March 2021

Understanding the Cyber Security Recruitment Pool

Research Report for the Department for Digital, Culture, Media and Sport

Harry Williams, James Kearney, and Gabriele Zatterin, Ipsos MORI

Sam Donaldson, Perspective Economics

David Crozier, Centre for Secure Information Technologies, Queen's University Belfast

Dr Jason Nurse, University of Kent

Ipsos MORI

Queen's University Belfast | CSIT Centre for Secure Information Technologies

Department for
Digital, Culture
Media & Sport

Perspective Economics

Contents

Executive Summary

Introduction

Ipsos MORI and Perspective Economics have been commissioned by the Department for Digital, Culture, Media and Sport (DCMS) to undertake research to quantify and provide understanding of the cyber skills recruitment pool in the UK. The research aims to gain a better understanding of the cyber skills recruitment pool in the UK, its size and geographic location, the types of skills and experience that are prevalent in the pool and recommendations on how employers can effectively recruit from the pool.

Key Findings

Overall, this research considers the estimated size of the total UK cyber security workforce, and the size of the UK cyber recruitment pool. These are estimated by Ipsos MORI and Perspective Economics, based upon a review of existing literature and wide range of labour market datasets.

These estimates are used to inform the potential scale of interventions that might be required to help address the perceived shortage of cyber security talent within the UK (that could feasibly enter employment within the next twelve months). The key quantitative findings are below:

- The current UK cyber security workforce currently has an estimated 98,000 (low) – 171,000 (high) employees. We take the mid-point for modelling purposes (i.e. 134,500 individuals);

- The demand for cyber security professionals has grown by an average of 14 percent per annum since 2016. In the most recent year, it has grown by nine percent. This implies that the UK cyber security workforce would need to grow by approximately 12,000 people per annum (to meet expected demand). However, we do recognise that this assumes a direct relationship between demand and employment (which may be partially affected by processes such as automation and labour costs);

- The cyber security workforce is also losing approximately four percent of staff each year to retirement or exiting to other sectors. We estimate that this consists of approximately 4,000 – 7,000 (mid-point of 5,500) people each year;

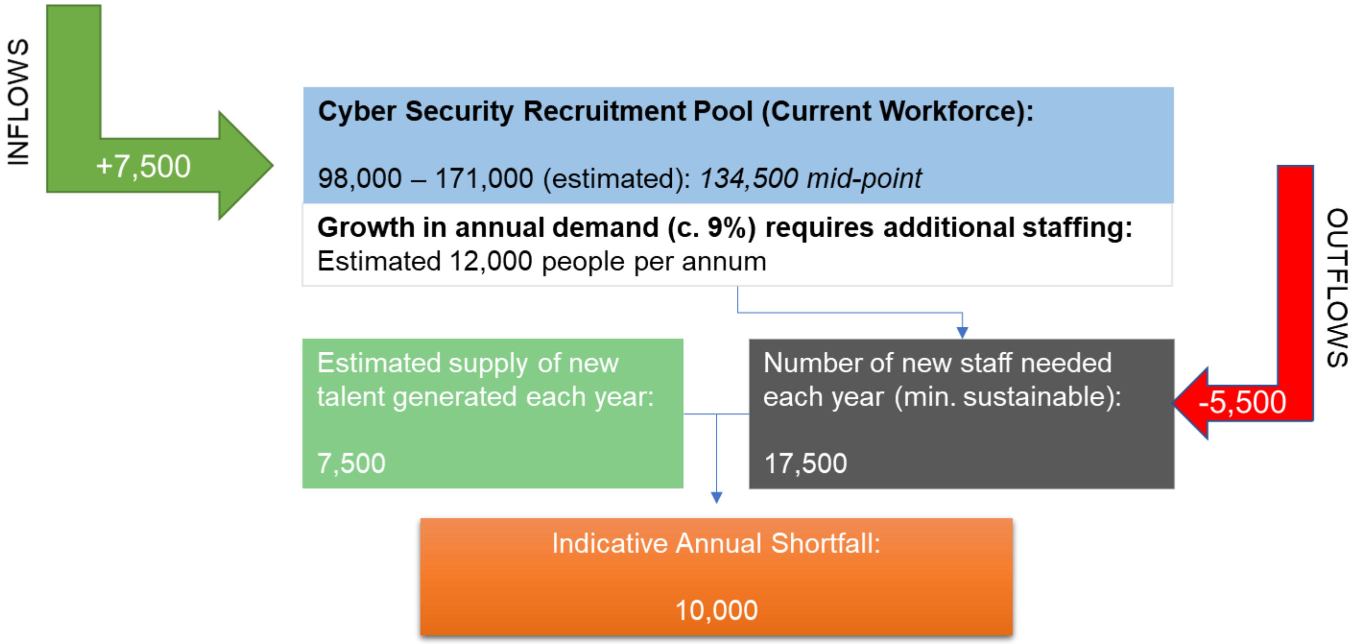
- In total, this implies that the UK cyber security workforce needs to attract at least 17,500 people each year to meet both new demand and replace lost workers. This broadly aligns with the Cyber Skills in the UK Labour Market research, which indicates there were over 33,000 online job vacancies posted by employers in the UK seeking core cyber security talent in 2020.

- With respect to inflows, we estimate that there are approximately 7,500 **new** individuals entering into a cyber security career each year. This includes approximately 4,000 UK university graduates (undergraduate and postgraduate level) entering employment in cyber security roles, up to 2,500 undertaking career conversion, re-training, or entering the UK pool elsewhere, and up to 1,000 involved in apprenticeships in cyber security. This figure could be increased in the future through re-training initiatives, support with certifications and skills, and potentially expansion of the volume enrolled in higher and further education courses;

- This implies that the UK should be attracting c. 17,500 new people each year into cyber security employment to meet demand but is currently only generating c. 7,500 in new supply. **This suggests an annual shortfall (2021) of c. 10,000 people**, and this is in addition to existing perceived shortage of talent currently, as well as potential for further demand to increase in future. This highlights that the cyber skills shortage is an ongoing challenge that needs to be addressed rapidly in order to mitigate some of the resulting issues (e.g. loss of talent and experience, challenges in staff retention and productivity, risk of staff burnout etc.);

- This also suggests that, left untreated, the extent of the shortfall will continue to worsen, as cyber security remains an area where demand for talent exceeds supply; and

Figure ES1: Summary of Estimated Cyber Security Recruitment Pool, Workforce, Inflows and Outflows


INFLOWS
+7,500
Cyber Security Recruitment Pool (Current Workforce):
98,000 – 171,000 (estimated): 134,500 mid-point
Growth in annual demand (c. 9%) requires additional staffing:
Estimated 12,000 people per annum
Estimated supply of new talent generated each year:
7,500
Number of new staff needed each year (min. sustainable):
17,500
-5,500
OUTFLOWS
Indicative Annual Shortfall:
10,000

Source: Perspective Economics Estimation

- However, we do consider the use of regional, national, and online re-skilling initiatives – if scaled, could considerably tackle this shortfall with sufficient funding and support. Further, these initiatives are often also useful in tackling barriers to entering the cyber security field (e.g. through provision of initiatives targeted to those with neurodiversity, those under-represented in the industry e.g. women, and those from ethnic minority backgrounds, and promoting cyber as a career to those previously in aligned pathways e.g. military and law enforcement).

We also undertook qualitative research with 25 stakeholders. These included cyber security employers, training providers, recruitment agents and employees. Employers stated they were struggling to fill roles, especially specialist roles for employees with 3-5 years experiences. However, training providers and recruitment agents believed the level of demand for courses and roles are high. This implied that there are not enough suitable candidates in the pool. A low indicative ratio of high-quality applicants being seen as suitable to their role further backed this up.

Other stakeholders felt that there was sufficient quantity in the pool. Some consultees felt that employers were trying too hard to find the perfect candidate. They mentioned that there were entry-level candidates in the pool from other areas, such as the military. These groups had a strong set of soft skills, such as leadership, project management and communication skills. They felt they were able to learn technical skills via on the job training. Other barriers to entry were noted, with poor awareness amongst the wider population of cyber security, and unsuitable recruitment methods stopping some candidates from finding roles. Consultees suggested the government could help increase quantity and quality by increasing education and information on cyber security in schools.

There was also a lack of diversity in the pool. Recruitment and interview processes, unsuitable working environments and inaccessible training made it difficult for neurodiverse candidates to enter the pool, and once in it, find a role. There are specialist training providers attempting to alleviate this. However, government can help alleviate this by facilitating relationships between training providers, autism charities and employers, and by setting an example themselves in how to improve neurodiversity in the workplace.

