge (3.05)
10. Stevenage (2.84)
11. Basingstoke and Deane (2.76)
12. Nottingham (2.55)
13. Glasgow (2.49)
14. Newport (2.48)
15. Warwick (2.45)



Source: Lightcast

Base: 27,788 online job postings for core cyber roles with local authority location data from January to December 2025

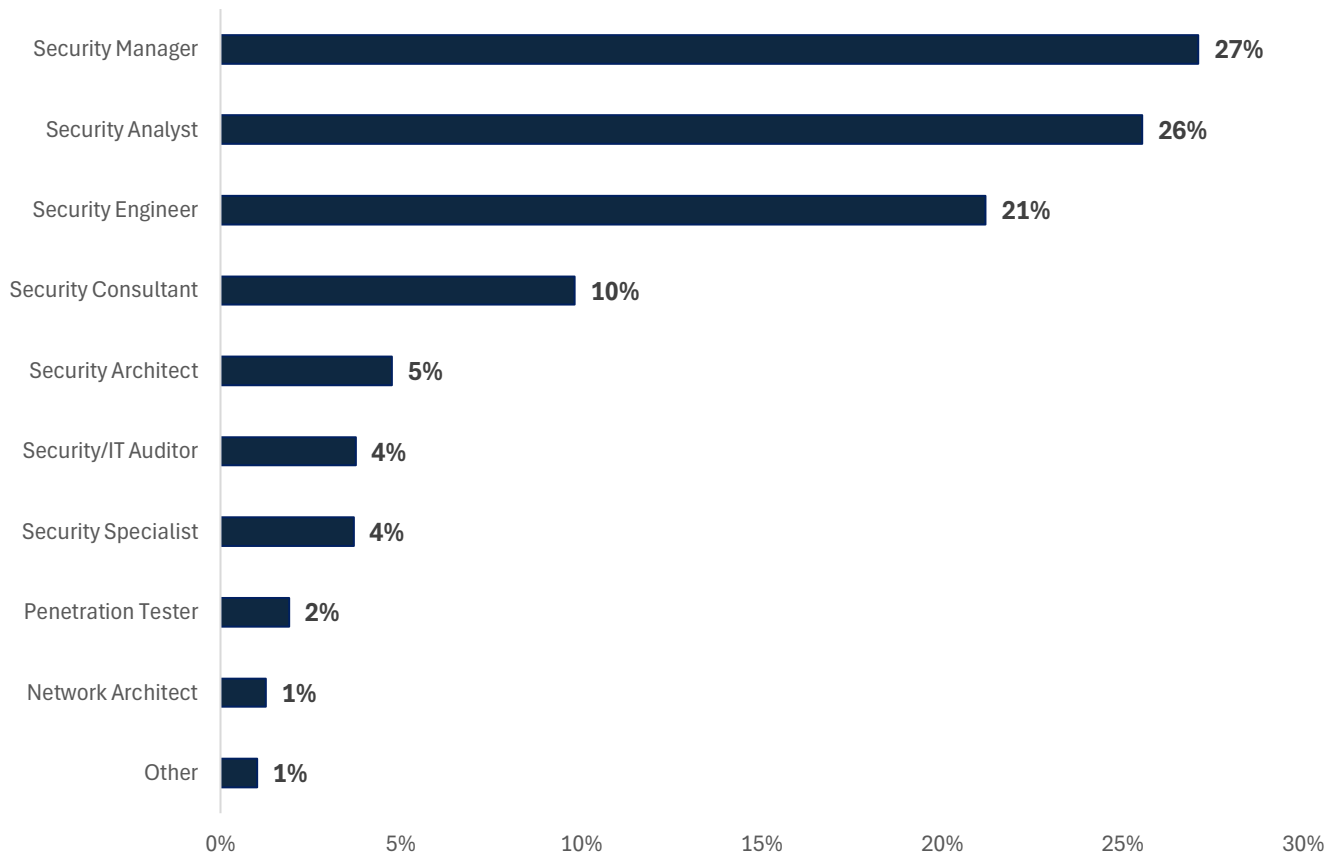
4.3 The job roles being advertised

Figure 4.5 lists the identified core cyber roles by job title.¹³ The most demanded roles have remained consistent since 2022, with some changes in the specific proportions each year. Demand for Security Analyst and Security Engineer roles have maintained a steady level of demand since 2024 (28% and 26% in 2024 respectively). Security Consultants have also increased in relative terms (from 8% in 2024 to 10% in 2025).

¹³ The top 50 job titles appearing in the data have been categorised. This covers 11,784 of the total 32,370 core cyber job postings for the latest calendar year. It means some of the very specific variants (e.g., "Security Manager – Banking") may have been missed. However, a manual review of the Lightcast platform suggests that the top 50 job titles are representative of the wider dataset.

There has been an increase in demand for Security Managers (from 22% in 2024 to 27% in 2025), perhaps indicative demand for roles within managed services, advisory activity, and security leads across firms. These roles are often prominent in consultancies, professional services companies, financial institutions, and government organisations.

Figure 4.5: Top recurring job titles among the UK core cyber job roles identified (January to December 2025)



Source: Lightcast

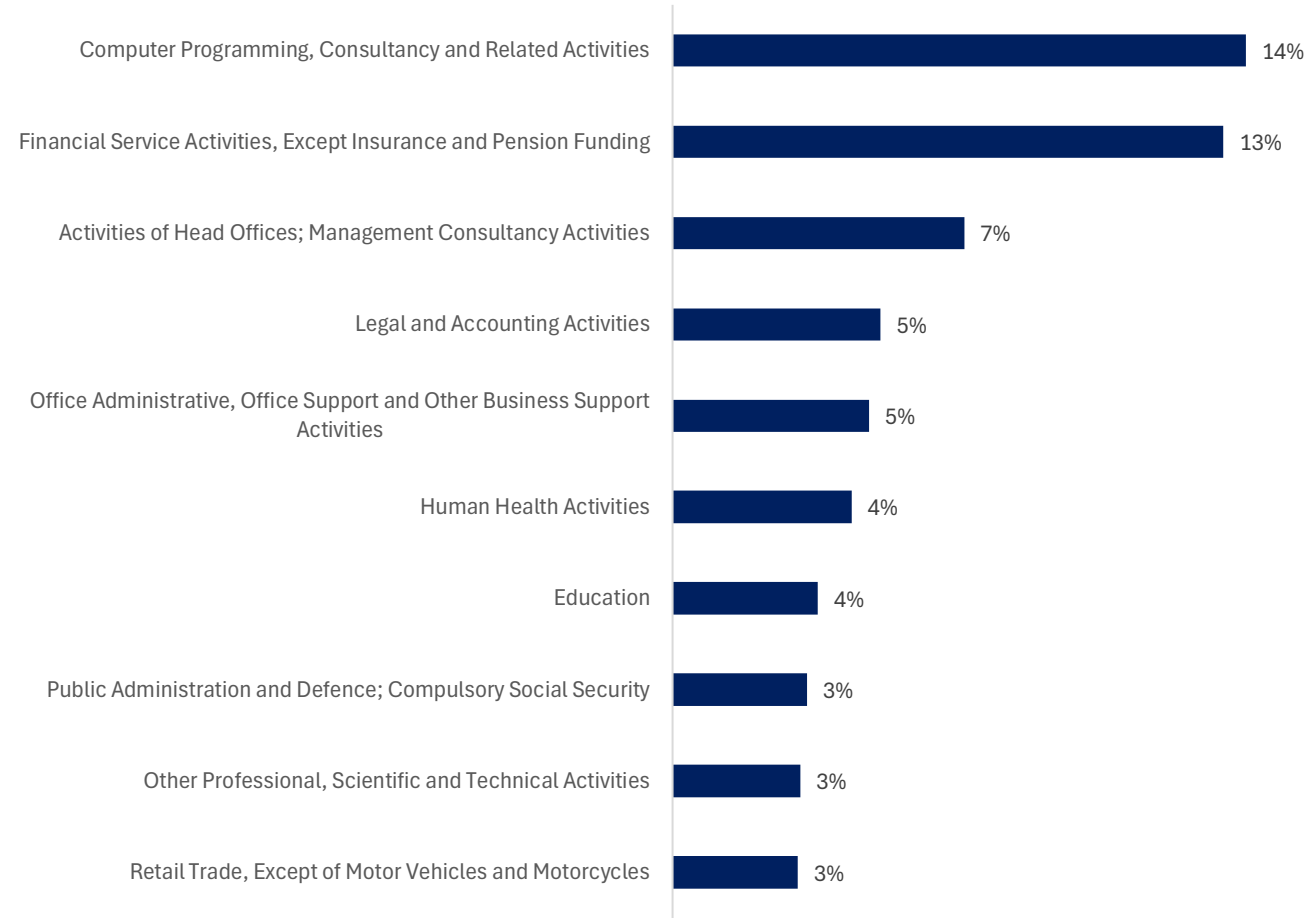
Base: 11,980 online job postings for core cyber roles with job titles from January to December 2025 (Note: The top 50 job titles appearing in the data have been categorised. See footnote in previous text for further information.)

4.4 Sectoral demand for cyber roles

The following explores the sectors advertising for core cyber roles in 2025. The proportion of job postings that were advertised through a recruitment agency appears to have continued to decline, from 42% in 2023, 33% in 2024, to 26% in 2025. For the remaining 20,406 core cyber roles (excluding the 26% advertised through a recruitment agency), Figure 4.6 sets out the sectoral breakdown of demand.

As with previous years, key employers included organisations such as the NHS, BAE Systems and ARM. In 2025, there was also high demand for cyber roles from government departments and the Ministry of Defence. Several multinationals also continue to have significant demand for core cyber roles in the UK (e.g., Unilever, Amazon, Microsoft) alongside professional services and finance firms (e.g., Virgin Money, JP Morgan Chase, Deloitte, Barclays), and telecommunications (e.g., BT, Vodafone).

Figure 4.6: Percentage of UK job adverts for core cyber roles attributed to a specific Standard Industry Classification (SIC) 2007 code (where the employer is named, January to December 2025)



Source: Lightcast
Base: 20,406 core cyber job postings for core cyber roles with sector data from January to December 2025 (excluding recruitment agency postings) ¹⁴
N.B. human health activities typically refer to the health and social care sector – the NHS is the largest employer of cyber security roles within this sector.

4.5 The skills, experience and qualifications being demanded

Specific skills mentioned in job postings

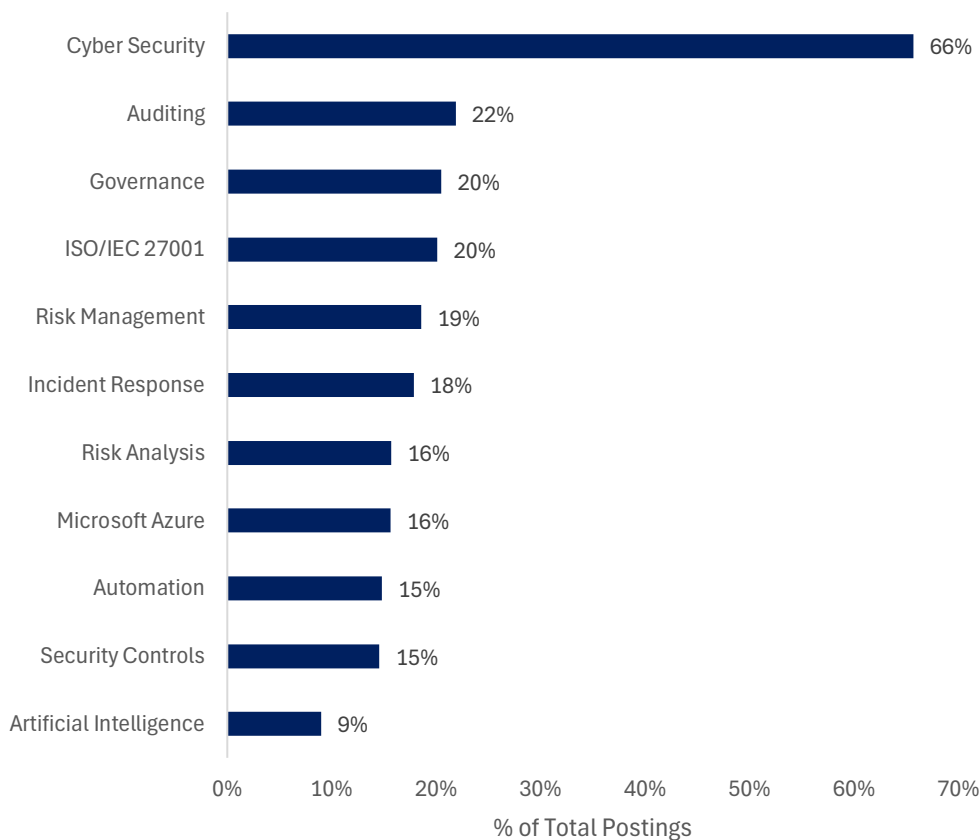
Figure 4.7 sets out the top skills that employers of core cyber roles sought in 2025. The top technical skills mentioned include ‘cyber security skills’ (a classification group within the Lightcast platform), in addition to auditing and governance.

14 As in previous years, this is not necessarily a comprehensive breakdown. The Lightcast dataset may omit some key large employers that do not post job adverts on recruitment sites online and instead use alternative avenues (e.g., directly recruiting through their own website). Consequently, the following explores the top sectors for core cyber postings, excluding direct employer-led recruitment activity.

Other sought-after skills areas include risk management, risk analysis, Microsoft Azure, incident response and automation. Automation skills continue the year-on-year trend of growth, rising from 9% in 2023 to 11% in 2024, and increasing further to 15% of postings in 2025.

The specialised skills showing the greatest demand growth in core cyber postings are governance, automation, continuous improvement processes and artificial intelligence, all of which are closely related to the growth of AI and its role in cyber security. AI skills were also directly requested in 9% of job postings (3,153 out of 34,932). This is an increase from 4% in the previous study, suggesting proportional demand for these skills has more than doubled in the previous year. This growth also aligns with the ongoing growth within the AI security market, as set out within DSIT's [Cyber Security Sectoral Analysis 2026](#). The Sectoral report shows the number of cyber security professionals employed in firms offering AI security has increased by 51% from 9,740 employees across 66 firms¹⁵ to 14,718 staff across 111 firms.¹⁶

Figure 4.7: Top skills requested for UK core cyber job roles (January to December 2025)



Source: Lightcast

Base: 34,932 online job postings for core cyber roles from January to December 2025

¹⁵ DSIT (2025) AI and software cyber security market analysis. <https://www.gov.uk/government/publications/ai-and-software-cyber-security-market-analysis>

¹⁶ DSIT (2026) Cyber Security Sectoral Analysis. <https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2026>

Experience and qualifications requirements

In line with all previous years of this analysis, the most common request from employers was for applicants with mid-level experience of between 2 and 6 years (accounting for 64% of core cyber job postings in 2025).

Similarly, demand for entry-level applicants with under 1 year of experience remained low in 2025 (16%), decreasing over the last 3 waves (from 25% in 2022 to 17% in 2024). This continues the trend highlighted in Figure 4.2b, with demand for entry and early-stage roles now at half the 2022 level.

A total of 77% of employers required applicants to have a minimum of a bachelor's degree (or equivalent), for a core cyber role, with a further 10% wanting postgraduate qualifications such as a master's degree or PhD. This is in line with the previous study, with 12% of roles open to applicants with GCSE, A-Level or Foundational level education.

The full data on experience and qualifications has been included in Annex D.

Perceptions around hard-to-fill vacancies were explored in the qualitative research. Consistent with the previous studies, recruitment agents and employers noted continuing demand for specialist technical skills such as penetration testing and secure software development. Recruitment agents reported more interest in incident response roles, which was attributed to recent high-profile breaches and increasing threat levels. Candidates who combined both technical and complementary skills remained highly sought after.

“To get someone that is technically skilled but also can manage people is virtually impossible.”

Large cyber security sector business

Some recruitment agents noted an increase in demand for AI-related skills, notably around defence, governance and security engineering and architecture. As discussed in Section 6.5, participants predicted that the need for these skills would further increase in the future.

In general though, falling demand for cyber security professionals had led to increasing competition for jobs. Some employers reported that they were inundated with applications for cyber security roles.

“We don't even advertise anymore because we put an advert on LinkedIn, I think we had 1,300 CVs in the first week.”

Micro cyber security sector business

Some employers found that a high volume of candidates lacked the required skills and experience for the advertised role. This could be apparent from the application itself but in some cases, it was because candidates were overclaiming in their application what skills they have.

“Lots of people turn up for interview and claim they can do the stuff and then they fail the technicals.”

Large non-cyber security (private sector) business

Some participants felt that unrealistic expectations about salaries were a factor in encouraging candidates to apply for cyber security jobs they did not have the skills for. As discussed in Section 5.4, this was thought to be a particular issue for entry-level roles.

Some employers commented on the growing use of AI in job applications and CVs. This was increasing the burden of recruitment by making it easier for people to apply but harder for employers to assess candidates.

“The big thing that we're finding is just in the last few months is CVs that look like they've been written by AI. We're seeing CVs that come in that we don't really trust and are fairly sure it's AI.”

Small cyber security sector business

The challenges posed by higher volumes of applications could potentially result in employers relying more on informal networks and referrals for recruitment. This might then negatively impact the diversity of the sector, particularly at senior level.

Despite a strong employment market for cyber security employers, it could still be challenging to find the right person for the job. There continued to be intense competition among employers for strong candidates with the right skillsets. A couple of employers had lost people just as they were about to start their jobs because another employer had made them a better offer.

In addition, and as was the case in the previous studies when demand for cyber security professionals was higher, some employers were still struggling to match the market rate for cyber security salaries.

“It's really difficult because we're in construction, we're not noted for paying a huge wage. We can't pay more than we pay the rest of the IT staff.”

Large non-cyber security (private sector) business

4.6 Salaries

UK-wide salary data

In 2025, the mean advertised salary was £60,800 for a core cyber job posting, with a median value of £58,050. This suggests a nominal increase in both the mean and median salaries for core cyber roles since 2024 (up 3% from £58,800, and 6% from £55,000 respectively).

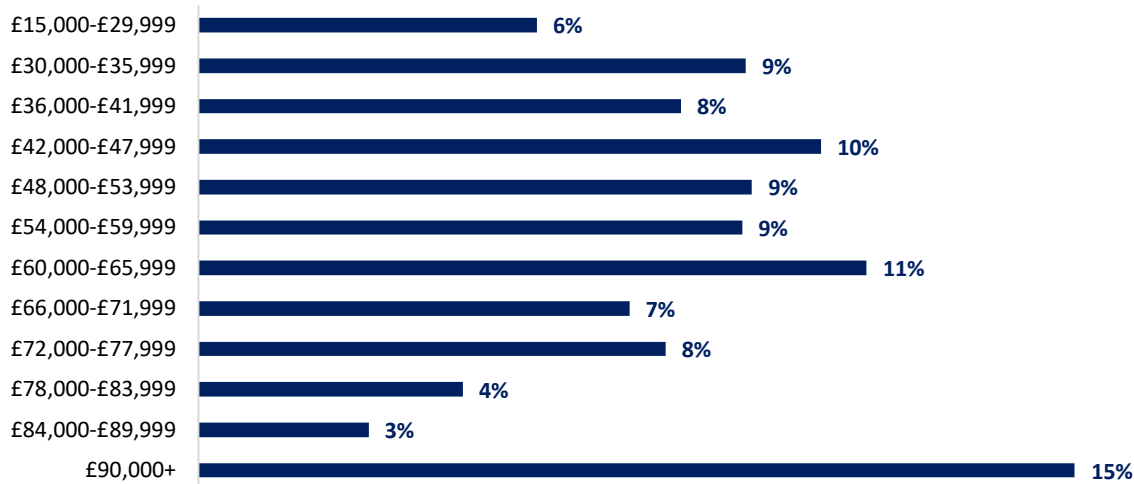
Comparison with official external data on salaries, from the 2025 Provisional ONS Annual Survey of Hours and Earnings (ASHE) for FTEs within SIC 2007 code 62 (“computer programming, consultancy and related activities industry”)¹⁷ suggests these increases mirror broader sectoral changes. This data shows that the mean annual pay increased from £57,600 in 2024 to £68,100 in 2025 (+12%). The median also increased from £48,900 in 2024 to £55,000 in 2025 (+7%).

Expanding the comparison to the broader IT sector (SIC Section J), ASHE data serves as a proxy for overall IT job salaries in the UK. Based on median salaries, this suggests that there is a wage premium of approximately 11% for core cyber jobs (£58,050) compared to IT jobs (£52,260), a level that has remained relatively steady since 2024 (when it was 12%). As highlighted in the previous study, this wage premium has continued to decline from a figure of 25% in 2023 and 33% in 2022, possibly reflecting the pay increases experienced by the wider IT sector over these years.

¹⁷ See the 2025 Provisional ONS [Annual Survey of Hours and Earnings](#), or ASHE.

Figure 4.8 sets out the percentage of core cyber roles offering salaries within each of the salary ranges, where the salary was advertised. It is also worth noting that 76% of online core cyber job postings in 2025 did not contain any salary information. This has increased steadily from 70% in 2023 and 75% in 2024 suggesting a continued decline in salary transparency.

Figure 4.8: Percentage of UK core cyber job postings offering the following salaries (where a salary or salary range is advertised, January to December 2025)



Source: Lightcast

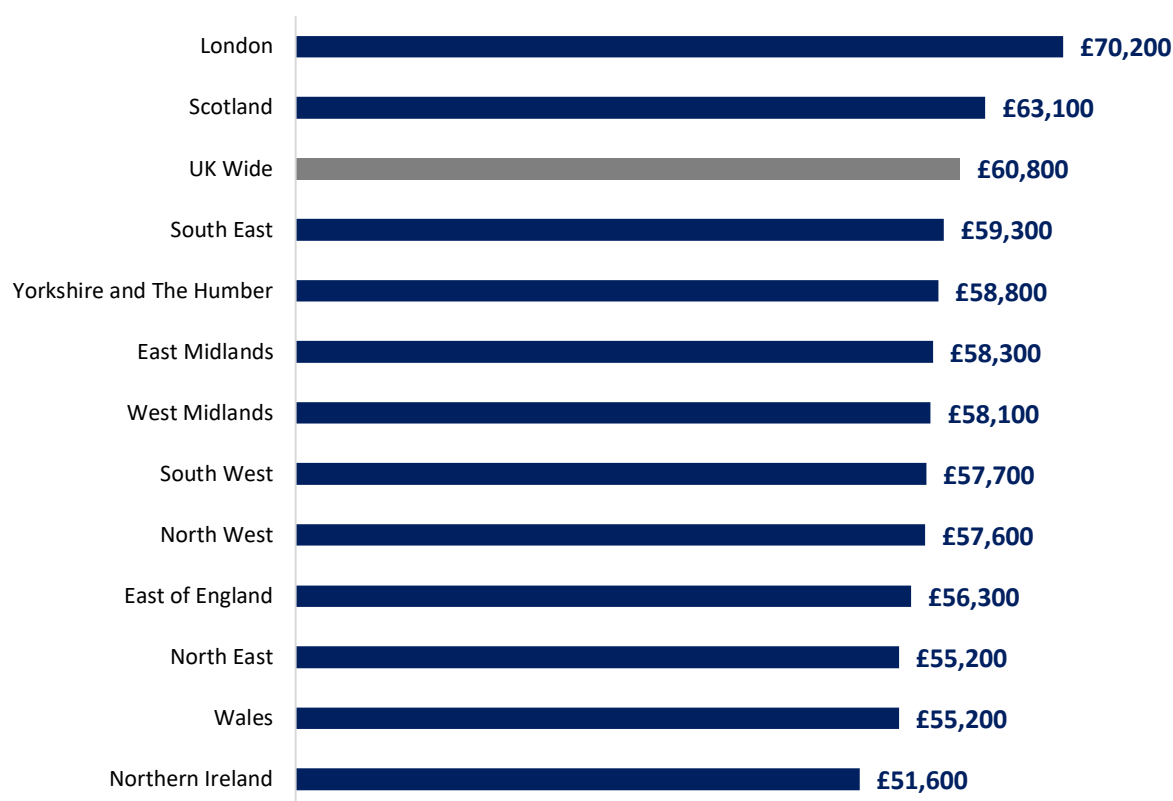
Base: 8,481 online job postings for core cyber roles with advertised salaries from January to December 2025 (24% of all online job postings for these roles)

Regional variations in salaries

Regional salary trends in job postings revealed persistent regional disparities across the UK. London continued to offer the highest mean salary (£70,200) for core cyber roles, as illustrated in Figure 4.9.

However, the regional pay landscape is continuing to change. The gap between regional salaries on core cyber job postings has been steadily narrowing in recent years. In 2021, the difference between the highest and lowest paying regions stood at £23,200. This gap has consistently decreased, falling to £17,100 in 2024, but it has risen slightly to £18,600 in 2025. The difference between the UK average (mean) advertised salary and the lowest-paying region has also increased slightly since 2024, standing at £9,200 in 2025, which represents an increase from the previous year.

Figure 4.9: Mean salary offers for UK core cyber job postings, by region (where the salary or salary range is advertised, January to December 2025)



Source: Lightcast

Base: 8,481 online job postings for core cyber roles with salary data that can be mapped to a specific UK region from January to December 2025 (the remainder are based in the UK, but do not mention a region, and may be likely to offer a remote working option)

5 Supply of skills

This chapter looks at the skills pipeline – those entering the cyber security labour market. The analysis is based on secondary data covering Higher Education pathways, apprenticeship programmes, and professional retraining and upskilling initiatives. The data from this chapter maps back to our estimate of inflows into the labour market in 2025 (the most recent calendar year) in Chapter 2, which forms part of the overall workforce size calculation reported in that chapter.

This is followed by qualitative insights on the effectiveness of entry-level pathways.

The current picture

There were 24,770 total enrolments in cyber security courses in UK Higher Education Institutions (HEIs) in the 2023/24 academic year, and 7,950 cyber security graduates (at both the undergraduate and postgraduate levels).

In the qualitative research, participants continued to be concerned about the impact of AI and automation on the development of the talent pipeline. Employers felt that as demand for entry-level employees was falling, the pathway to becoming an experienced cyber security professional was narrowing. Participants wanted evidence of stronger partnerships between employers, educational institutions and government to support entry-level pathways.

What's new since the 2025 report?

There has been approximately 14% growth in the number of cyber security graduates between 2022/23 and 2023/24 (to 7,950), on the back of 20% growth in the previous year. However, the pattern of growth has shifted when compared with the previous year. Postgraduate growth has been more moderate compared to the previous year's surge (enrolments increasing by 2%, and number of graduates increasing by 17%) while undergraduate provision has increased (enrolments increasing by 13%, and number of graduates by 10%).

5.1 Higher Education data

This section focuses on the latest published data on graduate enrolments from the HESA and Jisc, and graduate outcomes from the HESA Graduate Outcomes survey. The most recent higher education courses and enrolments data available is for the 2023/24 academic year. Later subsections here focus on graduate outcomes, where the latest data (Graduate Outcomes Survey 2023/24) covers graduates from the 2022/23 academic year, around 15 months since they graduated.

Enrolments and Graduates

In the 2023/24 academic year, enrolments and graduations in cyber security and computer science courses provided by UK HEIs have continued to grow year on year, responding to market demand.

- There were 88 universities providing cyber security undergraduate courses, and 95 universities providing cyber security postgraduate courses in the UK. This is a small increase from 82 and 91 universities respectively in last year's report.
- The number of universities providing computer science courses has also moderately increased, from 140 universities offering undergraduate places in 2022/23, to 151 in 2023/24.

- Student enrolment in cyber security courses grew by 9% between 2022/23 and 2023/24 (to 24,770), while computer science enrolment increased by 4% (to 173,990). The rate of annual growth of the number of students enrolled in cyber security courses remained level but dropped slightly for computer science courses (6% growth in previous year).
- The number of graduates also increased during this period, with cyber security rising by approximately 14% (to 7,950), and computer science showing an 18% rise (to 63,510).
- Increased course capacity in recent years has driven growth in cyber security graduate numbers. Postgraduate enrolments grew substantially in 2022/23 (+21%) before levelling off in 2023/24 (+2%), while postgraduate completions continued to rise (+17%) as earlier cohorts graduated. Undergraduate provision has expanded with enrolments up 13% and graduations up 10% in 2023/24.

The full data for this section is provided in Annex E.

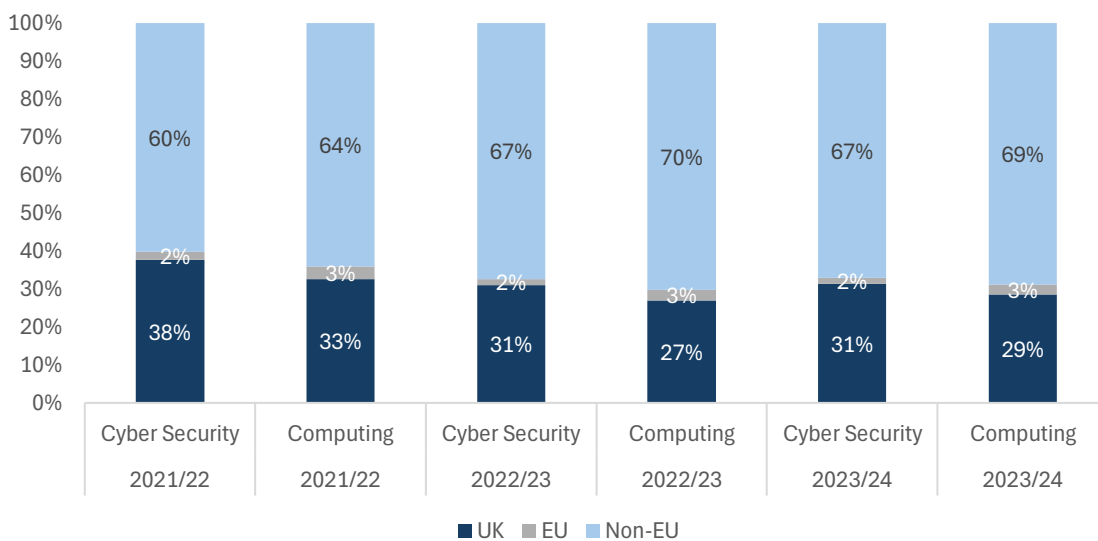
Domicile and domestic skills retention

In 2023/24, UK students comprised 87% of those enrolled in undergraduate cyber security programmes, a figure that has remained relatively steady over recent years reflecting an important inflow into the UK cyber security workforce or further study among graduates.

The postgraduate population shows a distinctly different composition of student domicile, with international students making up the vast majority of enrolled postgraduates. As Figure 5.1 shows, the proportion of UK students enrolled in postgraduate cyber security and computer science programmes has remained stable at around 31% and 29% respectively. As highlighted in Figure 5.1, less than a third of postgraduate students in these subject areas are from the UK, while over two thirds are from non-EU countries.

The proportion of cyber security postgraduate students from non-EU countries has been continually risen in recent years. The previous report documented growth from 29% in 2018/19 to 67% in 2022/23 (an increase of 38 percentage points). As displayed in Figure 5.1, this proportion appears to have levelled off, remaining at 67% in 2023/24.

Figure 5.1: Domicile of cyber security and computer science enrolled postgraduate students (2021/22-2023/24 academic years)



Source: HESA/Jisc data (2021/22-2023/24) Bases (for 2023/24): 8,280 cyber security postgraduate students, 59,200 computer science postgraduate students

This demonstrates the continued international appeal of the UK's higher education sector in these fields. However, it raises ongoing questions about the domestic skills pipeline, particularly as many international students may return to their home countries after graduation due to visa requirements or career opportunities abroad. This will be important to monitor in coming years. It is also worth recognising that attracting international students to postgraduate programmes brings significant benefits and contributes to the UK's research and innovation capabilities.

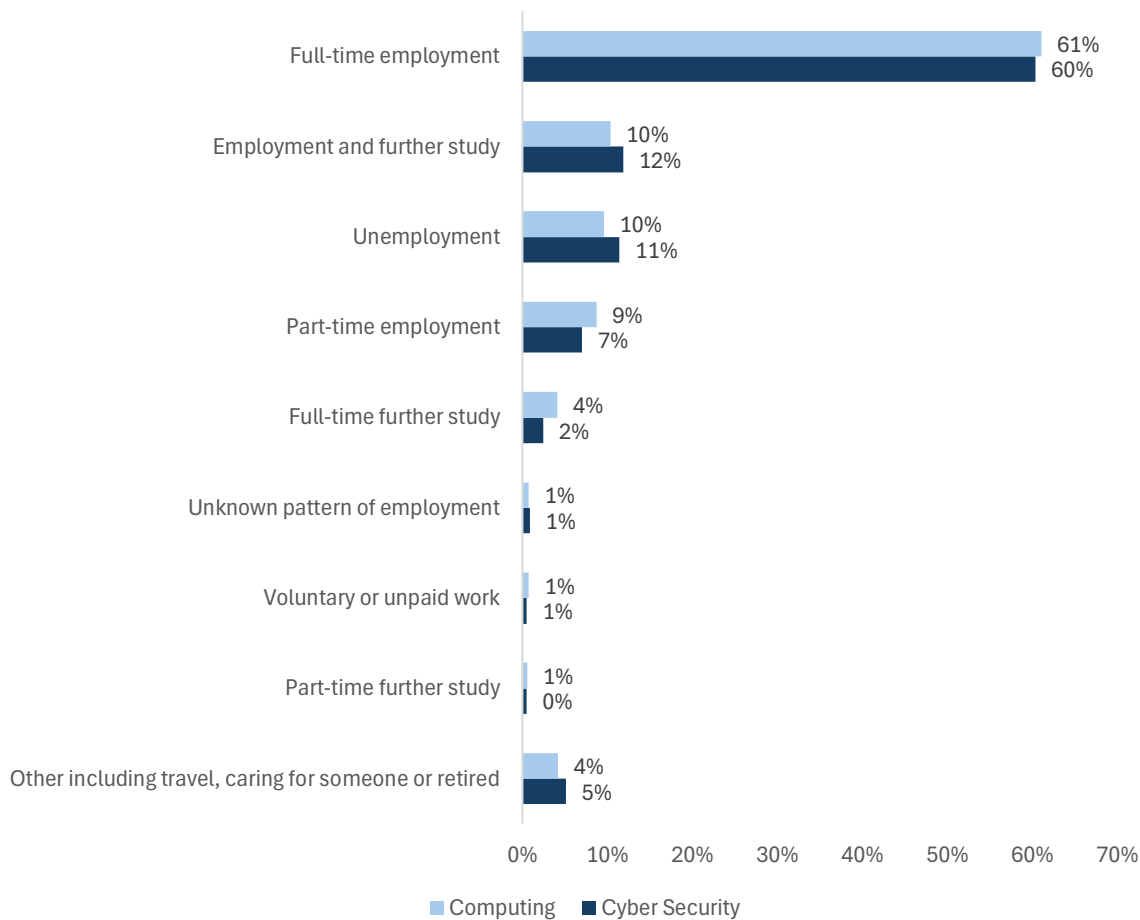
Among the 1,190 cyber security graduates who were employed and provided job role and location data in the 2023/24 Graduate Outcomes survey, 94% were working in the UK. Across cyber security and computing graduates combined, the UK retention rate was 92%, equating to over 9,000 graduates working in UK jobs.

Graduate employment outcomes

The most recent HESA data from the 2023/24 Graduate Outcomes survey covers graduates from the 2022/23 academic year (who are asked to complete the survey approximately 15 months after graduation, i.e., late 2024).

The results (Figure 5.2) show that 60% of cyber security graduates entered full-time employment, with an additional 12% combining employment and further study. Part-time employment remained similar to last year's report at 7% of graduates (6% in 2021/22). Combining these figures, we estimate that approximately 79% of the 6,980 students graduating in cyber security in 2022/23, and the 7,950 graduating in 2023/24, will have entered the labour market within 15 months of graduating.

The unemployment rate for cyber security graduates has risen to 11% in the 2022/23 academic year (9% in 2021/22), [compared to 6% across all graduates](#). This gap is persistent and has grown across years and suggests ongoing challenges in the transition from education to employment, where cyber security graduates may face specific difficulties in meeting employer requirements. As discussed in Section 5.4, in the qualitative research some employers felt that graduates lacked job skills such as understanding business context, up-to-date cyber security skills and that their salary expectations could be unrealistic.