When it came to demographic diversity, women were under-represented at all levels in the pool, with ethnic minority candidates less successful in getting roles at leadership level. At senior levels, blind recruitment and transparent promotion processes could help alleviate this, with positions currently heavily reliant on networking. Consultees felt the government could advise employers on this, as well as lead the way in making them adhere to standards if bidding for government contracts. There was also a perception issue amongst women who could potentially enter the pool. Consultees felt the government can help alleviate this by helping educational institutions make it clear what a career in cyber truly entails.

Those with lower educational qualifications were also under-represented, with suitable candidates tending to be educated to degree level. Government could help by improving and increasing further education courses and apprenticeships. Training providers were looking to help improve their offering to diverse groups and those living in deprivation by targeting their offering with links to charities and improving overall accessibility. However, they felt government could help fund their courses, particularly where they were offered for free or at a low cost.

Despite concerns about diversity and getting candidates with strong complimentary skills into roles, there was broad agreement that there is a low level of technical expertise relative to demand. This was evidenced by employers stating that specialist roles such as penetration testers or firewall engineers were most difficult to fill. Internal on the job training by employers for individuals with strong complementary skills and encouraging employees to seek external accreditation could help alleviate this in the short term. In the long term more bespoke FE courses and apprenticeships are required.

Overall, there was a sense that the future of the recruitment pool is positive and that current government interventions, such as CyberFirst, are working. They felt that the increase in digital employment has made training more accessible, and will broaden the pool both in terms of raw numbers, and the wider diversity of the pool. They felt that successful education interventions and reskilling would mean candidates come from a greater range of educational pathways, and that remote working would help improve the working environment for women.

The coronavirus pandemic further provides an opportunity. There was a sense that it could be used as a catalyst for the government to increase their role in reskilling the wider workforce in cyber security. This could be used to help those who are unemployed or furloughed because of the pandemic, with a perception amongst new entrants that cyber security offers stable employment. They could also use this to further help reskill groups already targeted, such as those leaving the military.

Recommendations

Theme 1: Boosting the supply of new talent, and recognising the role of cyber security roles in driving economic recovery

- **Recommendation 1:** This research highlights that the traditional cyber recruitment pool (e.g. graduates and experienced staff) is much smaller than some employers might recognise. In order to address the shortage of cyber security talent, we recommend that alternative and innovative routes to a cyber security career need to be clear, funded and accelerated. These should also be targeted to a diverse range of individuals.

- **Recommendation 2:** The economic impact of the COVID-19 pandemic has demonstrated the critical role of retraining and upskilling. The current economic conditions mean that there is much greater demand for engaging in retraining initiatives, particularly among individuals that have faced redundancy or reduced hours of working in existing roles. There is a window of opportunity for the UK to rapidly invest in cyber security retraining initiatives, courses, and learning models to increase future productivity.

- **Recommendation 3**: Leading by example. Throughout this research, we note several examples of good practice in increasing the supply of new talent into the cyber security industry. We recommend further activity should be undertaken to better promote the understanding and take-up of such initiatives. This could include greater public sector uptake of such schemes (including retraining) where possible, and the sustained promotion of 'what works' across industry.

Theme 2: Supporting pathways into cyber security employment

- **Recommendation 4:** Time to scale up. As noted, there are several pilot and early-stage initiatives that appear to have gained traction in improving diversity and access to cyber security training and entry-level employment. There is now a strong mix of examples across further and higher education, private training initiatives, bootcamps, employer-led training models, and academies targeted at retraining particular groups such as neurodiverse and former Armed Forces. We recommend that further support to help successful pilot initiatives scale-up faster (and to do so across the UK) would be particularly welcome given the identification of the current cyber security skills gaps.

- **Recommendation 5:** We further recommend that in addition to supporting supply-based initiatives, government and training providers should work closely with industry at a regional level to help match skills with local demand. For example, these models should ideally have a clear outcome whereby those supported can enter a role with a local employer in need of such skills. We note that this should also be considered as an important component of the Levelling Up Agenda, as the type of demand for cyber security professionals can vary across the UK, and there is significant potential to increase regional productivity given the longer term salary premium associated with cyber security roles.

- **Recommendation 6:** The nature of cyber security roles has expanded in recent years. We recommend that addressing the cyber security recruitment gap will also require providing and supporting other digital skills pathways, and supporting individuals move into highly complementary roles such as Governance, Risk and Compliance roles. In this respect, improved segmentation, and definition of what skills (including less technical') and type of 'cyber security career' an individual could have may help to ease some of the shortage, and better improve allocation of resources.

Theme 3: Undertaking workforce planning to meet the needs of the cyber security industry today, and into the future

- **Recommendation 7:** We recommend that government further explores a Capacity Review of Higher Education Institutions (HEIs) in the UK with respect to cyber security provision. Whilst this study has explored the number of students graduating within 'Cyber Security' and Computer Science courses, a capacity review of undergraduate and postgraduate cyber provision may be useful to understand if and how HEIs may be able to increase supply (if at all, and without impacting quality) of cyber security teaching, and to further understand the prevalence of cyber security modules across all degree pathways.

- **Recommendation 8:** Building on this theme, we would also recommend that a 'workforce planning' approach should be explored at regional and national levels, particularly by Local Enterprise Partnerships (LEPs) and devolved equivalents. This research has estimated a UK based shortfall in the number of new entrants to the recruitment pool. However, this availability of supply will vary regionally, as will employer demand. Improving alignment between regional skills supply and employer demand, and understanding regional growth ambitions should help regions to make informed decisions and investments to support retraining.

  This research has suggested that across the UK, interventions to the scale of generating an additional c. 300 people (in cyber security) per 1m of working age population (in addition to existing supply) would help to address this annual shortfall. We recommend that each region, particularly those with high density of cyber security employment explore this in further depth.

Theme 4: A strong focus on improving diversity in supply

The Cyber Skills in the UK Labour Market (2021) explores themes of diversity within the cyber security labour market. However, the following recommendations are included below:

- **Recommendation 9:** Retraining initiatives to support individuals get into cyber security can be life changing. They can allow people to learn new skills, meet new people, and increase their earning power. However, we recommend that such initiatives should place a sustained emphasis where possible, on improving accessibility to all extents. Whilst many individuals may want to retrain, the barriers to undertaking such initiatives such be continually explored. For example, this might include provision of financial support (e.g. direct, or support with child-care) to enable the take-up of the training place.

- **Recommendation 10:** As set out in the research, whilst there have been a number of initiatives aimed at improving diversity within the industry, there are still significant issues reflected in the inflows of new talent (e.g. female take-up of cyber security courses remains low). We recommend that these figures are closely monitored in future years, alongside the continued promotion of schemes such as CyberFirst.

Acronyms Table

The following table sets out some of the acronyms used within this report:

Acronym	Description
(ISC)2	International Information System Security Certification Consortium
ACE-CSE	Academic Centres of Excellence in Cyber Security Education
ACE-CSR	Academic Centres of Excellence in Cyber Security Research
BTEC	Business and Technology Education Council
CISO	Chief Information Security Officer
CSIIF	Cyber Skills Immediate Impact Fund
CTP	Career Transition Partnership
CyBOK	Cyber Security Body of Knowledge
DCMS	Department for Digital, Culture, Media and Sport
FE	Further Education
FTE	Full Time Equivalent
GCSE	General Certificate of Secondary Education
GVA	Gross Value Added
HE	Higher Education
HEI	Higher Education Institution
HESA	Higher Education Statistics Agency
MOD	Ministry of Defence
MOOCs	Massive Open Online Courses
NCSC	National Cyber Security Centre
NVQ	National Vocational Qualifications
PG	Postgraduate
PhD	Doctor of Philosophy
SOC	Standard Occupational Classification
STEM	Science, Technology, Engineering, and Mathematics
UG	Undergraduate

1 Introduction

Ipsos MORI and Perspective Economics have been commissioned by the Department for Digital, Culture, Media and Sport (DCMS) to undertake research to quantify and provide understanding of the cyber skills recruitment pool in the UK. The research aims are to gain a better understanding of the cyber skills recruitment pool in the UK, its size and geographic location, the types of skills and experience that are prevalent in the pool and recommendations on how employers can effectively recruit from the pool.

1.1 Research Objectives

The objectives of the study are to:

- Provide a quantified estimate of the size of the cyber security recruitment pool for advanced cyber security skills, specifically the top shortage gaps identified in the Labour Market Survey including penetration testing, forensic analysis, security architecture and threat intelligence. This includes a disaggregation by factors including: Levels of experience (entry level, senior staff, principal level staff and director level) and skill set; Geography (nation / region of the UK); and diversity (including gender, ethnicity, sexual orientation/sexuality and if possible, neurodiversity and socioeconomic diversity) where possible.