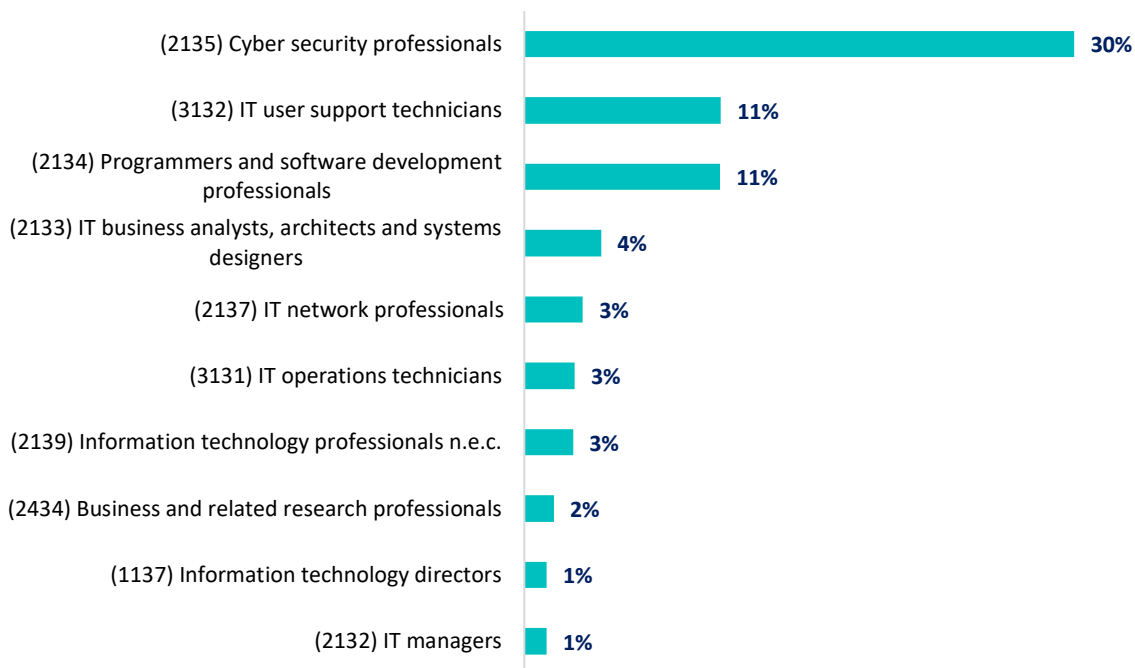
Figure 5.2: UK graduate employment outcomes (2022/23 academic year)

Source: HESA Graduate Outcomes survey 2023/24 (2022/23 academic year). Bases: 2,370 cyber security graduates and 16,710 computer science graduates

The most recent Graduate Outcomes survey also contains SOC data for the 2022/23 academic year.

As shown in Figure 5.3, 30% of cyber security graduates entered cyber security professional roles, consistent with the previous year's figure of 31% in 2021/22. Many of those in programming roles, or the other IT-related roles covered in the chart, may ultimately work for cyber security employers. The next 5 most common SOC codes may also signify jobs that require or benefit from cyber security expertise or are with cyber security employers.

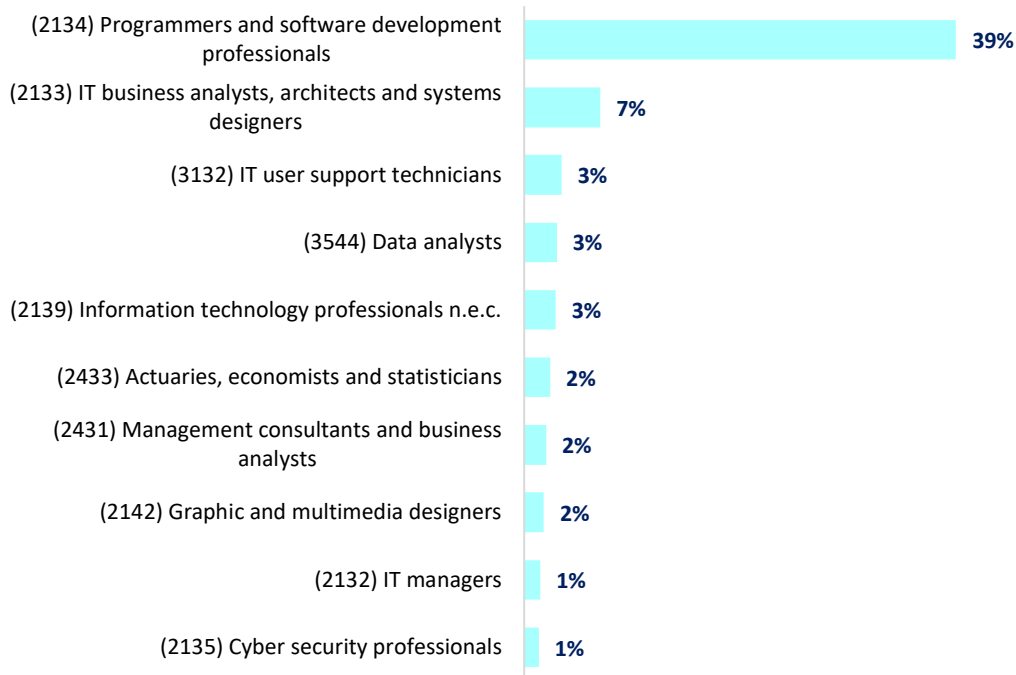
Figure 5.3: Top 10 most commonly coded job roles for UK cyber security graduates based on SOC 2020 (2022/23 academic year)



Source: HESA Graduate Outcomes survey 2023/24 (2022/23 academic year). Base: 1,310 cyber security graduates in full-time employment with SOC details

Figure 5.4 shows that 39% of computer science graduates reported employment as programmers and software development professionals. In line with the previous year, only 1% of computer science graduates from 2022/23 entered cyber security professional roles (not shown in chart), suggesting persistent challenges in attracting these graduates to the sector amid competition from other industries, including software, graphic design and professional services.

Figure 5.4: Top 10 most commonly coded job roles for UK computer science graduates based on SOC 2020 (2022/23 academic year)



Source: HESA Graduate Outcomes survey 2023/24 (2022/23 academic year). Base: 9,500 computer science graduates in full-time with SOC details

Broader educational pathways into cyber security

To understand the diversity of educational pathways into cyber security, we analysed the academic backgrounds of graduates working in cyber professional roles (SOC 2135) within fifteen months of graduation. The sample included 670 graduates (from the 2022/23 academic year) who completed the latest Graduate Outcomes survey. This shows that:

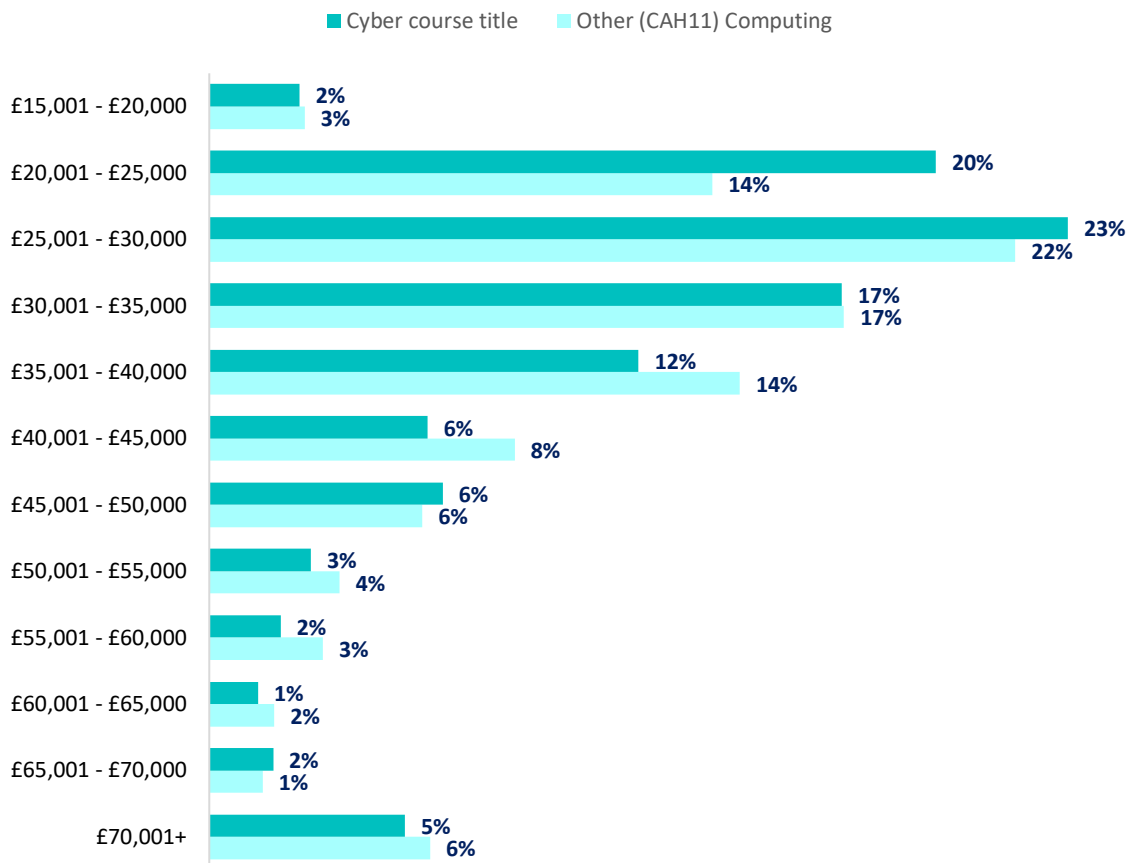
- 59% of these students studied a cyber security course
- 18% studied computing or computer science course
- 7% studied a science, technology, engineering and maths (STEM) related course
- 9% studied humanities or social sciences
- 6% studied accounting, business, economics or finance.

This suggests that although a substantial proportion of cyber security professionals came from cyber security, computing and computer science backgrounds, graduates from other disciplines continued to feed into the cyber security workforce. This highlights the value in encouraging graduates from a wide range of pathways into the cyber security profession, as well as postgraduate reskilling bootcamps.

Salaries

Analysis of Graduate Outcomes data on full-time employment salaries (Figure 5.5) indicates that both cyber security and computer science graduates earn median salaries in the £30,001-£35,000 range within 15 months of graduating.

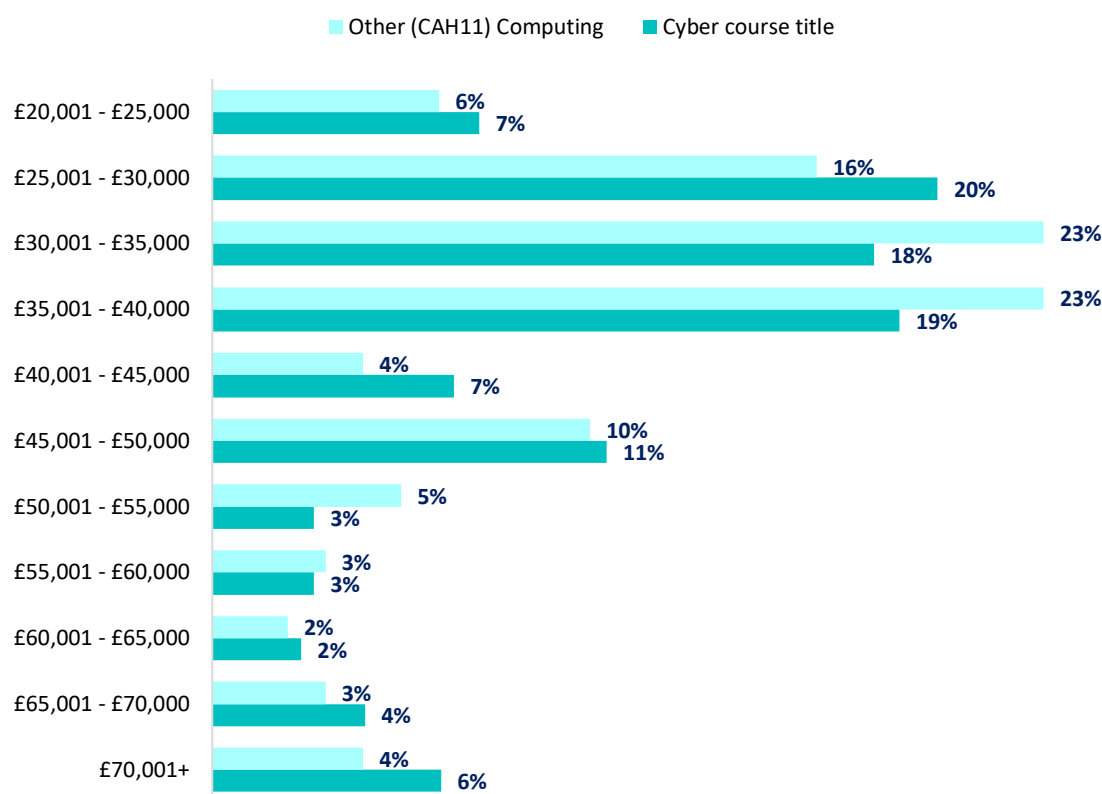
Figure 5.5: Reported salaries of UK cyber security and computer science graduates in full-time equivalent employment (2022/23 academic year)



Source: HESA Graduate Outcomes survey 2023/24 (2022/23 academic year). Bases: 980 cyber security graduates and 7,110 computer science graduates in full-time employment with reported salaries

Further analysis focusing specifically on graduates who entered into cyber professional roles (SOC2135) reveals the same median salary band of £30,001-£35,000 (Figure 5.6). This analysis also shows that the salary distributions were similar between cyber security and computer science graduates working in these cyber professional roles. **The latest data suggests that the previous salary disparity between these 2 graduate groups, on entering these roles, has diminished.**

Figure 5.6: Reported salaries of UK cyber security and computer science graduates in full-time equivalent cyber professional roles (SOC 2135, 2022/23 academic year)



Source: HESA Graduate Outcomes survey 2023/24 (2022/23 academic year). Bases: 230 cyber security graduates and 100 computer science graduates in full-time cyber security roles with reported salaries

5.2 Apprenticeship data

Further Education continues to provide an increasingly important route into the labour market for cyber security students, introducing them to fundamental concepts and acting as a stepping stone to other career pathways. This section focuses specifically on the apprenticeships pathway, covering digital apprenticeships (which include ICT and technology-related programmes), as well as specific cyber security apprenticeship standards. Apprenticeship data from the Department for Education only covers apprenticeships in England (not the whole of the UK). The latest data covers the 2024/25 academic year.

Digital apprenticeships

Digital apprenticeships encompass a range of ICT and technology-related programmes, including areas such as software development, cyber security, data analysis, and IT support. These apprenticeships provide practical, work-based training routes into the sector.

The number of apprenticeship enrolments¹⁸ in Digital apprenticeships in England has continued to grow strongly, rising from 53,280 in 2023/24 to 61,250 in 2024/25 (+15%). The number of apprenticeship

¹⁸ Apprenticeship enrolments are the count of enrolments at a programme level for each academic year. Learners will be counted for each apprenticeship they take. Therefore, each learner may be counted more than once.

starts¹⁹ also increased substantially, from 26,060 in 2023/24 to 31,410 in 2024/25 (+21%). These figures highlight the increasing inflow of students pursuing Digital apprenticeships.

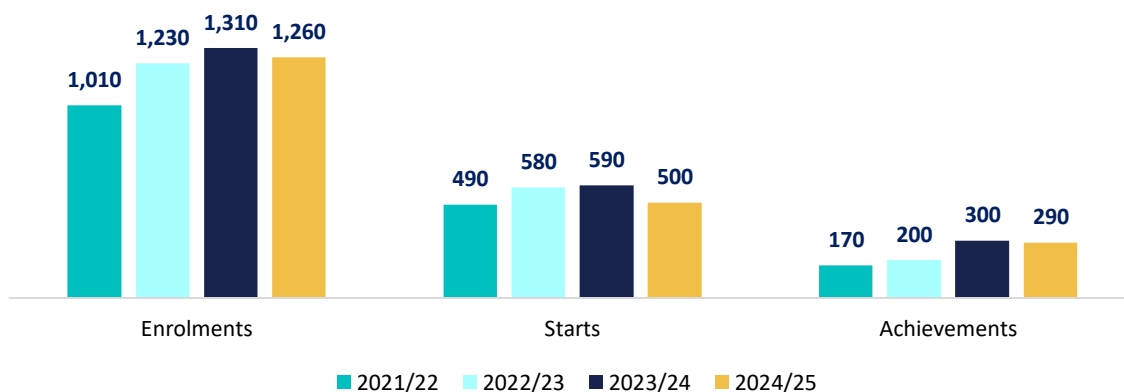
In 2024/25, female starters made up 40% of all Digital apprenticeship starts. Female starters exceeded male starters in 4 specific apprenticeships: Data Technician (4,300 female vs 3,300 male), Digital Learning Designer (110 vs 60), Digital Accessibility Specialist (20 vs 10), and Digital User Experience Professional (30 vs 10). Notably, Data Technician remains the apprenticeship with the largest absolute number of female starters and continues to attract more women than men. The proportion of female starters across all Digital apprenticeships (40%) is double the proportion of female students enrolled cyber security courses in Higher Education (20% on average across undergraduate and postgraduate).

The full data for this section is provided in Annex F.

Cyber security apprenticeships

Figure 5.7 shows the number of apprenticeship enrolments, starts and achievements in cyber security apprenticeships in England over the past 4 academic years. Following growth between 2021/22 and 2023/24, the number of students starting cyber security apprenticeships has declined by 15% in 2024/25 (from 590 to 500). However, achievements²⁰ have remained relatively stable, declining marginally by 3% from 300 to 290, suggesting that learners who are enrolled continue to successfully reach the end point of assessment.

Figure 5.7: Number of cyber security-related apprenticeships in England (2021/22-2024/25 academic years)



Source: Department for Education [apprenticeships data](#)

Bases: 7,930 learners who have been enrolled in, started or achieved apprenticeships in England; 1,670 in 2021/22; 2,010 in 2022/23; 2,200 in 2023/24; 2,050 in 2024/25

N.B. numbers are rounded to the nearest 10 to avoid disclosure and may not sum due to rounding.

It is important to remember that the data only includes apprenticeships in England, rather than the whole of the UK. As such the UK figure is likely to be slightly higher. The estimated number of cyber security apprentices entering the UK-wide cyber security labour market therefore rounds up the figure for the number of achievements in England in the most recent academic year. Overall, an estimated 500 new apprenticeship entered into the UK labour market (down from 600 in the previous study).