- Develop a greater understanding of:

  - Individuals based in other sectors with the required skills, their career stage and the sectors they currently work in;

  - The skills sets (breadth and depth) of those that are in the pool, including the advanced cyber security skill areas identified above;

  - The diversity or lack of diversity present within the recruitment pool;

  - The geographic location of people in the pool;

  - The impact events such as the coronavirus pandemic and EU Exit have had or may potentially have on the recruitment pool; and

- Identify key lessons and recommendations on what government and industry can do to ensure the recruitment pool can serve the needs of prospective employers.

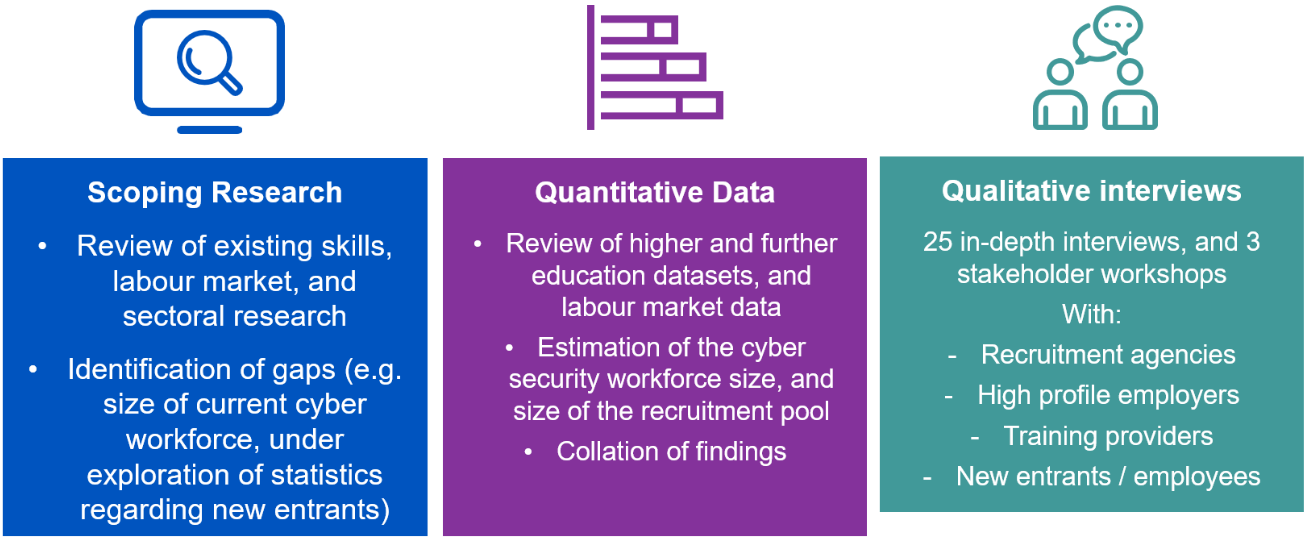
1.2 Methodology and Sources

This research intends to build on the current evidence base and provide a detailed understanding of the cyber security recruitment pool in the UK, including identifying how many people are in the pool, what types of skills and experience they have, and where they are dispersed geographically. This is new research without an established methodology to follow.

As such, this research focuses on the current recruitment pool (people eligible for employment) and those about to enter it in the short term (e.g. finishing relevant cyber education or training courses in the next 12 months). It also considers those undertaking relevant apprenticeships and, where possible, incorporate those leaving military service who may have relevant or transferable skills.

The research outputs from this piece of work are intended to inform national cyber security skills programs of activity.

Figure 1.1: Methodology Summary



Scoping Research

- Review of existing skills, labour market, and sectoral research
- Identification of gaps (e.g. size of current cyber workforce, under exploration of statistics regarding new entrants)

Quantitative Data

- Review of higher and further education datasets, and labour market data
- Estimation of the cyber security workforce size, and size of the recruitment pool
- Collation of findings

Qualitative interviews

25 in-depth interviews, and 3 stakeholder workshops

With:

- Recruitment agencies
- High profile employers
- Training providers
- New entrants / employees

1.3 Interpretation of qualitative data

The qualitative findings offer 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 examples or insight are highlighted, this is to illustrate findings that emerged more broadly across multiple interviews. These examples are not intended to be statistically representative of the wider population of UK organisations.

1.4 Acknowledgements

The authors would like to thank all the training providers, employers, employees and recruitment agents who took part in the interviews. We would also like to thank the Cyber Security Skills and Professionalisation Team at DCMS for their project management, support and guidance throughout the study.

2 Rapid Evidence Review

The cyber security landscape, with respect to definition, scope, and inclusion of job roles is complex. There are varying definitions and views as to what constitutes a cyber security job role or employer, with respect to skills required and technicality of the role.

However, a common thread within existing research exploring the cyber security labour market is that there is a known supply shortage or misalignment in the labour market. Employers continue to cite the challenge in recruiting and retaining suitably skilled cyber security professionals in the UK (and globally).

The first stage of this research was to undertake a rapid evidence review. This examines recent literature exploring the cyber security skills shortage, albeit focusing upon **supply** factors. This includes papers or datasets that explore:

- Known supply shortages in the cyber security labour market;
- Initiatives to improve or address supply shortages (and how these have worked where known); and
- Existing data demonstrating why and where supply shortages exist, and how this compares with respect to location, type of role, and diversity / access.

Just under one hundred sources relevant to the **supply side** were identified. However, in line with expectations and as with the previous rapid evidence review for the cyber skills study, the evidence overwhelmingly demonstrates a cyber security skills shortage.

In this respect, the focus the research is based upon understanding:

- **The volume of potential cyber security talent in the UK** (and extent to which this could be potentially subject to recruitment within the next twelve months);
- **How this talent (supply) aligns with employer demand** (and to what extent wider trends may impact the extent of the cyber skills shortage);
- **What initiatives work well in improving cyber security workforce availability** (with respect to volume, but also efficiency – e.g. reducing burnout, or improving allocation of tasks); and
- **Which skills areas are the gaps most pronounced** – and what impact this may have upon employers? (e.g. impact on ability to manage current workloads, secure market growth, or combat threats etc).

Further, the literature review also demonstrates there is considerable breadth in estimation of:

- **The size of the current cyber security workforce:** As there is no formal measurement (e.g. Standard Occupational Classification, SOC[1]) of the number of people working in a cyber security related role, there is variation in estimates of the number of people working in a cyber role in the UK. These include the Cyber Sectoral Analysis (2021) (46,683 estimated FTEs (Full Time Equivalents), focused on cyber firms only), Tech Partnership (2017, 58,000 FTEs), and ISC[2] (289,000 professionals). This highlights the need to consider roles across sectors (private, public and third

[1] True when research was undertaken. Cyber security professionals will be subject to SOC code classification (SOC2020).

sector), consider the role of contractors / freelancers, and also to consider the extent to which a role meets a defined criteria for being a 'cyber security role' – e.g. does it require sufficient alignment to a knowledge area, or job title?

- **The volume of the cyber security skills shortage (usually measured by 'unfilled vacancies'):** There is extensive literature citing the 'global shortfall' of cyber security jobs (ISC^2 estimated 3.5 million skills shortages globally by 2021). These estimates will be aligned to the Burning Glass vacancy data and considers the extent to which jobs were 'not posted' due to employer perception of challenges to fill these roles.

- **The volume of potential entrants that could address the skills shortages**: Within the literature (and the workshop discussion) there was a significant discrepancy between the volume of those studying cyber security courses (set out in Section 3) and then the wider estimates of those who **could** potentially be either trained then move into an entry-level cyber role, or commence immediately (and learn on the job etc). However, there is some expressed agnosticism regarding potential entrants having a specified qualification. For example, within the workshop, one attendee mentioned 'problem solving' as the key-skill.

  This highlighted the need for this research to be sufficient tailored to define what constitutes the 'cyber recruitment pool' (e.g. sufficient alignment to known qualifications or skills frameworks) without omitting potential for measuring broader entrant routes (e.g. career conversion, or non-STEM (Science, Technology, Engineering, Maths) graduates undertaking a bespoke academy or training course focused on cyber skills or retraining). This has ultimately informed the quantitative estimates, and the qualitative research approach.

2.1 Defining a Cyber Security Role

Within the Cyber Security Skills in the UK Labour Market (2020) research, cyber security roles are split into two groups, 'core' and 'enabled':

- **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 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 is broader than just network security). Typical job titles include Computer Support, IT Support Analyst and Applications Analyst.