¹⁹ Apprenticeship starts show the take-up of programmes each academic year. As with apprenticeship enrolments, learners will be counted for each apprenticeship they start. Therefore, each learner may be counted more than once.

²⁰ Apprenticeship achievements signify a learner reaching the end point of assessment. This is not necessarily the same as reaching the end of their learning/apprenticeship.

5.3 Retraining and upskilling

Beyond formal Higher and Further Education qualifications, many employers seek candidates with skills demonstrated through professional certifications and specialist training programmes. There has been growing recognition in recent years of how certification and training pathways can enable rapid upskilling for those entering cyber security roles or expanding their expertise within the field. Innovative training models, including cyber security academies and bootcamps, alongside improved access to affordable online learning platforms, have contributed to increased engagement with cyber security training.

These technical accreditations represent an important component of the cyber security workforce supply, complementing traditional educational routes. The previous 3 iterations of this research estimated these routes could be generating approximately 2,500 additional individuals entering into the cyber security recruitment pool each year²¹. This year, this estimate has been revised to 1,500 as a conservative figure due to less data being available on conversion course uptake and completion. This reflects the limited new data available to fully update this figure, as explored below. Where new data is available, there appears to be relative consistency or modest growth from previous years.

Certifications

ISC2 previously published annual data on CISSP certifications among its membership but has ceased to do so. The most recent figure, reproduced from [last year's report](#), suggests that there were approximately 8,500 ISC2 members in the UK holding the CISSP certification (an increase of 8% between January 2021 and January 2023).

CompTIA is also a prevalent certification provider, offering certifications in Penetration testing, Security analysis, Network administration such as a+ Network, CySA+, Security+, and PenTest+.

Armed forces

Close to 15,600 individuals left the Armed Forces between April 2023 and the end of March 2024. In this period, over 11,172 service leavers used support from the [Career Transition Partnership](#) (a scheme to support leavers into employment). Of these, 814 entered Science, Research, Engineering and Technology Professional roles, of which 166 reported a role as a Cyber Security Professional under SOC 2020. This represents an increase of 38% from the 2022/23 figure of 120, and a 124% increase from the 2021/22 figure. The consistent year on year growth demonstrates an encouraging and viable retraining pathway, with increasing interest in cyber security as a career transition route for service leavers.

Specific UK-based retraining and upskilling initiatives

A variety of retraining and upskilling programmes operate across the UK, delivered by providers including [Immersive Labs](#), [Capslock](#), [QA](#), [SANS](#), and numerous online platforms. Consistent with last year's analysis, an estimated 1,200 individuals may enter the cyber security recruitment pool annually through these channels. This estimate reflects analysis of multiple UK initiatives, including Assured Skills Academies, publicly funded skills programmes (UK Skills Bootcamps), and the Career Transition Partnership referenced above.

²¹ **Cyber security skills in the UK labour market 2025.**

<https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2025>

5.4 The effectiveness of entry-level pathways

Impact of AI and automation on entry-level roles

In the qualitative research, there was growing concern about the impact of AI and automation on the talent pipeline and the development of skills of entry-level employees (the impact of AI on cyber security skills more generally is discussed in Section 6.5).

Participants felt that as routine tasks such as monitoring and reporting threats were increasingly automated, entry-level opportunities were being reduced. This was thought to have particularly impacted Security Operations Centre (SOC) analyst positions that have historically served as key training opportunities for entrants into the industry. These changes had created a situation where entry-level candidates required more advanced skills and experience but had fewer opportunities to develop these skills.

"I'm quite fearful what [AI] might do. I look at a SOC as being a great entry-level function, but so much of a SOC is being replaced with AI for diagnostics and triages. You need to be more skilled at the point you enter, but with no low entry point to gain that skill."

Large non-cyber security (private sector) business

However, a few employers saw opportunities in the AI-savviness of entry-level candidates, who had grown up in an age of rapidly advancing technology. They felt this could equip candidates with the skills both to operate AI-powered cyber security tools (as discussed in Section 6.5, regarded as a key capability for the cyber security workforce in the future) and defend against emerging AI threats.

Overall, employers were concerned about the long-term implications of AI and automation on entry-level roles because the pipeline for senior roles would likely be diminished. While human oversight was believed to still be essential, employers felt the pathway to becoming an experienced cyber security professional was narrowing.

"I think we have had the debate internally around if you don't have enough entry-level roles, where do you get seniors from later?"

Large non-cyber security (private sector) business

Current entry-level recruitment

The entry-level market was described as saturated in the past 12 months, reflecting the wider trend (discussed in Section 4.5) of a slowing demand for cyber security professionals. Employers reported being overwhelmed with applications from junior candidates who lacked the right skills. Some employers and recruitment agents commented that entry-level cyber security roles increasingly required IT experience, such as working on an IT help desk.

Some participants described a mismatch between the reality of the job market and the expectations of entry-level candidates of plentiful opportunities and excellent pay. This has led to employers having to sift through numerous applications for increasingly scarce entry-level positions.

"We've been seeing an influx of people starting or trying to move into cyber... I am finding more and more people are now scrapping over these entry-level jobs."

Micro cyber security sector business

Barriers to entry-level recruitment

AI, automation and market conditions had all increased barriers to entry-level recruitment. The other key obstacles highlighted in the previous studies were largely unchanged in this study's qualitative research. Employers continued to reference the resource-intensive nature of developing junior talent, both in terms

of time and money. Another ongoing risk was entry-level employees leaving for higher salaries once they were trained up, making investments in these employees challenging to justify. Remote working, now embedded in many organisations, continued to complicate mentorship and hands-on training opportunities, which were considered crucial for entry-level staff.

"I would love to bring in apprenticeship schemes and placements. But I can't do that because I don't have a senior [employee] who I can attach to an office, who can have a junior or an apprentice literally sitting on their shoulder and watching what they do."

Large cyber security sector business

Apprenticeships, academia-industry collaboration, and government programmes

Employers once again talked about a disconnect between university education and industry needs. Cyber security degrees were regarded by some as outdated, and there was a perception that courses were failing to cover developments in technologies like AI (the training providers spoken to were incorporating AI into their training either as modules or stand-alone courses). Course content was thought to be lagging a few years behind industry requirements. Some employers felt that graduates lacked skills which were required for real-world application of cyber security, for instance communication skills and understanding business context.

"A lot of people are coming out of university thinking they know cyber security and how the industry works, but they are so far behind the curve because of the way the industry moves and evolves so quickly that universities and education systems can't keep up."

Micro cyber security sector business

These concerns led some employers to regard apprenticeships more favourably than graduate recruitment. Apprenticeships were valued for enabling enthusiastic early talent to be moulded to the organisation's needs, as well as making cyber security careers more accessible to anyone for whom university was not a viable option. However, other employers preferred university graduates, viewing these employees as less time-consuming to train up, particularly those from academic backgrounds which required strong analytical skills.

Consistent with the previous studies, participants wanted to see evidence of stronger partnerships between employers, educational institutions, and government to address entry-level challenges. Participants encouraged universities to update curriculums in partnership with industry. Some also felt that larger employers had a responsibility to work with educational establishments to provide structured entry-level pathways.

"I think once you get to a certain size, you should be putting in an entry-level pathway. You've actually got to plan it – you've got to partner with educational resources."

Large non-cyber security (private sector) business

Findings on current collaboration between cyber security employers and educational institutions were also consistent with the previous studies. While some employers were actively engaging through guest lectures and curriculum input, others had reactive relationships, reaching out when specific training or recruitment needs arose. Some employers were not engaging with educational establishments at all.

As covered in Section 3.4, the government's CyberFirst initiative was praised in depth interviews as a way to attract young people into the sector. Employers also praised other courses and initiatives, such as Cyber Resilience Centres and cyber security-focused training providers, which were engaging potential entrants with the sector and supporting them into the industry.

As in the previous studies, financial support was consistently highlighted as essential for making entry-level programmes available, especially for SMEs.

6 Skills gaps and shortages including estimating the recruitment pool

This chapter explores the cyber security skills that organisations feel they need, as well as skills gaps and skills shortages. Cyber security skills gaps exist when individuals working in or applying for cyber security roles lack the skills necessary for those roles. Skills shortages are when there is a shortfall in the number of skilled individuals working in or applying for cyber security roles.

Most of this chapter focuses on private sector businesses (referred to simply as businesses), charities and public sector organisations, with the exception of Sections 6.1 and 6.9, which are exclusively about the cyber security sector.

AI skills and their impact on cyber security was also an important theme in this study's qualitative research. This is covered in Section 6.5.

The current picture

This year 808,000, or 57%, of UK businesses reported having a basic technical skills gap. This is an increase from 49% in 2025, highlighting the continued and increasing need for support and guidance on basic cyber hygiene. This skills gap was especially wide for small businesses and charities. The area with the biggest skills gap was in detecting and removing malware.

This year saw 35% of businesses outsourcing at least one aspect of their cyber security, a figure remaining consistent with previous years. However, there was an increase in outsourcing among public sector organisation (69%) compared to 2025 (58%). As per last year, medium and large businesses were more likely to outsource.

What's new since the 2025 report?

There was a notable increase in the use of AI in everyday activities among cyber security businesses, up 17 percentage points compared to last year. There was a similar increase in those expecting their needs for AI skills among employees to rise in the next 12 months.

In the qualitative research, participants reported that AI was increasingly being integrated into cyber security tools and cloud security platforms. Some cyber security firms continued to take a cautious approach to adopting AI. Cyber security firms' and cyber security leads' involvement in securing AI systems typically related to education, training and developing policies on AI use and governance.

There was widespread agreement among participants that AI and automation would transform the cyber security skills landscape. As discussed in Chapter 5, this was thought particularly likely to impact entry-level roles. Some felt that AI would reduce the need for specialist technical skills in the sector as a whole, while others believed that demand for technical skills and specialist AI cyber security roles would increase. Participants predicted a rise in AI governance roles

Although participants thought it was difficult to predict what skills would be needed in the future, some highlighted the ongoing need for foundational cyber security skills such as applying security principles to systems.

6.1 Technical skills gaps within the cyber security sector

Prevalence of technical skills gaps

A quarter of cyber security businesses (24%) reported that a lack of technical skills among their existing employees affected their ability to meet their business goals. This rose to almost 4 in 10 (38%), when asked if they had been affected by job applicants who lacked technical skills.

The proportion of firms reporting that a lack of technical skills among job applicants was an issue has not changed since this was first measured in the 2020 study. In contrast, firms reporting a lack of technical skills among existing employees has trended upwards since the 2021 study (18% in 2021, vs. 24% in 2026). This problem was most pronounced in the 2025 study, when it peaked at 28%, but dropped slightly in this study to 24%.

Areas in which there are technical skills gaps

As shown in Figure 6.1, the top perceived skills gaps within the cyber security sector were in security testing (21%) and digital forensics (20%). All the skills areas covered in Figure 6.1 are taken from the UK Cyber Security Council's [Cyber Career Framework](#).

Figure 6.1: Percentage of UK cyber security businesses that had skills gaps in the following technical areas, among those that identified any skills gaps



Base: 113 cyber security businesses identifying technical skills gaps among employees or job applicants

Changes since the previous study were:

- A drop in skills gaps for auditing and assurance (23% in the 2025 study, vs. 8% in this study) and cryptography and communications security (22% in the 2025 study, vs. 14% in this study)
- A wider skills gap for cyber security governance and risk management (11% in the 2025 study, vs. 16% in this study)
- A rise in the proportion of firms reporting that they had no skills gap or were not missing any of the skills from the Cyber Career Framework (8% in the 2025 study, vs. 14% in this study)

6.2 Technical skills gaps outside the cyber security sector

In line with previous waves, cyber security leads in organisations in the private, charity and public sectors were asked to report how confident they or anyone else in a cyber security role would be at carrying out specific cyber security tasks or functions. Those who were not confident were understood to have a skills gap in this area.

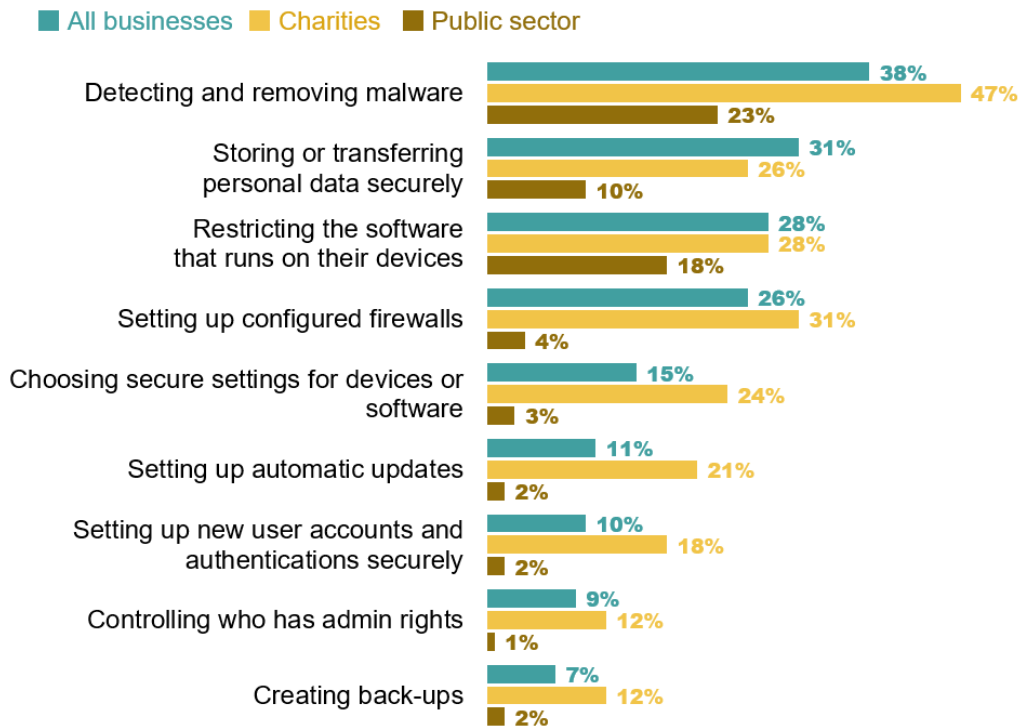
Where organisations outsourced a cyber security task or function to external service providers, this was not counted as a skills gap (as the function was being fulfilled through skills sought externally). The proportions outsourcing each task are covered in Section 6.9 below.

Basic technical skills gaps

The survey explored organisations' ability to confidently cover a range of basic technical cyber security tasks and functions. These tasks, listed in Figure 6.2, were a combination of the technical areas covered under the government-endorsed [Cyber Essentials](#) scheme and other basic aspects of cyber security. The list does not include incident response, which is covered separately in Section 6.3, as an important skill in its own right.

The areas where skill gaps were most prevalent were in detecting and removing malware (38% among businesses, 47% among charities and 23% among public sector organisations), followed by storing or transferring personal data securely, restricting software that runs on devices, and setting up configured firewalls.

These areas have been at the top of this list in all previous studies, but this study saw a greater proportion of private sector businesses reporting skills gaps. Increasing skills gap were found for detecting and removing malware (23% in the 2025 study, vs. 38% in this study) and storing and transferring personal data securely (25% in the 2025 study, vs. 31% in this study). This highlights the ongoing need for basic cyber security advice and guidance to organisations outside the cyber security sector.

Figure 6.2: Percentage not confident in performing basic cyber security tasks, by type of organisation in the UK

Bases: 982 businesses; 162 charities; 117 public sector organisations

N.B. these figures are rebased on the full survey samples, but the questions were only asked of a subsample.

N.B. 'All businesses' refers to all private sector businesses.

As a measure of the overall basic skills gap, all 9 tasks listed in Figure 6.2 were combined. This conveys the overall percentage of organisations that were not confident in carrying out at least 1 of these basic tasks. From this, 57% of businesses had a basic technical cyber security skills gap. This equates to approximately 808,000 UK businesses,²² and represents an increase from 49% in the 2025 study, equating to approximately 699,000 businesses.²³

This change may be due to higher awareness of organisations' cyber security posture rather than a decline in perceived capabilities. In the qualitative research, cyber leads reported that recent high-profile breaches experienced by well-known UK companies have increased attention on cyber security in their organisations.

"I don't think there's significantly more attacks, but it's been a lot more public. So obviously with Marks and Spencer, Co-op, Harrods and a plethora of others, and JLR more recently as well, it's been very much the focus of the exec and the board."

Large non-cyber security (private sector) business

²² The business population data is taken from the [DBT business population estimates 2025](#). These were the latest estimates as of the publication of this report, identifying a business population of 1,417,730 (for businesses with 1 or more employees). The extrapolated figures presented here and later in this chapter are rounded to 3 significant figures. These figures are subject to a margin of error, as with all the results from the survey. The margin of error for businesses on this result is ± 4 percentage points. This means that the true figure could be between approximately 751,000 and 865,000 businesses.

²³ The margin for error for businesses on this result is ± 3.9 percentage points. This means that the true figure could be between approximately 644,000 and 755,000 businesses.

The basic cyber security skills gap was, once more, lower for large businesses (24%, compared to 57% for smaller businesses), indicating that smaller organisations faced the greatest difficulty in meeting these basic cyber security requirements.

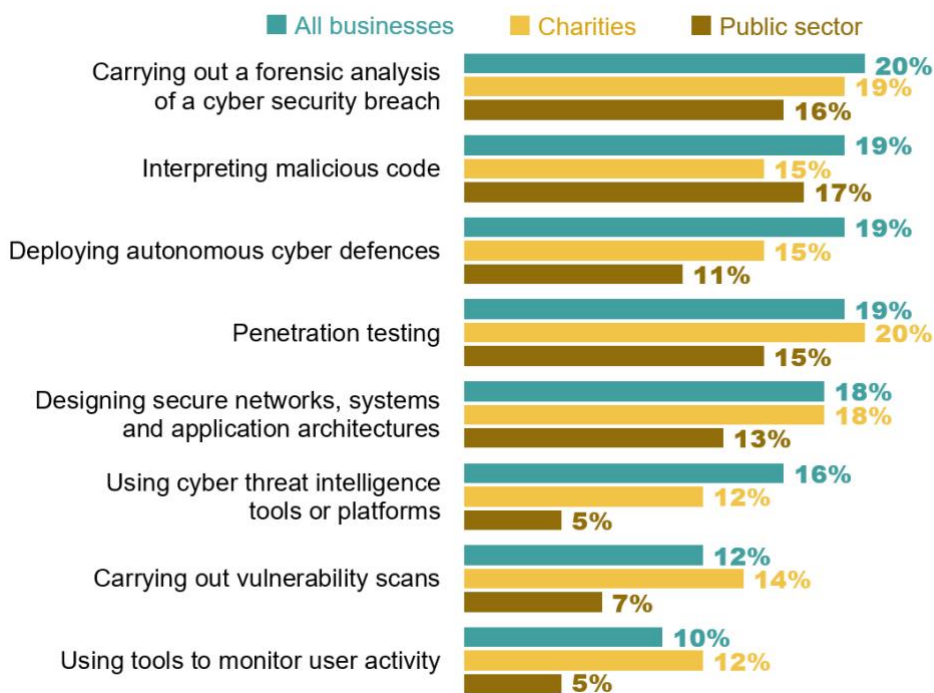
Reflecting a pattern from the previous studies, this estimate was considerably lower for public sector organisations (27%) than for private sector businesses (57%). Although, notably, the skills gap has almost doubled for public sector organisations, versus last year (27% this year, vs 14% in the previous wave). Almost 6 in 10 charities (58%) had a basic skills gap, in line with the previous study.