However, the report also notes that both core and cyber-enabled job roles typically require a mix of technical and non-technical cyber security skills. Therefore, these cannot simply be differentiated as technical vs. non-technical jobs in cyber security.

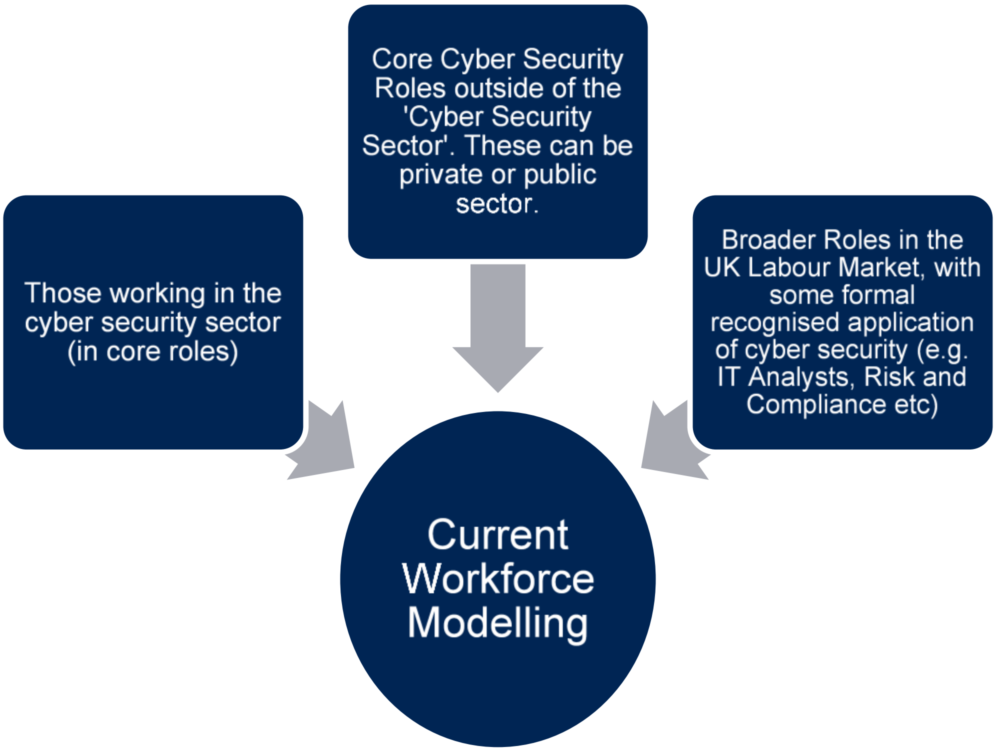
The rationale for identifying and classifying potential cyber security roles in the UK economy is that, there is no formal definition that exists of a cyber security role. The UK SOC2010 does not include cyber security roles in the same way it does for other IT professions. Whilst this will change in future, there is still subjectivity regarding what does or does not constitute a cyber security role.

Within the analysis presented in this report, the number of current core and enabled cyber security roles in the UK economy will be estimated, in addition to the number of potential entrants to the recruitment pool. It is recognised that these estimates are informed by known market conditions (e.g. number of employers, typical prevalence of qualifications) – however, there is notable difference between some roles within the cyber security sphere. For example, a Penetration Tester will require different skillsets and / or qualifications / certifications to a Cyber Risk Analyst.

2.2 Measuring the Existing Workforce

Prior to understanding the size and scale of the cyber security recruitment pool, it is important to consider the size of the existing workforce. We consider there to be three distinct[2], but complementary, areas for consideration within the research.

Figure 2.1: Groups included in the research


Core Cyber Security Roles outside of the 'Cyber Security Sector'. These can be private or public sector.
Those working in the cyber security sector (in core roles)
Broader Roles in the UK Labour Market, with some formal recognised application of cyber security (e.g. IT Analysts, Risk and Compliance etc)
Current Workforce Modelling

Subsequently, the research team sought to identify a range of current estimates for the size of the cyber security workforce in the UK (and internationally). There is a wide range of literature citing the perceived 'gap' in the number of information security / cyber security professionals globally; however, there is less consistency regarding the estimation of the current size of the workforce involved in cyber security.

This is due to the challenges that exist in defining and measuring the prevalence of cyber security roles in the economy. Firstly, there is no shared or agreed definition of a cyber security role under a formal structure

[2] Contractors are not omitted from this analysis, although contractors are not easy to identify in secondary datasets.

(such as SOC2010), and secondly, there are varying methodologies that exist to try to inform and estimate the size of this population.

The following studies provided the research team with a range of estimates to help inform the current understanding of the cyber security workforce, and therefore aid in modelling the potential size and scale of the cyber recruitment pool.

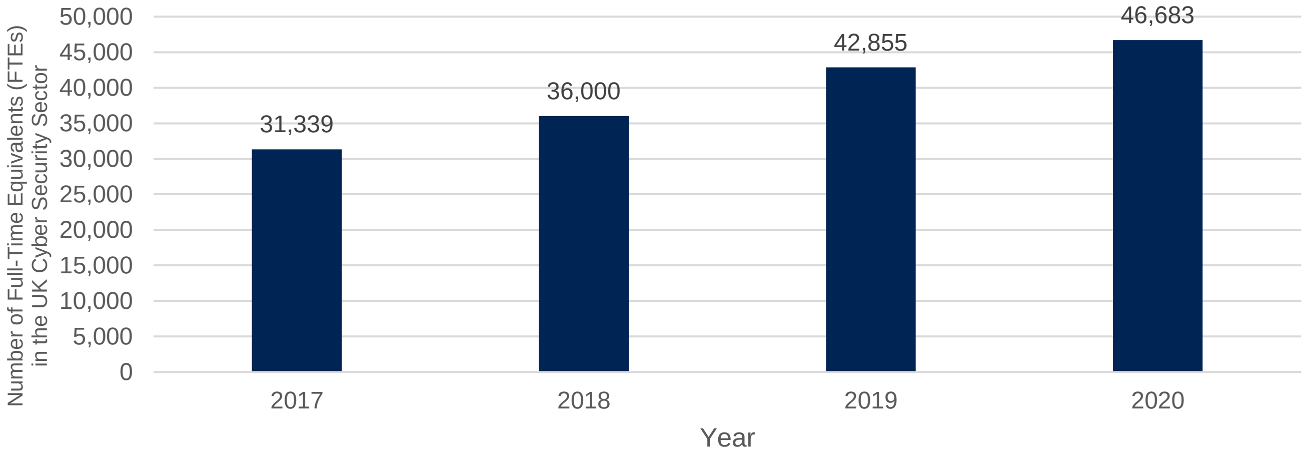
2.2.1 DCMS Cyber Security Sectoral Analysis

DCMS undertakes annual analysis of the size and scale of the UK cyber security sector, including analysis of the number of businesses in the UK offering cyber security products and services (to market), and their respective revenues, Gross Value Added (GVA) and employment.

The employment analysis provides an indication of the number of full-time equivalents (FTEs) working within registered companies that provide cyber security products and services in the private sector. However, it does not capture those working in cyber security roles within contract or freelance roles, those working within public sector bodies (including universities or further education institutions), or organisations that are not considered ‘cyber security providers’ but do employ dedicated staff for cyber security roles e.g. Chief Information Security Officers (CISOs) within financial institutions.

In this respect, it only covers employment within identified providers of cyber security products and services registered in the UK.

Figure 2.2: Cyber security sectoral analysis estimates, 2017-2020[3]



Source: DCMS UK Cyber Security Sectoral Analysis (2017 / 2020 / 2021)

This analysis indicates that over the last four years:

- The number of FTEs working in the cyber security sector has increased by between 4,000 – 7,000 FTEs per annum (subject to growth rates). These roles are well-aligned to the ‘core cyber role’ definition.

[3] There was no study in 2018. The figure presented for 2018 is the mid-point between the 2017 and 2019 figures.

- The growth in cyber security employment is broadly aligned to wider sectoral growth e.g. between 2017 and 2020, employment has grown by 49 percent. In this period, annual cyber security revenues increased from £5.7bn to £8.9bn (56 percent).

2.2.2 DCMS Cyber Skills in the UK Labour Market

The DCMS Cyber Skills in the UK Labour Market (2020) research does not formally estimate the size of the current size of the UK cyber security workforce. However, it does explore the volume of online job vacancies in roles aligned to cyber security.