Advanced technical skills gaps

Advanced technical skills are those that expected not to be required in every organisation but important for those with more sophisticated cyber security needs. A total of 15% of businesses (rising to 48% of large businesses), 14% of charities and 33% of public sector organisations considered high-level technical skills among their cyber security staff to be essential to their organisations. This was based on a rating of 0 to 10 in the survey, where 10 meant “essential”.

Participants were then asked about confidence in carrying out higher level cyber security tasks. Figure 6.3 shows 8 such skills measured in the survey.

Figure 6.3: Percentage not confident in carrying out ‘higher level’ cyber security tasks, by type of organisation in the UK



Bases: 982 businesses; 162 charities; 117 public sector organisations

N.B. these figures are rebased on the full survey samples, but the questions were only asked of a subsample.

As shown in Figure 6.3, skills gaps for businesses were highest in carrying out forensic analysis of a cyber security breach (20%), interpreting malicious code (19%), deploying autonomous cyber defences (19%) and penetration testing (19%). Charities saw some skills gaps on par with businesses in penetration testing (20%) and carrying out forensic analyses of cyber security breaches (19%). Skills gaps tended to be lower for public sector organisations (except for carrying out vulnerability scans). The

smallest skills gap was in using tools to monitor user activity (10% not confident in businesses, 12% in charities, 5% in public sector organisations). These results were broadly in line with the previous study, although there seems to be slightly less confidence in carrying out higher-level tasks among public sector organisations in this study, compared to the previous study (e.g. 16% of public sector organisations not confident in carrying out forensic analysis of a cyber security breach in this study, vs. 13% in the 2025 study).

As a measure of the overall advanced skills gap, all 8 tasks were combined to calculate the percentage of organisations that were not confident in carrying out at least 1 of these advanced tasks. From this, 27% of businesses had an advanced technical cyber security skills gap, broadly similar to the figure from the 2025 study (30%). This equates to approximately 383,000 UK businesses.²⁴

The overall advanced skills gap was broadly similar for large businesses (29%), charities (25%) and public sector organisations (31%). Compared to the previous study, there was a large widening of the 'higher-level' skills gap in public sector organisations (21% in the 2025 study), whereas the figures for large businesses and charities remained broadly the same.

6.3 Incident response skills

Incident response has remained a challenging area for organisations. Almost half of individuals responsible for cyber security in UK businesses and charities (47% each), lacked the confidence to deal with cyber security breaches or attacks, and had not outsourced this function (Figure 6.4). Staff responsible for cyber security in large businesses and the public sector were less likely to identify incident response as a skills gap than businesses overall (only 11% not confident for large business and 13% for public sector organisations). This pattern was also seen in previous waves.

Despite some fluctuations over the past few studies, the skills gap for incident response has generally plateaued, but remains higher than in the 2021 study.

²⁴ The margin for error for businesses on this result is ± 5.1 percentage points. This means that the true figure could be between approximately 310,000 and 455,000 businesses.

Figure 6.4: Organisations not confident in dealing with cyber security breaches or attacks

Bases (for 2026): 646 businesses who did not outsource this function, 39* large businesses who did not outsource this function 55 public sector organisations who did not outsource this function, 115 charities who did not outsource this function. *Low base, treat with caution

Separately, cyber leads were asked about their confidence in writing an incident response plan. In this, 49% of cyber leads in businesses, 46% in charities and 20% in public sector organisations were not confident. The figure dropped to 23% and 26% not confident in medium and large businesses, respectively. For context, the [Cyber Security Breaches Survey 2025/2026](#) also reported that formal incident response plans were not widespread (25% of businesses and 19% of charities had them, rising to 57% of medium businesses and 76% of large businesses).

6.4 Complementary skills

In the context of cyber security, complementary skills include all the non-technical skills that cyber security sector employees and cyber leads in the wider private sector require to do their jobs well – sometimes referred to as “soft skills”. They cover aspects such as communication, leadership, management, and sales and marketing skills.

Complementary skills gaps in the cyber security sector

1 in 3 cyber security businesses (33%) reported that a lack of complementary skills among job applicants had impacted their ability to meet their business goals in the last 12 months. A similar proportion (35%) said a lack of these skills among their existing employees had also had an impact.

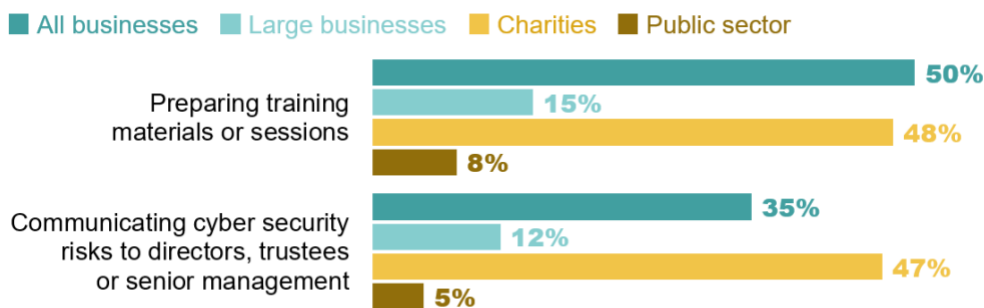
These figures have not notably shifted from the last wave, suggesting this was a relatively constant skills gap. However, a lack of complementary skills remained higher than the lowest recorded results from 2021 (when 18% said job applicants lacked these skills, and 23% said existing employees lacked these skills).

Complementary skills gaps outside the cyber security sector

The survey also examined the confidence that cyber leads had in carrying out specific tasks required to develop and embed good cyber security practice within organisations. These included preparing training for non-cyber staff and communicating cyber security risks to senior internal stakeholders. For wider context, the [Cyber Security Breaches Survey 2025/2026](#) found that 19% of all businesses (84% for large businesses) and 17% of charities had provided cyber security training to staff.

Figure 6.5 shows the percentage of organisations where cyber leads reported that they had a skills gap in these areas. Half (50%) of cyber leads in private sector businesses were not confident in preparing staff training on cyber security, while 1 in 3 (35%) were not confident in communicating cyber security risks to senior individuals in their business. This was less of an issue among large businesses and public sector organisations – though training challenges were still substantial in public sector organisations (48% not confident) as was communicating cyber security risks to senior individuals (47%).

Figure 6.5: Percentage not confident in carrying out tasks that require complementary skills, by type of organisation in the UK



Bases: 487 businesses; 40 large businesses (with 250+ staff); 83 charities; 58 public sector organisations
N.B. these questions were asked of approximately a third of the relevant sampled groups, chosen at random.

6.5 AI skills in cyber security

Cyber security businesses were asked about their use of AI in cyber security. 70% of all cyber security businesses reported that staff were using AI in their day-to-day work, up from 53% in the 2025 study. This is a substantial growth from the integration of AI in the daily work of just over half of firms, to its integration in a clear majority of firms' work. Firms also reported that significantly more of their staff had received AI training (42% in the 2025 study, vs. 53% in this study).

The increased integration of AI was also reflected in recruitment and expected skills needs. Firms were increasingly recruiting for AI specific skills in cyber security roles: among the 53% of cyber security businesses that had tried recruiting since January 2024, 24% had recruited someone with AI skills into a cyber security role (compared to 15% in the last study). Additionally, just under three-quarters (73%) expected their needs for AI skills among employees in cyber security firms to increase over the next 12 months, a rise from 65% in the 2025 study.

The use of AI in cyber security

In the qualitative research, participants reported that AI was increasingly being integrated into cyber security tools and cloud security platforms. One cyber security lead felt that it was not possible to buy security products which did not include AI.

“Specifically in cyber security, we're not going out of our way to use AI, but most of our cyber security tools adopted AI. So it's being foisted upon us. Not that that's a bad thing, it's just a natural progression of getting the job done.”

Large non-cyber security (private sector) business

Cyber security firms taking part in the qualitative research were most commonly using AI in cyber security through third-party security tools or publicly available AI models such as Copilot, ChatGPT, Claude and Gemini.

These AI models were being used by cyber security firms for a range of purposes including administrative tasks such as job scheduling, as well as core parts of their services such as report writing, coding and providing customer support. A few were using AI in their product development.

As found in the previous study, some cyber security firms were taking a cautious approach to AI because of concerns about security or effectiveness. These firms were therefore using AI in limited ways or not at all. Others were in the process of considering how to incorporate AI into their work or were yet to find specific uses for AI.

"I think we're still in the early phases of working out what AI can do for us."

Micro cyber security sector business

Cyber security for AI systems

Private and public sector organisations who took part in the research were typically using publicly available AI models such as Copilot or Gemini in their business activities. A couple were using private AI models created for their organisation.

Cyber security leads were involved with developing policy, guidance and processes, for instance around data governance and blocking the use of unauthorised AI models. There was only one example of a business with a dedicated AI team which did not seek support from the cyber security support team on AI security.

“We've restricted everyone to using Copilot, so we don't allow any other AI tooling at the moment just because we can't control it. The agentic side of things has huge amounts of possibilities, but we're not quite there yet. We're just trying to build the right foundations and the right governance in place first before everyone gets a bit carried away.”

Large non-cyber security (private sector) business

Cyber security firms' involvement in securing AI systems typically related to education and training on using AI safely and helping organisations develop policies on AI use and governance. A few said they were increasingly being asked to security test AI-based applications.

"We're using [their own onboarding training] to provide assistance to clients, general hygiene rules like don't copy and paste private information, don't put the name of the company in there, etc. etc. They're trained to make sure that they understand the use cases for AI, where it works and where it doesn't."

Micro cyber security sector business

The development of AI skills in the cyber security workforce

Employers highlighted the need to adjust to the rapid adoption of AI both in cyber security tooling and organisations' broader operations.

“We have a situation where people want to use AI, which is great, but they're not aware of the potential risks. I need to understand what they're doing, what the risks are and what

they can do. So I need a combination of understanding AI and then applying that to the risk assessment."

Large non-cyber security (public sector) organisation

While a few employers said their organisations provided training on AI, learning about AI was more commonly self-led. This was through hands on experience, sharing knowledge internally (for instance through dedicated sessions on AI) and networking with peers, clients and suppliers.

"Our first few [security tests of AI apps] were a bit shaky. It's a brand-new area. How do you test this compared to usual web apps? But we very quickly developed processes, and we've got a good pedigree in doing those now."

Small cyber security sector business

"Back in May, we did an 'AI week', a week that was dedicated to introducing AI tooling and all kinds of different things to do with AI. And we encouraged people to go and do self-led exploration, trying out tools and becoming more AI-literate."

Medium cyber security sector business

One cyber security lead argued that there was a need to integrate developing knowledge on AI and cyber security into training courses and frameworks.

"We need to start industry or government or NCSC or whoever to build frameworks on this now. Because everyone's learning this on the job, so everyone should be writing these things down and putting together frameworks saying okay, now we understand best practice in managing AI."

Large non-cyber security (public sector) organisation

Some employers commented that there was little or no training relating to AI available. A few were using vendor training, notably from Microsoft on Copilot.

"We've got AI built into a lot of our security tools. That's all embedded in and it's very intuitive, it's very simple. We're a big customer of Microsoft, so if I need some help with it, they can just throw some people at me, and we can get some people trained up."

Large non-cyber security (private sector) business

However, training providers said they were increasingly incorporating training on AI into their cyber security offer, both as modules and stand-alone courses. Echoing the concerns of employers, some highlighted the challenges of training keeping up with rapid change.

There was an expectation that more training on AI would become available in the future. Some participants felt there needed to be affordable and accessible training courses to keep organisations up to date with AI risks and cyber threats more generally.

"If you're going to use these [AI] tools, we've got to have a full understanding. I think there's going to be a lot of growth in that sector of education courses going forward."

Small cyber security sector business

Future AI skills

In the qualitative research, there was widespread agreement that AI and automation would transform the cyber security skills landscape. As discussed in Section 5.4, this was thought particularly likely to impact entry-level roles as routine tasks become increasingly automated. However, some predicted that AI tools would also take on tasks performed at higher levels.

Participants also highlighted the impact of AI, and technology innovation more broadly, on the threat landscape. The volume and sophistication of attacks was thought likely to increase. In parallel, the growing complexity of digital systems and increasing adoption of agentic AI would make cyber security more challenging.

“The application set that we use is constantly evolving. There's a far greater mix of infrastructure and software as a service [SaaS] being used amongst companies. The supply chains in those SaaS services are getting longer and longer, so the point of the threat becomes less obvious and less visible. We are going to have to be doing a lot more work around understanding our threat landscape.”

Large cyber security sector business

There were mixed views about the impact of AI on the technical knowledge required for cyber security roles. Some felt that AI would reduce the need for specialist technical skills, as the focus would shift to operating and managing AI cyber security tools. Nevertheless, participants generally believed that the need for human oversight would remain, in particular decision-making about complex issues where an organisation's specific context would need to be taken into account.

Others thought that demand for technical skills and specialist AI cyber security roles would increase. It was argued that securing AI models required a strong foundation in both cyber security and software engineering, including the ability to test AI-driven code, assess the security of AI infrastructure and applications, and adapt security testing to software development cycles increasingly automated by AI.

“I think that is definitely going to create jobs not just in AI governance, but also engineers, architects. Securing the AI models, that's got to be the biggest thing.”

Recruitment agent

Some participants expected that cyber security tools would become more specific to individual products, increasing the need for product-specific skills. More broadly, cyber security employees would need to keep on top of updates and innovations in cyber security tools.

“So much of it is becoming so product-specific that it's really difficult. You get somebody to get really deep into a product and understand how it works in terms of your protection. But no one else knows as much. When that person's on leave, you're exposed.”

Large cyber security sector business

Some employers were concerned that an overreliance on AI could impede the development of key technical cyber security skills such as defensive expertise, coding software securely, and understanding infrastructure.

“[AI] will have a catastrophic effect on the creativity of the defenders. The attackers who are out there writing malware and compromising systems and ransomware in hospitals, they're not going to change. They're probably using AI, but they're not complacent.”

Micro cyber security sector business

6.6 Qualitative feedback on other future skills needs

Beyond AI, some participants emphasised the increasing importance of skills to secure hardware components and real-time operating systems, such as automotive control systems and critical infrastructure technologies.

Looking further to the future, a few participants highlighted the transformational impact that quantum computing would likely have on cyber security and therefore the skills required for cyber security employees. However, when this would happen was regarded as unclear.

Although it was considered difficult to predict what skills would be needed in the future, some participants highlighted the ongoing importance of foundational cyber security skills. In particular, the ability to apply security principles to systems and to solve problems, as well as the capacity to adapt quickly to change.

“[AI] changes the way you go about your job. And it changes the things you have to do, but it doesn't alter the fact that you have to stay abreast of the technology and the advances and the threats, as we always have.”

Large non-cyber security (private sector) business

6.7 Governance and compliance skills

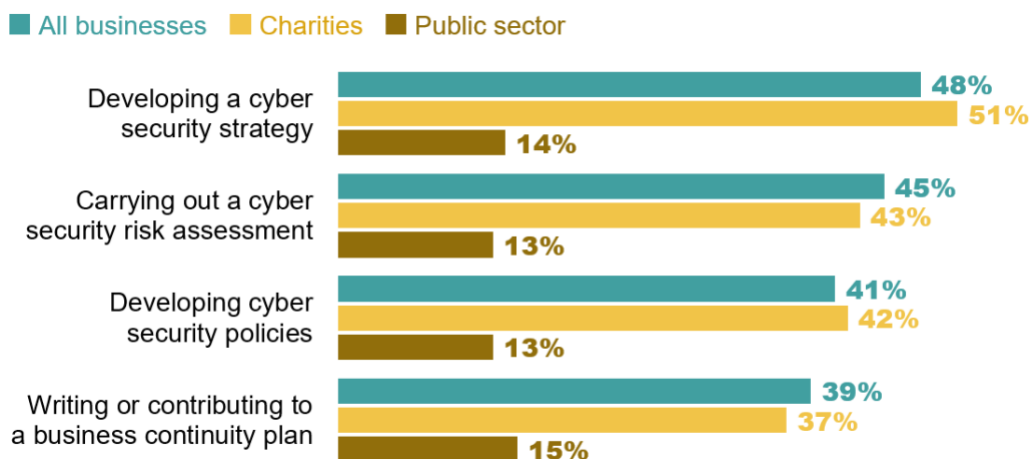
Cyber leads in the wider private, charity and public sectors are often relied upon to develop cyber security policies and strategies, contribute to business continuity planning, and to carry out cyber security risk assessments. The survey covers these 4 governance tasks, as shown in Figure 6.6.

Once again, for wider context, the [Cyber Security Breaches Survey 2025/2026](#) reported that:

- 36% of businesses and 33% of charities had formal cyber security policies in place
- 30% of businesses and 27% of charities undertook cyber security risk assessments
- 33% of businesses and 20% of charities had a business continuity plan that covered cyber security
- 57% of medium businesses and 74% of large businesses had a formal cyber security strategy (this question was only asked of these larger businesses).

Our skills-related survey shows that half of all businesses (48%) were not confident developing a cyber security strategy. Around two-fifths also lacked the confidence to undertake risk assessments (45%), develop relevant policies (41%) and contribute to a business continuity plan (39%). Once more, charities were relatively similar to businesses, while public sector organisations tended to have fewer skills gaps in these areas.

Figure 6.6: Percentage not confident in carrying out a range of cyber security governance tasks, by type of organisation in the UK



Bases: 487/495 businesses; 83/79 charities; 58/59 public sector organisations

N.B. these questions were asked of approximately a third of the relevant sampled groups, chosen at random. The split-sampling meant that some statements had the lower of the 2 base sizes noted here. These lower base sizes do not allow for subgroup analysis by business size. For further information about this sampling approach, please see the technical report.

In the qualitative research, participants predicted a rise in AI governance roles and a stronger focus on governance, risk, and compliance (GRC). It was pointed out that organisations would need to safeguard the security and data integrity of AI systems against potential threats and misuse, for instance, ensuring AI systems use trustworthy data and providing a clear audit trail of how data is sourced, processed and used.

“Governance is really where it's at, to make sure that security is factored in at all points for business architecture.”

Medium non-cyber security (private sector) business

A related point was that along with an increase in GRC roles, there would be more demand for complementary skills relating to communications and engaging with key groups of people in the organisation.

“How do we evolve as a sector to need different kinds of skills because we don't need so much deep technical expertise? We need the human bit, that's what's harder to automate. It's very difficult to automate the ability to influence and communicate effectively.”

Micro cyber security sector business

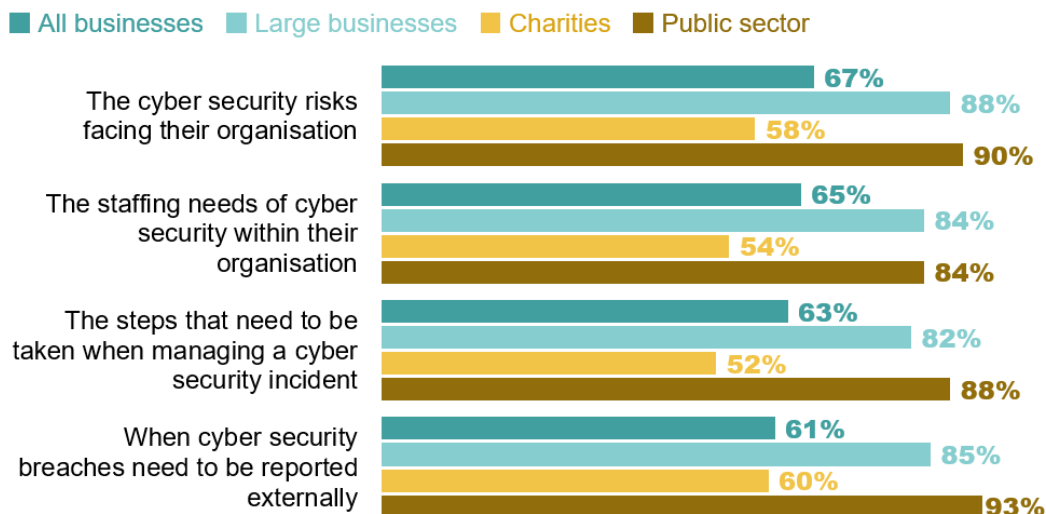
6.8 Cyber security skills gaps in the wider workforce

Wider studies such as the [Cyber Security Breaches Survey](#) series have consistently found that wider staff outside cyber teams have an important role to play in cyber security. Board-level staff influence or decide budgets and assign strategic importance to cyber security. Wider staff are often the first line of defence, helping to identify and report cyber security breaches or attacks.

Board-level skills gaps

As in the previous studies, most cyber leads felt that senior management at their organisations had an adequate understanding of the risks, rules and processes relating to cyber security (Figure 6.7). Once again, these results were notably higher for large businesses and public sector organisations, whereas results were either similar or lower for charities compared to businesses overall. The figures were mostly consistent with the 2025 study, except the proportion of charities saying senior management understood the cyber security risks facing their organisation, which fell from 72% in the 2025 study to 58% in this study.

Figure 6.7: Percentage of cyber leads that felt their organisation's senior management understood the following aspects of cyber security "very well" or "fairly well", by type of organisation in the UK



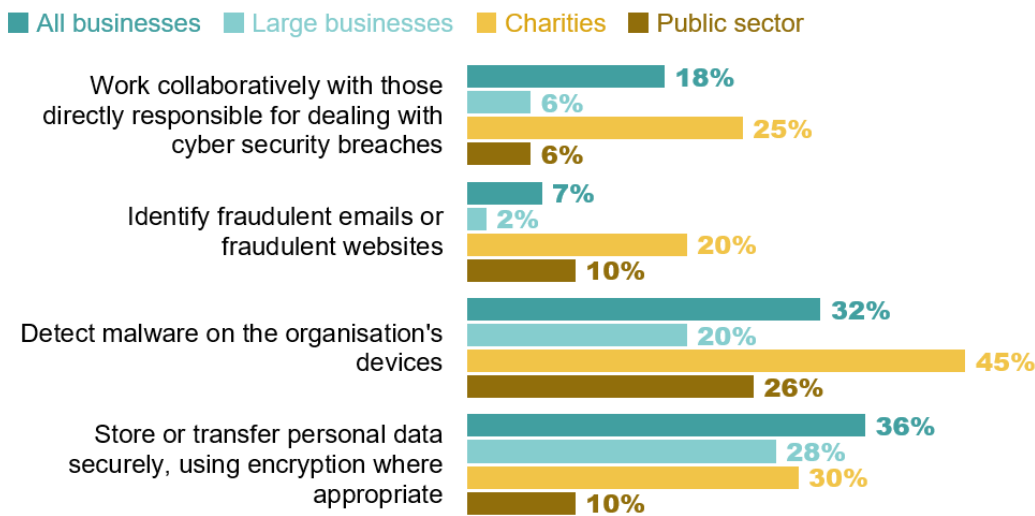
Bases: 982 businesses; 89 large businesses (with 250+ staff); 162 charities; 117 public sector organisations

Finance and insurance businesses, as well as information and communications businesses, were more likely than average to report that senior managers understood all four aspects of cyber security measured well. Administration and real estate businesses were also more likely to suggest that their senior managers understood the cyber security risks facing their organisation (82%, vs. 67% overall).

Skills gaps among wider staff

Relatively few cyber leads had concerns that the wider staff in their organisations could identify fraudulent (phishing) emails or websites (e.g., 7% of businesses were not confident about their wider staff being able to do this, as per Figure 6.8). There was more concern around staff being able to deal with storing or transferring personal data using encryption (36% of businesses not confident), detecting malware (32% of businesses not confident), and working collaboratively with IT or cyber teams (18% of businesses not confident).

Figure 6.8: Percentage not confident in non-specialist staff being able to carry out various tasks that can impact on cyber security, by type of organisation in the UK



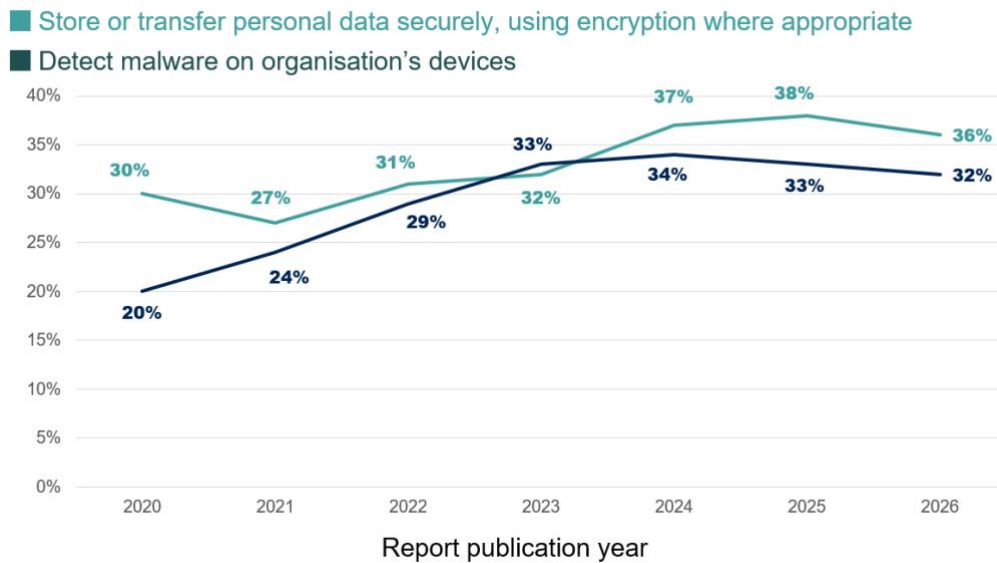
Bases: 495/487/907 businesses; 40*/89/80 large businesses; 162/153 charities; 117/114 public sector organisations. *Low base, treat with caution

N.B. these questions were asked of approximately half the relevant sampled group among businesses, chosen at random, and the full sample among charities and public sector organisations and to the full sample in some cases for businesses.

Charities were markedly more concerned about staff's ability to detect malware compared to the previous study (45% in this study, vs. 26% in the 2025 study), while the figures for businesses and public sector organisations were consistent with the previous study.

As Figure 6.9 indicates, lack of confidence in non-specialist staff being able to securely store and transfer data, as well as detect malware, is higher than in 2020. However, it has remained broadly consistent for the last 3 waves, suggesting the issue has plateaued.

Figure 6.9: Percentage not confident in non-specialist staff being able to carry out various tasks that can impact on cyber security, by type of organisation in the UK



Bases: c.400-500 businesses in 2024, 2025 and 2026; c.1,000 businesses in earlier waves.
For consistency with previous reports, the x axis refers to the report publication year, which is one year on from the fieldwork year.

6.9 Outsourcing

Prevalence of outsourcing

One way for organisations to plug skills gaps is to outsource aspects of their cyber security to external experts. In this study, 1 in 3 businesses (35%) had outsourced at least one aspect of their cyber security. This was less common among charities (21%) but substantially higher in public sector organisations (69%).

Businesses outsourcing at least one aspect of their cyber security is in line with the longer-term trend (having been 31% in the 2025 report, 38% in the 2024 report, 33% in the 2023 report and 32% in the 2022 report). Public sector organisations were more likely to outsource this year compared to the previous wave (69% in this year's report, vs 58% in the 2025 report). Charities and public sector organisations fluctuated, with no consistent trend upwards or downwards over time in terms of outsourcing.

Following trends from the previous studies, outsourcing was more common among:

- medium businesses (51%) and large businesses (50%)
- the finance and insurance sector (48%), the professional, scientific and technical sector (48%) and the administration and real estate sector (46%)

This year, half of small businesses also outsourced at least one aspect of their cyber security.

In this study, the sectors least likely to outsource cyber security were construction (26%), information or communication (24%), arts or recreation (24%) and food or hospitality (18%).

Outsourcing of basic functions (including incident response)

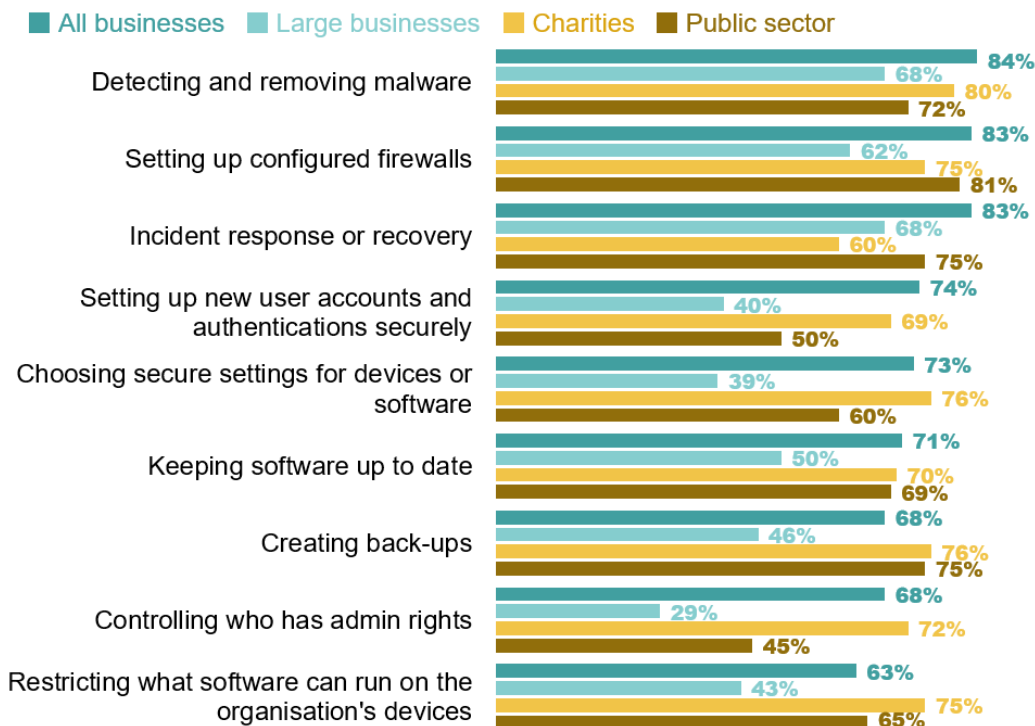
This subsection focuses on the organisations outsourcing specific aspects of their cyber security asked about in the survey (accounting for 35% of businesses). Among these, the basic cyber security activities that every organisation would need to cover are grouped together, regardless of their size or risk profile. These match the cyber hygiene activities from Figure 6.2 earlier in this chapter, as well as including incident response (another universal need across organisations).

Figure 6.10 below shows a recurring pattern from previous waves, in that the top 3 areas that tended to be outsourced among all private businesses were detecting and removing malware (84%), firewall configuration (83%), and incident response or recovery (83%). In line with previous studies, the lowest ranking area was restricting software installations (63%). Although businesses outsourcing the control of admin rights has increased compared to last year (68% this year, vs 57% in the previous wave), there has been no notable upwards or downwards trend in any aspects over time.

Whereas other sections in this chapter have shown large businesses and public sector organisations to be closely aligned in their approaches, they diverged in terms of outsourcing. Figure 6.10 shows that, among those outsourcing anything, public sector organisations were more likely than large businesses to outsource for most of these basic aspects of cyber security.

Among those that outsourced anything, a total of 29% of businesses, 25% of charities and 25% of public sector organisations had outsourced all 9 areas listed in the chart. In other words, most still performed various cyber security functions in-house.

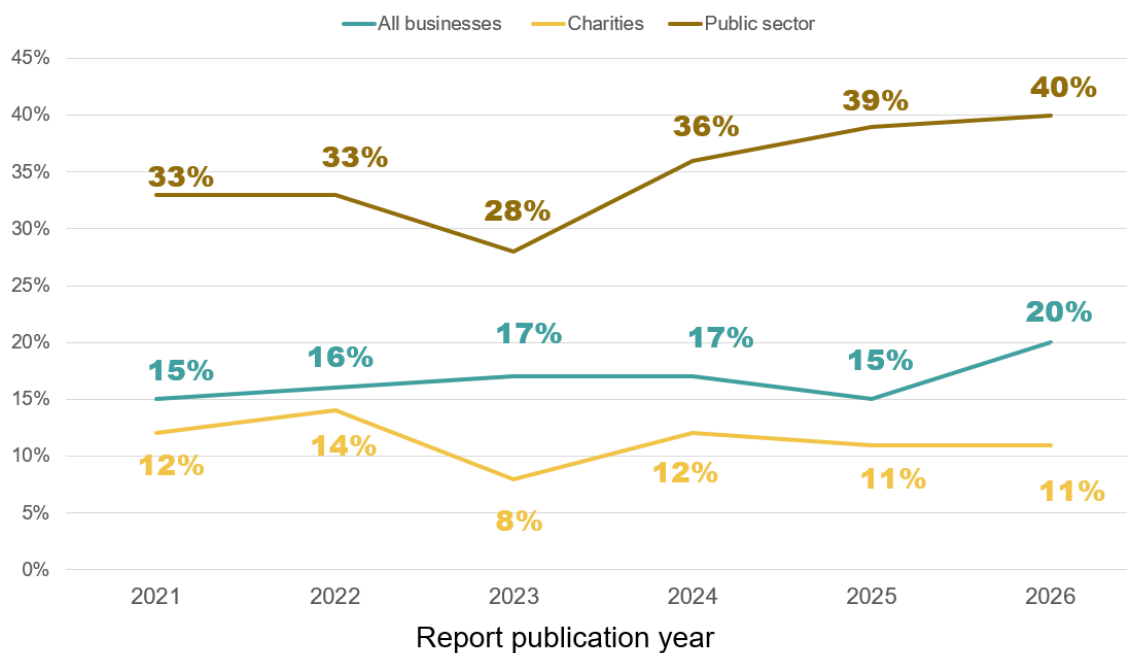
Figure 6.10: Percentage of UK organisations outsourcing various basic cyber security functions, among those that outsource any aspects, by type of organisation



Bases (among those outsourcing any aspects of their cyber security): 405 businesses; 43 large businesses; 63 charities; 82 public sector organisations.

Use of Security Operations Centres (SOCs)

This study saw no notable changes in the statistics. Among all (i.e., not just those outsourcing), 20% of businesses used Security Operations Centres (up 5% compared to last year). This figure was 40% for public sector organisations, compared with 11% for charities. Therefore, public sector organisations were the most likely to use Security Operations Centres, reflecting a pattern back to the 2021 study (when this question was first asked). This is shown in Figure 6.11.