The study undertakes the following steps:

- Initial identification of more granular search terms to use on the Burning Glass Technologies platform (which we aligned to the Cyber Security Body of Knowledge, or CyBOK);
- Extracting an initial dataset from Burning Glass Technologies with over 300,000 job postings, using the identified inclusion / exclusion terms from the first step;
- Reviewing the initial output and refining the inclusion/exclusion terms before extracting a second dataset from Burning Glass Technologies using the refined terms;
- Supplementing the second dataset with Burning Glass Technologies' own cyber security filter, which we used to distinguish between core cyber roles and cyber-enabled roles; and
- Confirming the final number of job postings within scope for this analysis (using the final, refined search strategy) with DCMS.

This refined search criteria yielded 105,194 core cyber security roles, and a further 288,063 cyber-enabled roles. In total, this identified 393,257 job postings in scope for this strand over a three year period.

This means that the study identified that **in the UK**, **there were approximately 3,000 core cyber security job postings, and a further 8,000 broader roles advertised online each month.**

It is important to note, however, that this only includes where the Burning Glass platform has identified and has permission to scrape relevant online job postings. It does not include recruitment activity through word-of-mouth or private postings (or where permission has not been permitted). Further, it is possible that for some job postings, these could involve multiple positions in a company e.g. a single advert for graduate intake that yields multiple graduate offers.

2.2.3 ISC^2

The (ISC)^2 publishes an annual Cybersecurity Workforce Study that explores the current size of the cyber security workforce, as well as the existing talent shortage.

Each study draws upon thousands of survey responses from cyber security professionals, and IT professionals that 'spend at least 25 percent of their time working on cyber security activities' globally.

In 2019, (ISC)^2 developed a methodology to explore the size of the current cyber security workforce, recognising that there is little data that exists publicly regarding this group. The 2019 study estimated that there were 805,000 cyber security professionals working in the United States, and that the US also had a cyber security workforce gap of nearly 500,000 people. In other words, the US workforce needed to grow by 62 percent to meet current demand levels.

The methodology used by (ISC)^2 used a combination of three methods for the United States:

- **Estimate of the US workforce represented by cybersecurity professionals:** This calculation includes the size of each state's workforce (using Census data) multiplied by the percentage of the expected cybersecurity workforce (based on the (ISC)^2 survey of professionals). They estimate in 2019 that cybersecurity professionals account for 0.43 percent of the workforce.

- **Estimate the average US headcount of cybersecurity professionals per business entity:** This takes the number of US businesses multiplied by the expected cyber security headcount per business. On average, they estimate 0.1 cyber security professionals per US business (i.e. for every 1m businesses, they expect 100,000 cyber security professionals).

- **Expand the average headcount of cybersecurity professionals across other countries.**

Through this approach, (ISC)^2 estimated cyber security workforce size across ten other countries, including the UK.

(ISC)^2 estimated in 2019 that the UK cyber security workforce had 289,000 professionals, and that this has increased to 365,823 in 2020 (an increase of 27 percent).

However, the 2020 study has also stated that the size of the cyber security workforce gap has decreased globally from 4m to 3.1m, and estimates a current UK workforce gap of c. 27,408 professionals.

2.2.4 Tech Partnership

In 2017, the Tech Partnership published that the UK cyber security workforce had reached 58,000 professionals by the end of 2016 – a significant increase from 22,000 in 2011 (an increase of more than 160 percent over the five year period).

Further, this research reflected those in salaried employment across the public and private sectors, and Tech Partnership estimated that approximately 12 percent of cyber security roles were within the UK public sector.

2.2.5 Other Estimates

The research team also identified that Indeed (job postings website) reported that the number of cyber security job postings had increased by 14.58 percent between 2017 and 2018.

Further, the LinkedIn platform also indicates that there are currently an estimated 75,000 user profiles in the UK that mention 'cyber security' within their current job profile (as of January 2021). Overall, this desk research identified that whilst there are limited estimates of the size of the UK's cyber security workforce, the research team consider that there are:

- An estimated 46,683 FTEs working with the cyber security sector (developing products or services) as within the Cyber Security Sectoral Analysis (2021);

- A broader estimate of 98,000[4] – 171,000[5] FTEs if we include cyber security roles within 'non-cyber security firms' e.g. financial institutions, public sector etc.;
- An estimated 75,000 individuals with a LinkedIn profile mentioning 'cyber security' in their career profile, and 366,000 mentioning 'information security' in their profile); and
- Up to 366,000 individuals estimated working within all (broader) cyber security roles in the UK by ISC[2] (2020).

These figures are explored in further detail in Section 3.7.

2.3 Identifying the Supply of Potential Talent

Within the rapid evidence review, the research team identified the need to consider the quantitative supply of potential talent in the cyber security recruitment pool on a wide basis. For example, there are many routes by which an individual can enter the cyber security workforce which need to be identified. Further, there are alternative routes that are likely to play a more significant part in filling the needs of employers, such as apprenticeships, retraining and reskilling, and online learning.

The following key areas were identified to explore the supply of new talent:

- Undergraduates, postgraduates and PhDs produced each year, in both cyber security courses (defined with Higher Education Statistics Agency, HESA, mark) and aligned courses;
- Degree apprenticeships in cyber security (including by employer type);
- Students with relevant A Level/NVQ qualifications moving into further or higher courses;
- Potential workers being retrained (or that could feasibly be retrained) into cyber roles from other occupations, such as law enforcement and military roles (to be estimated with scenarios);
- Existing IT professionals that could potentially move into cyber roles in the near future (estimated, drawing upon existing qualifications and use of DCMS Digital Economic Estimates);
- Potential supply gaps that could be addressed through lesser explored talent (e.g. neurodiverse groups, those returning to work and rehabilitated offenders); and
- Workers leaving cyber roles each year.

[4] Based upon the Tech Partnership 2016 estimate of 58,000 professionals in the UK in 2016, and a) applies an estimated growth rate of 14 percent per annum in the size of this workforce to the end of 2020 based upon average annual growth between 2016 – 2020 identified in the cyber sectoral analysis.

[5] Based on the ratio between core and enabled job vacancies within the Burning Glass data (1 : 2.67) – applied to the 2020 Cyber Security Sectoral Analysis employment figure of 46,673 (2020)

3 Quantitative Analysis

This section sets out an overview of the current volume, inflows, and outflows within the cyber security recruitment pool in the UK. It should be noted that the definition, estimation, and scenarios for the sizing of the recruitment pool are challenging and subject to debate and discussion.

It is intended that this sizing will inform a broad estimation of the current workforce, known or perceived gaps and barriers to the growth of this workforce, and to inform potential interventions at an appropriate scale to help address labour shortages within the UK cyber security workforce.

3.1 Methodology

The following data sources have been used to explore the size, scale, and location of the UK's cyber security workforce.

- **DCMS UK Cyber Security Sectoral Analysis (2017, 2020, 2021)**: This annual study explores the number of companies in the UK providing cyber security products or services, and estimates their respective revenue, Gross Value Added (GVA), and employment (in cyber security roles);

- **DCMS UK Cyber Skills in the UK Labour Market (2020 / 2021):** This annual study explores the nature and extent of cyber security skills gaps (people lacking appropriate skills), skills shortages (a lack of people available to work in cyber security job roles) and job vacancies in the UK;

- **Higher Education Statistics Agency (HESA) / Jisc:** The research team undertook a bespoke data request for 'Cyber Security' and Computer Science enrolments and graduate outcomes. This data request covers Academic Years 2017/18 and 2018/19;

- **Department for Education: Further Education and Skills Statistics:** DfE publishes further education and skills enrolment and outcomes data, as well as apprenticeship and traineeship data each year (since January 2014);

- ISC^2 Cybersecurity Workforce Study**:** This study is conducted annually to estimate the size of the current global cyber security workforce, and the size of the cyber security talent shortage;

- **LinkedIn:** The LinkedIn platform provides a useful benchmark for the volume of profiles in the UK mentioning respective job titles, education, experience, or certifications held;

- **Career Transition Partnership** offer support to Armed Forces service leavers as they transition from military to civilian life. Cyber security roles are often cited as highly complementary to the skills and aptitude of former military professionals;

- **Burning Glass Technologies Labour Insight** provides a dataset of online job postings in the UK, with search parameters in place to explore cyber security roles; and

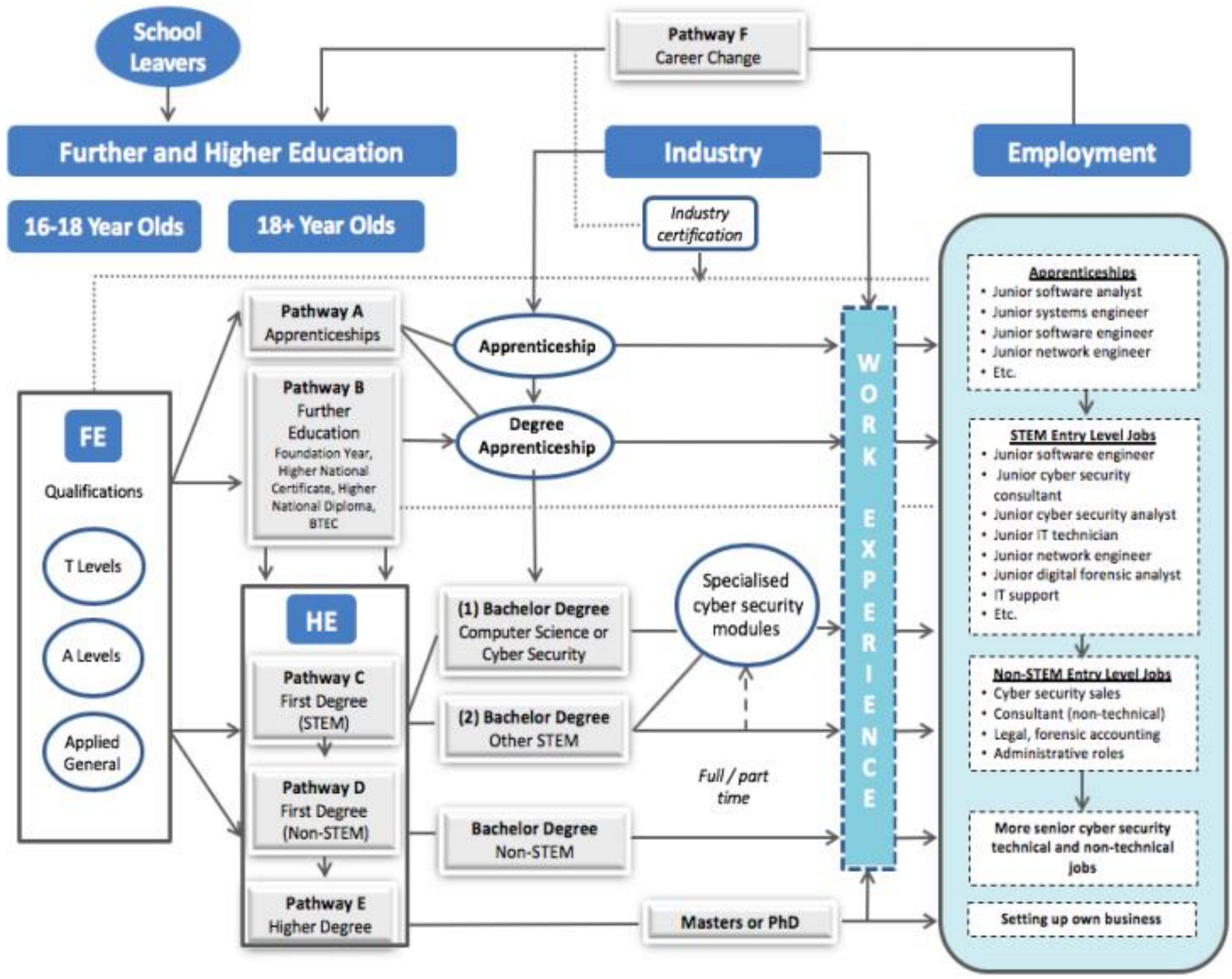
- **Regional Level Datasets:** Where appropriate, this study also explores regional estimates of the inflows and current volumes of cyber security professionals in the UK.

1.1 Pathways to Cyber Security (Mapping the Pool)

In 2018, DCMS commissioned research into ‘Identifying the role of Further and Higher Education in Cyber Security Skills Development’. This research identified a number of pathways into the cyber security sector, as highlighted in the figure below.

This shows that there are multiple routes into the cyber security sector, through both Further and Higher Education and previous work experience. These multiple routes are applicable for different types of occupations within the cyber security sector. We therefore explore these training routes in the subsequent sections.

Figure 3.1: Pathways into cyber security sector



Source: DCMS, CSES (2018)

3.2 Role of Further Education

Further Education (FE) is an increasingly important route for students, as they typically either study for A-Levels or technical qualifications. This stage is often the first exposure a student can have to concepts of cyber security, networking, and IT – and therefore can provide a platform towards further qualifications in cyber security, or indeed – the route into an entry level role in cyber security.

Within the UK, many students who go on to study Cyber Security (or broader IT or computing courses) may undertake FE courses in IT, Computing, or Programming – which may include elements of cyber security within the syllabus.

3.2.1 Courses

There are some dedicated courses at Level 2 and Level 3 for cyber security, such as Newcastle College's Level 3 in IT (Cyber Security), and Derby College's Diploma in Information Security, which have a minimum entry requirement of five GCSEs. However, the prevalence of such courses at Levels 2 and 3 in the UK is limited. Typical subsequent pathways may include moving onto a Level 4 Foundation Degree, or securing an entry level role in a cyber security organisation.

However, typically FE students will undertake a Level 3 class-room based course relevant to the wider ICT subject area (e.g. A-Level in ICT). It is estimated that approximately 50,000 students (Table 2.1) enrol each year on Level 3 class-based courses in the ICT subject area in England, of which approximately 60 percent study for a Diploma, c. 25 percent for an A-Level qualification, and the remainder for Certificates or BTEC qualifications.

3.2.2 Apprenticeships in ICT

In addition to class-based courses, in 2018/19, a total of 21,110 students were undertaking ICT subject area apprenticeships in England. This reflects an increase of 14 percent between 2017/18 and 2018/19. Further, the number of those undertaking ICT apprenticeships also increased by 14 percent between 2016/17 and 2017/18, suggesting a strong increase in the take-up of apprenticeships in recent years in ICT.

Table 3.1: Number of Apprenticeships (2017/18 and 2018/19) in England in ICT

Apprenticeship Type	2017/18 Starts	2018/19 Starts
Intermediate Apprenticeship	3,750	3,980
Advanced Apprenticeship	10,560	10,910
Higher Apprenticeship	4,170	6,220
Total	**18,480**	**21,110**

Source: Department for Education

The Department for Education (DfE) data mentioned above can be segmented into those undertaking 'ICT practitioner' and 'ICT for Users' type courses.

There has been considerable growth in the number of students enrolled on ICT practitioner courses at apprenticeship level, with the number of FE students increasing from **1,495 (2015/16) to 9,565 (2016/17)**

to 16,830 (2017/18) to 19,590 (2018/19). Breaking this down by subject level[6] as below demonstrates that:

- The volume of students enrolled within dedicated courses in cyber security (e.g. Cyber Intrusion Analyst) at Apprenticeship level is low compared to other specialisms (e.g. Digital Marketing).

- The volume of students identifying as female is proportionately low (20 percent) within these courses; however, female participation within areas such as networking and infrastructure is particularly low (e.g. only 6 percent of Level 3 Infrastructure Technicians or Level 4 Network Engineers identify as female). However, areas such as Digital Marketing appear to have greater gender diversity (a 50/50 balance for the Level 3 Digital Marketer course).

Table 3.2: Number of Enrolments[7] in ICT Apprenticeships (2018/19) in England

Detailed Level	Framework/Standard	Male	Female	2018/19 Starts
2	IT and Telecoms Professionals	**3,500**	**220**	**3,720**
3	Digital Marketer	**1,530**	**1,560**	**3,090**
3	Digital Support Technician	**20**	**0**	**20**
3	Infrastructure Technician	**3,060**	**210**	**3,270**
3	IT and Telecoms Professionals	**2,340**	**310**	**2,650**
3	IT Solutions Technician	**10**	**0**	**10**
3	IT Technical Salesperson	**290**	**110**	**400**
3	Software Development Technician	**610**	**90**	**700**
3	Unified Communications Technician	**400**	**20**	**420**
4	Cyber Intrusion Analyst	**10**	**20**	**20**
4	Cyber Security Technologist	**270**	**50**	**320**
4	Data Analyst	**1,130**	**630**	**1,760**
4	IS Business Analyst	**300**	**180**	**480**
4	IT and Telecoms Professionals	**290**	**30**	**320**
4	Network Engineer	**500**	**30**	**530**
4	Software Tester	**100**	**40**	**140**
4	Unified Communications Trouble Shooter	**40**	**0**	**40**
6	Cyber Security Technical Professional (Integrated Degree)	**20**	**10**	**30**
6	Digital and Technology Solutions Professional (Integrated Degree)	**1,170**	**340**	**1,510**
7	Digital and Technology Solutions Specialist (Integrated Degree)	**150**	**30**	**180**

[6] Please note not all of these apprenticeships are cyber security focused, but may include modules or learning with relevance e.g., basics of network infrastructure.

[7] Please note we examine the number of started enrolments in ICT Apprenticeships as the most recent data. Numbers may not sum due to rounding.

Source: Department for Education (2018/19). Numbers may not sum due to rounding[8].

The role of dedicated cyber security apprenticeships is explored in further detail in Section 3.6.

3.2.3 Destination of Further Education Students

Of the students that completed a Level 3 course in England in 2016/17, 64 percent of them progressed to a sustained Level 4 or higher qualification within the following two years. Of these, 59 percent were studying for a degree (Level 6+), three percent were studying at Level 4 or 5 (e.g. HND) and one percent were participating in a Level 4+ Apprenticeship (see data tables, and report).

Overall, the majority of FE course provision in the UK does not provide students with the dedicated skills required for a cyber security career. However, they do provide a foundation to build upon. This can help to provide initial knowledge and encourage interest in subsequent entry routes to the cyber security recruitment pool. These routes include enrolling in either a Cyber Security course at Higher Education (HE) level, or undertaking an entry-level role or Degree Apprenticeship, or moving onto a Computer Science or STEM subject.

3.3 Role of Higher Education

UK HE provides a considerable range of courses, modules, and opportunities to explore cyber security at both undergraduate and postgraduate level. As the demand for cyber security professionals has grown considerably in recent years, the HE sector has responded through the provision of dedicated cyber security courses (in addition to Computer Science and Computing courses).

Indeed, courses can include general computer science courses with one (or more) module(s) in cyber security, for example Computer Science (with a cyber module), specialist cyber security courses (Cyber Security and Digital Forensics), or non-technical courses with one (or more) module(s) in cyber security (Psychology with Cyber-Crime).

In recent years, the National Cyber Security Centre (NCSC) has certified several of these degrees at Bachelor's and Master's level under the 'NCSC-certified degrees' programme, as well as undertaking calls for Academic Centres of Excellence in Cyber Security Research (ACE-CSR) and Academic Centres of Excellence in Cyber Security Education (ACE-CSE).

This subsection explores the volume of courses and number of students enrolled and graduating from cyber security courses in the UK, and those within Computer Science courses. This data is informed by a bespoke data request from Jisc / HESA utilising HESA Student Record Data, and HESA Graduate Outcomes Survey Results (2017/18 and 2018/19).

3.3.1 Courses

Using the HESA student data extract, we have identified the following number of courses offered by UK Higher Education Institutions in Cyber Security and Computer Science[9] (unique course titles in 2017/18 and 2018/19).

[8] Figures are rounded to the nearest '10'.

[9] These two groups of courses are exclusive, there is no overlap between the groups.

Table 3.3: Number of Related Courses and Providers (UK)

Qualification	Cyber Security	Computer Science
Undergraduate (First Degree)	239[10] (from 63 universities)	1,965 (from 121 universities)
Other Undergraduate (e.g. Foundation)	13 (from 9 universities)	149 (from 49 universities)
Postgraduate	182 (from 73 universities)	1,446 (from 121 universities)
Total	**434**	**3,560**

Source: Jisc / HESA

Overall, 64 universities offering undergraduate courses and 73 universities offering postgraduate courses in Cyber Security were identified. In recent years, dedicated cyber security courses within UK universities have often been offered at Master's level, following completion of a relevant Bachelor's degree in a related subject such as Computer Science. However, there has been a notable increase in the number of universities offering dedicated cyber security courses at Bachelor's level, often with strong volumes of student enrolments and good engagement with local employers.

Table 3.4: Breakdown of Student Enrolment and Qualifiers in UK Higher Education Institutions (HEIs) (2017/18 and 2018/19): Cyber Courses

	Number of HEIs offering a relevant course		Number of Students Enrolled[11]		Number Graduating	
Academic Year	*2017/18*	*2018/19*	*2017/18*	*2018/19*	*2017/18*	*2018/19*
Undergraduate	58	64	7,240	8,670	1,820	2,060
Postgraduate	66	73	2,650	3,020	1,080	1,310
Total	**76**	**83**	**9,890**	**11,690**	**2,890**	**3,360**

Table 3.5: Breakdown of Student Enrolment and Qualifiers in UK HEIs (2017/18 and 2018/19): Computer Science Marker

	Number of HEIs offering a relevant course		Number of Students Enrolled[12]		Number Graduating	
Academic Year	*2017/18*	*2018/19*	*2017/18*	*2018/19*	*2017/18*	*2018/19*
Undergraduate	122	122	86,930	89,760	20,630	20,990
Postgraduate	124	121	18,630	21,050	8,890	9,890
Total	**130**	**128**	**105,550**	**110,820**	**29,530**	**30,890**

Source: HESA Data Extract (numbers are rounded to nearest 10. May not sum due to rounding.)

The HESA data extract highlights that UK HEIs are home to:

[10] Please note that the number of courses refers to the count of individual courses offered by the university. For example, 'Cyber Security' and 'Cyber Security and Digital Forensics' offered by the same university would be two courses.

[11] Counted in HESA standard registration population

[12] ibid

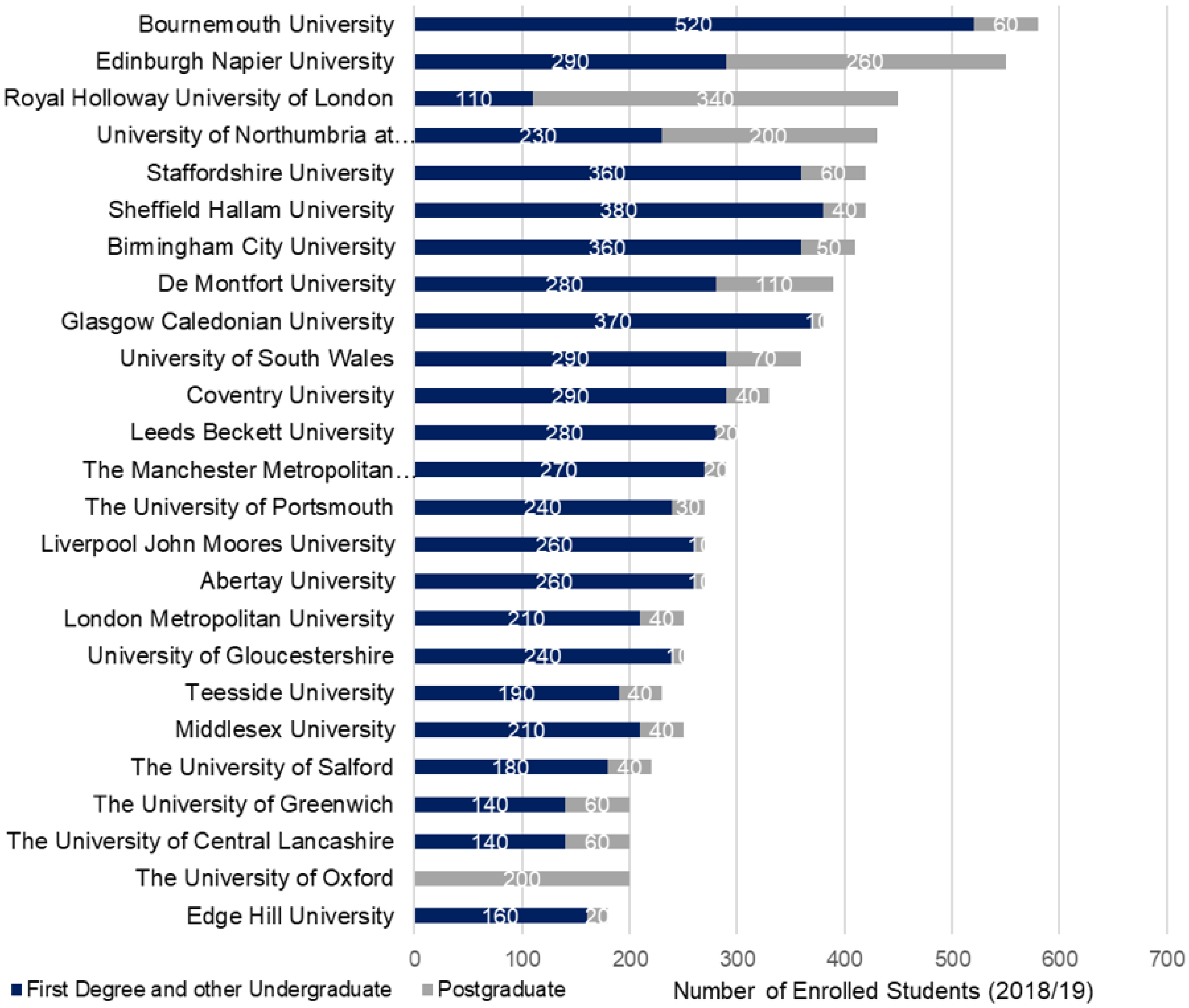
- Approximately 11,690 students (2018/19) enrolled in cyber security focused courses in the UK (8,670 at undergraduate level and 3,020 at Postgraduate level), and a further 110,820 enrolled in other Computer Science courses.

- In the most recent year, there were 3,360 students graduating with a cyber security focused degree, and a further 30,890 with a Computer Science degree.

3.3.2 Course Providers

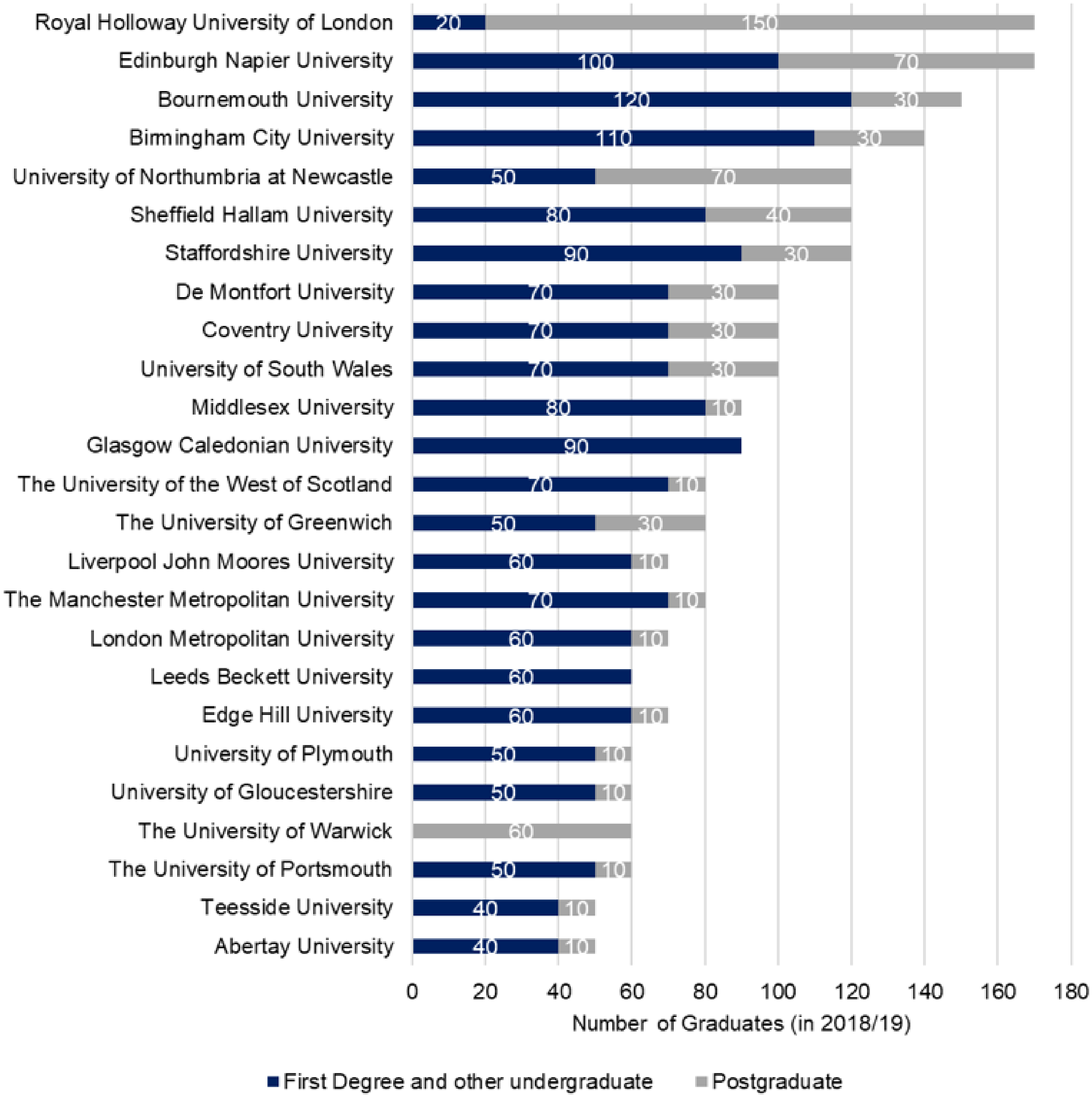
In 2018/19, there were 83 HEIs providing some form of taught cyber security course at any level. The following charts set out the institutions with the highest volumes of enrolled (and graduated) students in cyber security focused courses. This suggests some geographical variation, with particular growth in undergraduate provision in some regions outside of London.

Figure 3.2: Number of Enrolled Students by Higher Education Provider (By Volume)



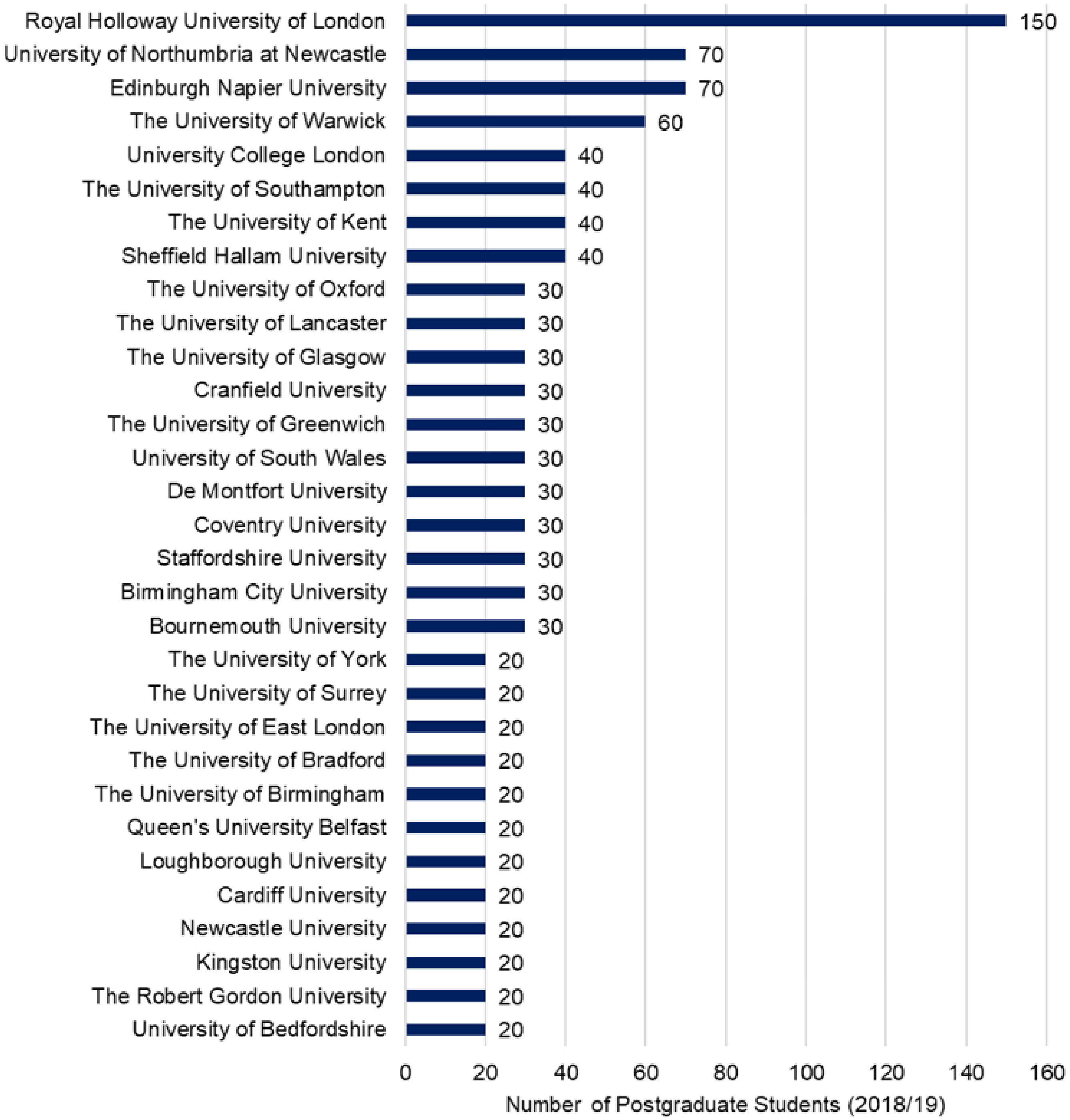
Source: Jisc / HESA (2018/19)

Figure 3.3: Number of Students Graduating in