Figure 6.11: Percentage of organisations that outsource using Security Operations Centres

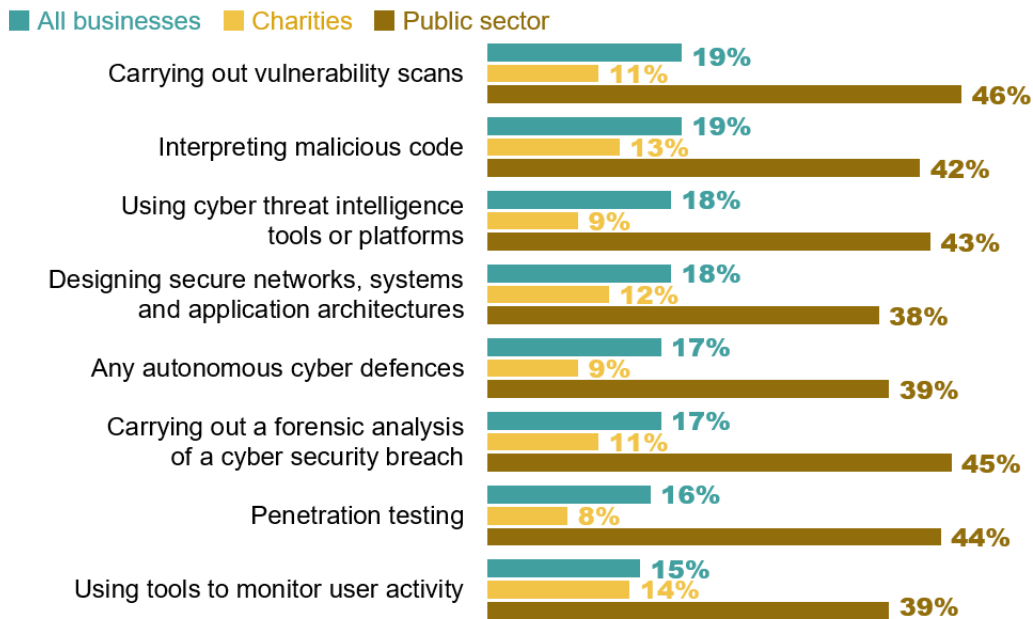
Bases: 982 businesses; 162 charities; 117 public sector organisations

Outsourcing of other more advanced functions

Across the population, around a quarter of businesses (23%) reported outsourcing at least one of the “advanced” cyber security functions listed in Figure 6.12, rising to 31% among large businesses. By comparison, 15% of charities and just over half of public sector organisations (54%) reported outsourcing any of these functions. These figures were similar to previous waves, again suggesting no upwards or downwards trend.

Large businesses outsourced advanced cyber security functions (63%) more often than basic functions (43%). This suggests that larger businesses focus their outsourcing on more complex cyber security skill areas. However, there were not enough large businesses sampled for these questions to break down the specific advanced activities outsourced in Figure 6.12.

Figure 6.12: Percentage of UK organisations outsourcing various “advanced” cyber security functions, by type of organisation



Bases: 982 businesses; 162 charities; 117 public sector organisations

Outsourcing functions outside of the UK

The proportions of organisations that had specifically outsourced any aspects of cyber security outside the UK were relatively low, encompassing:

- 7% of the businesses that outsourced any cyber security functions. This equals 2% of all businesses, which is the same proportion found in the previous study
- 6% of outsourcing charities (1% of all charities)
- none of the public sector organisations in our sample

Due to the low sample sizes, it is not possible to break down the specific functions being taken outside the UK.

6.10 Hard-to-fill vacancies and skills shortages in the cyber security sector

This section covers the cyber security sector. Cyber security businesses are the primary recruiters and employers of cyber-related positions (as covered in Chapter 2), so the survey has historically focused on measuring skills shortages among these businesses.

Half (52%) of cyber security businesses had tried to recruit someone into a cyber security role since January 2024 (i.e., roughly in the 18 months prior to the survey). This was broadly in line with the previous 3 waves (51% in the 2025 study, 47% in the 2024 study and 53% in the 2023 study).

Among those who had tried to recruit a cyber security role since January 2024, the average number of vacancies was 4.0. This suggests a slowdown or end to the fall seen between the 2023 and 2025 studies (from 8.2 in 2023, to 6.1 in 2024 and to 4.3 in 2025).

Hard-to-fill vacancies

Among the 52% of cyber security businesses that had tried to recruit, just over half (53%) reported that at least 1 vacancy was hard-to-fill. This is consistent with the previous wave, although notably lower than in the 3 waves before the 2024 study (70% in 2023, 67% in 2022 and 67% in 2021).

Overall, an estimated 34% of cyber security sector job vacancies themselves were hard-to-fill. This compares to estimates of 33%, 55% and 37% in the 2024, 2023 and 2022 studies, respectively.

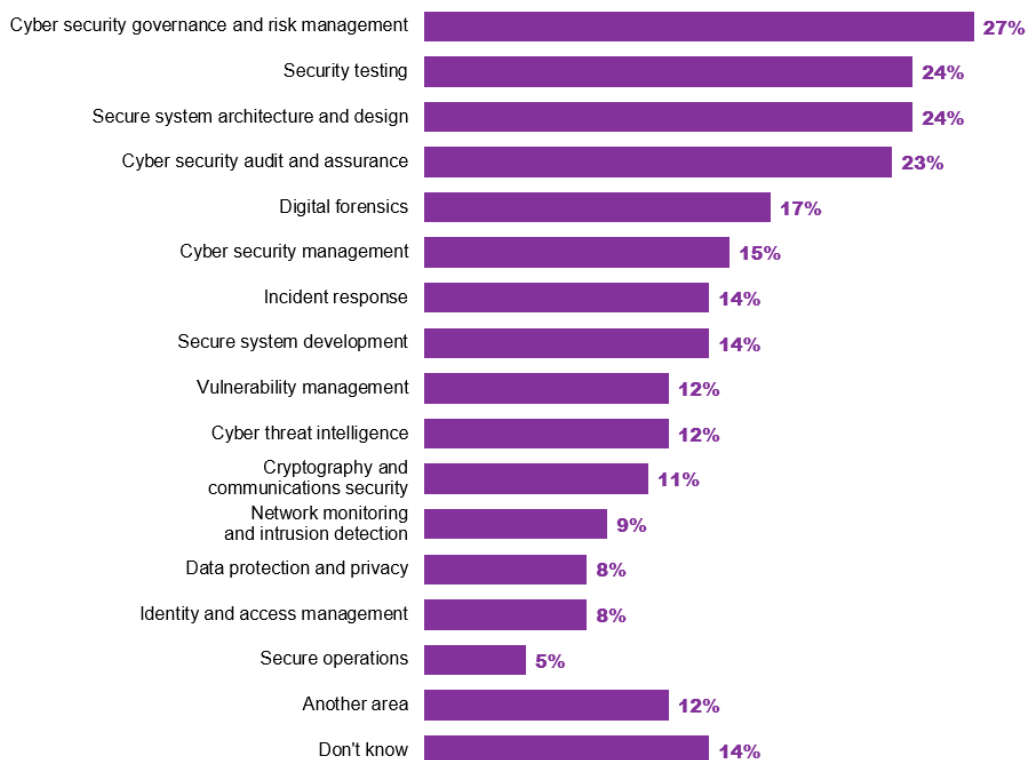
The drop in the number of cyber security sector employers highlighting hard-to-fill vacancies since the 2024 study, and in the number of hard-to-fill vacancies themselves, continue to indicate that the cyber security labour market is shifting from being a candidate's market to an employer's market. In a period of tougher competition for a smaller number of job vacancies, employers are potentially more able to identify and recruit the highest calibre candidates.

The roles and levels that were hard-to-fill

Cyber security businesses were asked to say in which specialisms they had incurred hard-to-fill vacancies (see Figure 6.13). The list of specialisms came from the [UK Cyber Security Council's Cyber Career Framework](#) (previously discussed in Chapter 2).

As Figure 6.13 shows, the top three specialisms which cyber security firms with hard-to-fill vacancies mentioned were governance and risk management, followed by security testing, and secure system architecture and design. Roles in security testing became harder to recruit for, compared to the previous study (16% in the 2025 study, vs. 24% in this study), as have secure system architecture and design roles (10% in the 2025 study, vs. 24% in this study). Qualitative insights on hard-to-fill vacancies are also discussed in Section 4.5 above.

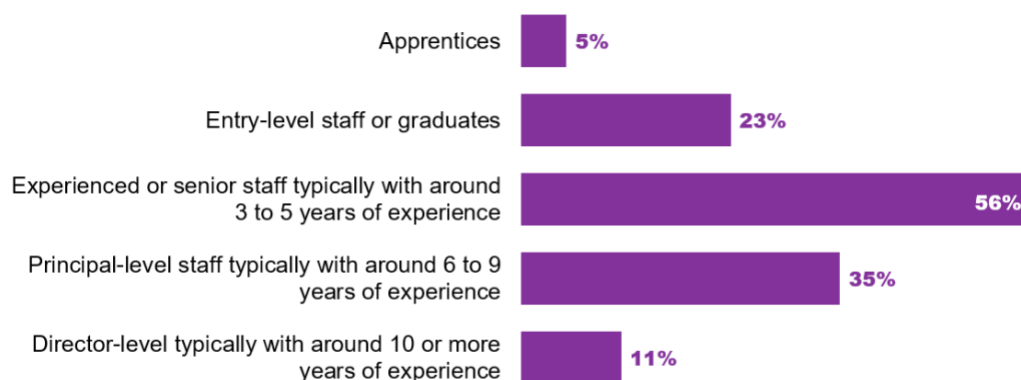
Figure 6.13: Percentage of UK cyber security businesses that have found it hard to fill job vacancies in the following specialisms, among those that had any hard-to-fill vacancies



Base: 66 cyber security businesses that had any hard-to-fill job vacancies in the 18 months prior to the survey

Finally, Figure 6.14 illustrates that most skills shortages continued to be in mid-level or more senior roles that require at least 3 years of experience. However, in the current study, principal level staff (those with around 6 to 9 years of experience) were more difficult to recruit (35%, vs. 16% in the 2025 study).

Figure 6.14: Percentage of UK cyber security businesses that have found it hard to fill job vacancies at the following levels, among those that had any hard-to-fill vacancies



Base: 66 cyber security businesses that had any hard-to-fill job vacancies in the 18 months prior to the survey
N.B. a further 2% said "don't know" at this question, which has not been included in the chart.

7 Conclusions

This year's findings on the UK cyber security labour market are set within the context of a number of policy and intervention programmes launched in 2025. Several new initiatives have been introduced since the previous report, including the [Government Security Profession](#) to develop public sector talent, the flagship [TechFirst programme](#) to improve diversity and skills within cyber security, as well as a schemes such as the [Cyber Access Network](#). This 2026 report provides an assessment of the landscape, revealing a challenging landscape with softened recruitment, increased staff turnover, and a rapid integration of AI which presents both opportunities and challenges for the talent pipeline.

The following are some of the key insights from this latest report:

A challenging labour market, with fewer businesses expecting to grow their workforce.

Recruitment expectations have softened significantly, with just 53% of firms expecting to grow their workforce in the next 12 months, a marked decline from 67% in the previous year. Respectively, 46% of firms now expected their workforce size to remain unchanged, up from 30% last year. Vacancy data and qualitative feedback also highlighted a slowing recruitment market. Furthermore, staff turnover as reported at the firm level (within the survey) has also increased from 12% to 14% in the 18 months prior to the survey, suggesting headcount reductions or freezes among many employers. There could be multiple reasons behind these shifts which are not directly evidenced in this research (e.g., changes in business spending on cyber security, increased recruitment costs, how employers are deploying new technologies, including AI, and increasing economic uncertainty in general).

Businesses continue to report skills gaps among specialist and senior level roles.

Despite challenging wider conditions and trends, many cyber security firms continue to recruit and demand talent. Over half (53%) of recruiting cyber security firms reported struggling with hard-to-fill vacancies. Principal level roles (those with around 6 to 9 years of experience) were significantly harder to fill this year – accounting for 35% of businesses with hard-to-fill roles versus 16% last year.

The qualitative work highlighted that despite a slowing market, there is still competition for the desired combination of technical and complementary skills. The skills in the highest demand have shifted slightly in the survey compared to previous years, with hard-to-fill vacancies most commonly being in Governance and Risk Management (27% of businesses finding roles hard to fill), Security Testing (24%), Secure System Architecture and Design (both 24%), and Audit and Assurance (23%). Demand for Secure System Architecture and Design roles has increased since the 2025 study (24%, up from 10%).

Progress on diversity is mixed. While neurodiversity is increasingly recognised among employers at a more junior level, barriers remain for women and other groups in reaching leadership positions.

The cyber sector workforce broadly remains less diverse than the wider UK workforce in terms of sex and disability, though broadly comparable on ethnicity; for example, 16% of the cyber security workforce was female compared to 48% of the UK average workforce, 9% were disabled compared to 18% of the UK workforce, whereas 19% were from ethnic minorities, compared to 16% of the UK workforce. These gaps widen significantly at senior levels, where the workforce is markedly less representative across all measures.

The qualitative research points to structural, not just historical, explanations for this. The underrepresentation of women in senior cyber roles was linked not only to a narrower pipeline at entry-

level, but to cultural barriers within organisations. These included assumptions about technical interests and, in some cases, a stated reluctance among some employers to appoint women to leadership positions. Notably, many firms acknowledged a lack of clear strategies for addressing this, suggesting these barriers are sometimes embedded and accepted rather than being actively tackled.

Recognition of neurodiversity in the sector has grown considerably. The estimated proportion of neurodiverse employees has risen to 22%, up from 9% in 2020. We note this may be a shift driven by improved awareness, openness to disclosure and willingness to self-identify, rather than a statistical change in the underlying workforce composition. Qualitative findings supported this, pointing to greater recognition and acceptance of neurodiversity among colleagues. However, this increased visibility has not yet translated into equal progression. Neurodiverse individuals continued to face barriers to progression into senior roles, often linked to assumptions about the interpersonal skills required for leadership.

Self-reported confidence in cyber security skills and capability has decreased across the wider UK economy, amidst increased awareness and concern around cyber security following several high-profile breaches.

The apparent basic skills gap among private sector businesses has widened, with 57% of firms lacking confidence in at least one basic cyber security task, up from 49% in the 2025 report. The reported advanced skills gap has also grown in some organisations, with 31% of the public sector reporting such a gap compared to 21% the previous year. Incident response remains a particular area of concern, with nearly half of businesses and charities (47% for both) lacking confidence in their ability to manage a cyber security breach.

However, this decline in self-reported confidence does not necessarily indicate reduced capability. It may instead reflect increased awareness in how organisations assess their own cyber security posture, driven in part by growing coverage of high-profile breaches, but also by an increased focus on areas such as supply chain security, risk management, and regulatory compliance. As the threat landscape evolves, this may make conditions more challenging for wider organisations.

Outsourcing of cyber security functions remains widespread, particularly in the public sector (69%) compared with private businesses (35%), with commonly outsourced functions including endpoint security, security information and event management (SIEM) and incident response. This use of specialist external providers may reflect a strategic approach to managing cyber risk, drawing on dedicated expertise and broadened provider capabilities.

Awareness of the UK Cyber Security Council (UKCSC) is high and its cyber security frameworks are valued, as is CyberFirst. In order to make the most impact, cyber security businesses want frameworks to be cost-effective and applicable to real-world situations.

Three-quarters (74%) of cyber security sector businesses were aware of the UKCSC. Its career framework was valued in the qualitative research for providing entry-level guidance. However, participants pointed out the ongoing practical challenge of making the framework applicable to the real world, where jobs span multiple specialisms. Views on the chartered professional standards remain mixed, as per last year. Cyber security businesses felt these could be even stronger as a value proposition if there was international recognition and they welcomed any attempts to reduce the cost burden for SMEs.

The government's CyberFirst initiative was spontaneously praised in qualitative discussions as a "perfect example" of how to bring education and industry together to build the talent pipeline. Awareness of

CyberFirst was also high in the survey, with nearly two-thirds of cyber security firms reporting that they were aware of this initiative (64%). Awareness of the successor TechFirst programme was lower, however, at 30%. Given that CyberFirst is ending, it will be important to reflect on the elements that were praised and ensure they are integrated into the new, broader TechFirst programme.

AI is driving demand for new skills and roles but may be narrowing down the traditional entry-level pipeline.

AI adoption across the cyber sector has accelerated. A total of 70% of cyber security firms reported staff using AI in their daily work, up from 53% in the previous study, and 73% expected their need for AI skills to increase over the next 12 months. Job vacancy data reflected this shift, with a 5 percentage-point increase in demand for AI skills across core cyber job postings (now 9% of postings), more than doubling compared to the previous year.

The AI security market itself is also growing. The [Cyber Security Sectoral Analysis 2026](#) found a 51% increase in the number of cyber security professionals employed in firms offering AI security, from 9,740 employees across 66 firms, to 14,720 across 111 firms.

This growth is expected to create new roles in areas such as AI governance, security engineering, and architecture, as well as increasing the importance of governance, risk, and compliance (GRC) functions in ensuring the data integrity of AI systems. However, qualitative feedback suggested that skills development in this area is often ad-hoc and self-led, with employers calling for more formal and regularly updated training frameworks.

A particular concern raised in the qualitative research was the direct impact of AI on junior roles. Entry-level positions, particularly in Security Operations Centres (SOCs) which have traditionally served as a crucial training ground, may be at risk of being displaced as agentic AI takes on more routine tasks. This creates a potential pipeline problem, as it limits the flow of junior talent to develop into the senior professionals of the future. This was stated more definitively than in previous studies, reflecting the strength of views gathered this year.

However, the increasing use of AI among bad actors means that the use of AI to identify, respond to, and mitigate attacks will become increasingly embedded. The findings also highlight that this will require sustained investment in tooling and compute alongside workforce development, rather than skills alone.

8 Annexes

Annex A: Graduate inflows into IT-related and cyber security professional roles

Table A.1: Estimated number of graduates moving into IT-related roles

Course type	Number of graduates	Proportion in full-time employment	Proportion in IT-related roles	Implied population
Cyber security	7,950	60%	95%	4,530
Other computer science	63,510	61%	85%	32,930
Total				37,460

Source: Perspective Economics estimates based on HESA Graduate Outcomes survey 2023/24 (2022/23 academic year) (Note: Graduate numbers refer to the 2023/24 academic year, applying 2022/23 GO proportions to these figures to find the implied population estimates.) N.B. student numbers are rounded to the nearest 10 to avoid disclosure and may not sum due to rounding.

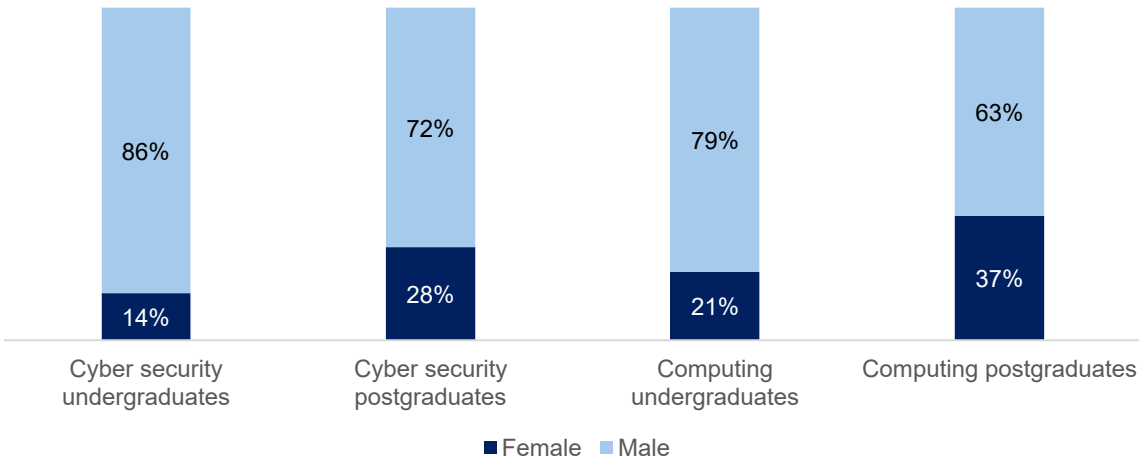
Table A.2: Estimated number of graduates moving into cyber security professional roles (SOC 2135)

Course Type	Number of Graduates	Proportion in full-time employment	Proportion in SOC 2135	Implied Population
Cyber security	7,950	60%	30%	1,431
Other computer science	63,510	61%	c.1%	387
Total				1,820

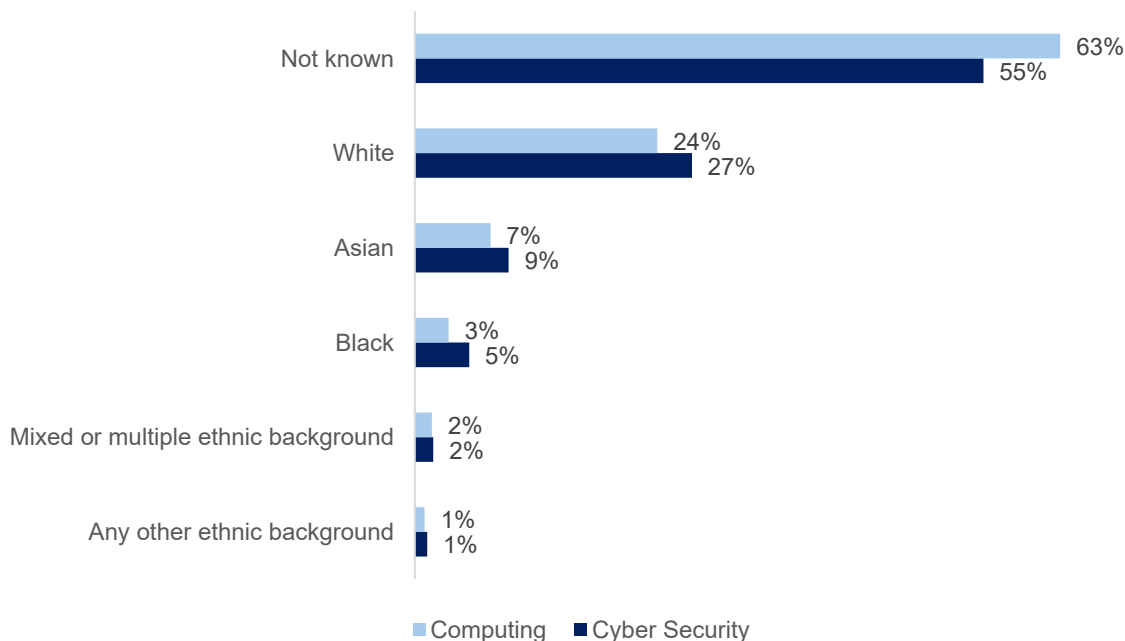
Source: Perspective Economics estimates based on HESA Graduate Outcomes survey 2023/24 (2022/23 academic year) (Note: Graduate numbers refer to the 2023/24 academic year, applying 2022/23 GO proportions to these figures to find the implied population estimates.) N.B. student numbers are rounded to the nearest 10 to avoid disclosure and may not sum due to rounding.

Annex B: Higher education student demographic profiles

Figure B.1: Sex of cyber security and computer science undergraduates and postgraduates (2023/24 academic year)

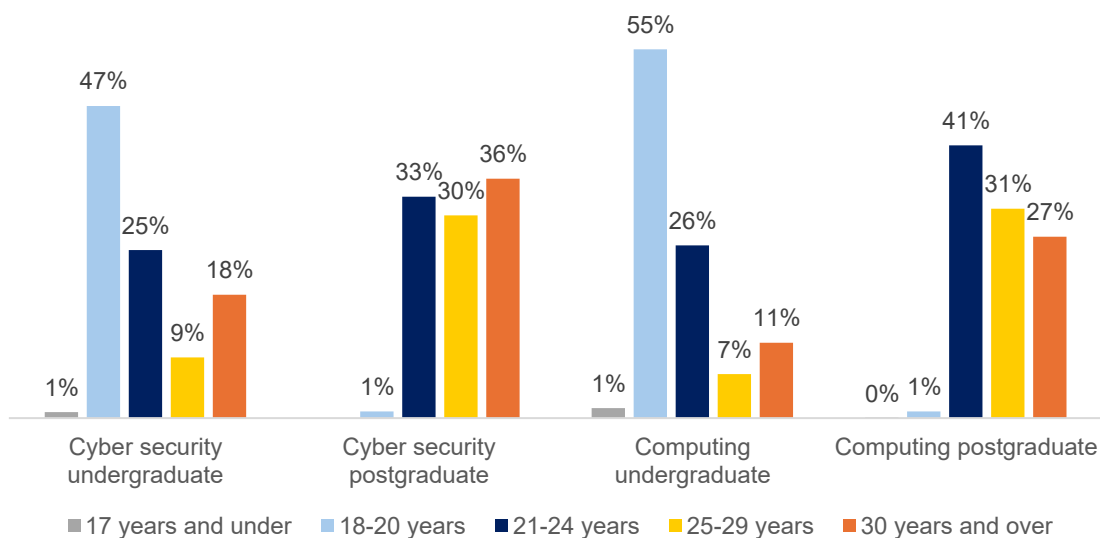


Source: HESA/Jisc data 2023/24
Bases: Cyber security undergraduates (3,410) and postgraduates (4,510); computer science undergraduates (27,570) and postgraduates (35,670)

Figure B.2: Ethnicity of cyber security and computer science graduates (2023/24 academic year)

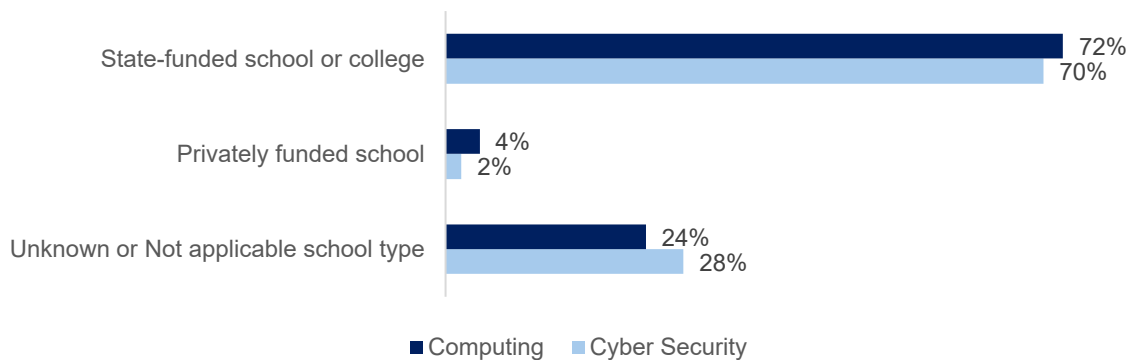
Source: HESA/Jisc data 2023/24

Bases 7,950 cyber security graduates; 63,510 computer science graduates

Figure B.3: Age of cyber security and computer science students (enrolled in 2023/24 academic year)

Source: HESA/Jisc data 2023/24 Bases: 24,770 cyber security students; 173,980 computer science students

Figure B.4: State school marker for cyber security and computer science students from the UK (enrolled in 2023/24 academic year)



Source: HESA/Jisc data 2023/24 Bases: 16,850 UK-domiciled cyber security students; 107,110 UK-domiciled computer science students

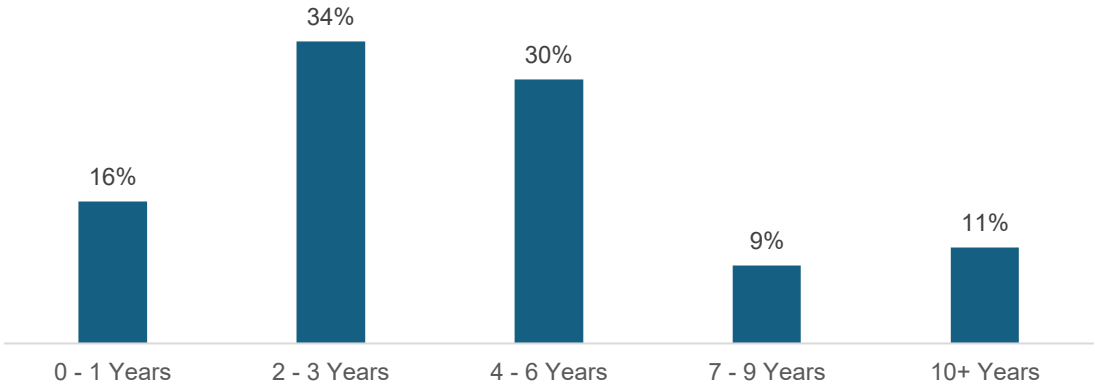
Annex C: Definition of core and cyber-enabled roles

The data across Chapter 4 refers to both “core cyber roles” and “cyber-enabled roles”. In certain charts in this chapter, both these groupings are combined to create an “all cyber roles” grouping.

- Core cyber roles are formally labelled or commonly recognised as cyber security jobs. They have a greater demand for skillsets and tools directly related to cyber security, such as information systems, cryptography, information assurance, network scanners, and security operations. In other words, 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.
- Cyber-enabled roles are not formally labelled or commonly recognised as cyber security jobs, but they still require cyber security skills. Alongside cyber security skills, they demand more general IT and business skills, such as project management, risk assessment, network engineering, SQL, system administration, and technical support. This might be because the job requires light touch knowledge and application of technical cyber security skills (e.g., for IT technicians or governance, regulation and compliance roles) or because the job role includes cyber security functions among other things (e.g., network engineers whose role includes but is broader than just network security). Typical job titles include Computer Support, IT Support Analyst and Applications Analyst.

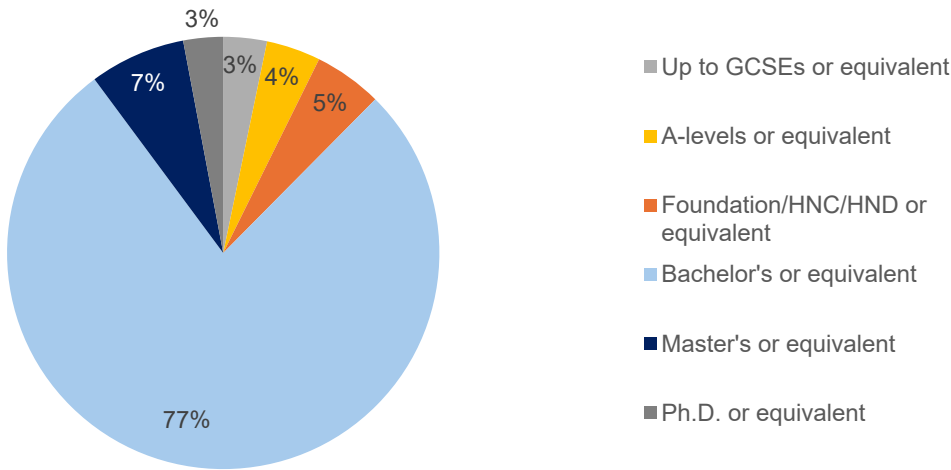
Annex D: Experience and qualifications requested in online cyber security job postings

Figure D.1: Percentage of core cyber job postings asking for the following levels of minimum experience (where any minimum requirement is identified)



Source: Lightcast. Bases: 10,566 online job postings for core cyber roles with minimum requirements listed from January to December 2025

Figure D.2: Percentage of core cyber job postings asking for the following minimum levels of education (where any minimum requirement is identified)



Source: Lightcast. Bases: 8,776 online job postings for core cyber roles with minimum requirements listed from January to December 2025

Annex E: Higher education courses and enrolments data

Table E.1: Breakdown of student enrolment and qualifiers in cyber security courses in UK HEIs (2022/23-2023/24)

Academic Year	Number of students enrolled		Number graduating	
	2022/23	2023/24	2022/23	2023/24
Undergraduate	14,620	16,480	3,120	3,430
Postgraduate	8,160	8,290	3,856	4,520
Total	22,780	24,770	6,980	7,950

Source: HESA/Jisc data (2022/23-2023/24)
N.B. student numbers are rounded to the nearest 10 to avoid disclosure and may not sum due to rounding.

Table E.2: Breakdown of student enrolment and qualifiers in computer science courses in UK HEIs (2022/23-2023/24)

Academic Year	Number of students enrolled		Number graduating	
	2022/23	2023/24	2022/23	2023/24
Undergraduate	107,330	114,730	24,950	27,760
Postgraduate	59,400	59,250	28,980	35,750
Total	166,730	173,980	53,930	63,510

Source: HESA/Jisc data (2022/23-2023/24)

N.B. student numbers are rounded to the nearest 10 to avoid disclosure and may not sum due to rounding.

Annex F: Digital apprenticeships data**Table F.1: Number of Digital apprenticeships in England (2023/24 academic year)**

	Starts	Achievements	Enrolments
Intermediate Apprenticeship	low	low	low
Advanced Apprenticeship	10,460	5,310	20,600
Higher Apprenticeship	11,500	5,040	22,150
Degree Apprenticeship	4,110	1,840	10,530
Total	26,060	12,190	53,280

Source: Department for Education [apprenticeships data](#)

N.B. numbers are rounded to the nearest 10 to avoid disclosure and may not sum due to rounding.

Table F.2: Number of Digital apprenticeships in England (2024/25 academic year)

	Starts	Achievements	Enrolments
Intermediate Apprenticeship	low	low	low
Advanced Apprenticeship	12,430	6,370	23,080
Higher Apprenticeship	14,020	5,850	25,810
Degree Apprenticeship	4,960	2,260	12,370
Total	31,410	14,490	61,250

Source: Department for Education [apprenticeships data](#)

N.B. numbers are rounded to the nearest 10 to avoid disclosure and may not sum due to rounding.

Table F.3: Number of starts in Digital apprenticeships in England by sex (2024/25 academic year)

Detailed Level	Framework/Standard	Female	Male	Total
3	Cyber Security Technician (ST0865)	10	20	30
3	Data Technician (ST0795)	4300	3300	7600
3	Digital Device Repair Technician (ST0682)	low	30	30
3	Digital Support Technician (ST0120)	780	910	1690
3	Information Communications Technician (ST0973)	300	2200	2500
3	Infrastructure Technician (ST0125)	low	low	low
3	IT Solutions Technician (ST0505)	10	70	80
3	Network Cable Installer (ST0485)	10	130	140
3	Radio Network Technician (ST0757)	30	200	230
3	Software Development Technician (ST0128)	40	110	150
3	Unified Communications Technician (ST0130)	low	low	low
4	Applications Support Lead (ST0949)	10	40	50

4	Business Analyst (ST0117)	1690	1930	3620
4	Cyber Intrusion Analyst (ST0114)	low	low	low
4	Cyber Security Technologist (2021) (ST1021)	70	350	420
4	Cyber Security Technologist (ST0124)	low	low	low
4	Data Analyst (ST0118)	3120	4010	7130
4	DevOps Engineer (ST0825)	50	170	220
4	Digital Accessibility Specialist (ST0863)	20	10	30
4	Digital Community Manager (ST0345)	low	low	low
4	Digital Forensic Technician (ST1343)	10	10	20
4	Digital Product Manager (ST0964)	120	110	230
4	Network Engineer (ST0127)	60	910	970
4	Software Developer (ST0116)	170	440	610
4	Software Tester (ST0129)	30	70	100
4	Unified Communications Trouble Shooter (ST0131)	low	low	low
5	Data Engineer (ST1386)	130	310	440
5	Digital Learning Designer (ST0974)	110	60	170
6	Creative Digital Design Professional (Integrated Degree) (ST0625)	40	30	70
6	Cyber Security Technical Professional (Integrated Degree) (ST0409)	10	50	60
6	Data Scientist (Integrated Degree) (ST0585)	90	190	280
6	Digital and Technology Solutions Professional (ST0119)	670	1670	2340
6	Digital User Experience (UX) Professional (Integrated Degree) (ST0470)	30	10	40
6	Machine Learning Engineer (ST1398)	20	140	160
7	Advanced Digital Forensic Professional (ST1409)	low	10	10
7	Artificial Intelligence (AI) Data Specialist (ST0763)	200	600	800
7	Digital and Technology Solutions Specialist (Integrated Degree) (ST0482)	360	860	1220
7	Game Programmer (ST0953)	low	low	low
Total	Total	12,490	18,920	31,410

Source: Department for Education [apprenticeships data](#)

N.B. numbers are rounded to the nearest 10 to avoid disclosure and may not sum due to rounding.

N.B. 'low' indicates the number is below 10.

Our standards and accreditations

Ipsos' standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a "right first time" approach throughout our organisation.



ISO 20252

This is the international specific standard for market, opinion and social research, including insights and data analytics. Ipsos UK was the first company in the world to gain this accreditation.



Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos UK endorse and support the core MRS brand values of professionalism, research excellence and business effectiveness, and commit to comply with the MRS Code of Conduct throughout the organisation & we were the first company to sign our organisation up to the requirements & self-regulation of the MRS Code; more than 350 companies have followed our lead.



ISO 9001

International general company standard with a focus on continual improvement through quality management systems. In 1994 we became one of the early adopters of the ISO 9001 business standard.



ISO 27001

International standard for information security designed to ensure the selection of adequate and proportionate security controls. Ipsos UK was the first research company in the UK to be awarded this in August 2008.



The UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (DPA)

Ipsos UK is required to comply with the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA). These cover the processing of personal data and the protection of privacy.



HMG Cyber Essentials

Cyber Essentials defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet. This is a government-backed, key deliverable of the UK's National Cyber Security Programme. Ipsos UK was assessed and validated for certification in 2016.



Fair Data

Ipsos UK is signed up as a "Fair Data" company by agreeing to adhere to twelve core principles. The principles support and complement other standards such as ISOs, and the requirements of data protection legislation.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos.com/en-uk
<http://twitter.com/IpsosUK>

About Ipsos Public Affairs

Ipsos Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.

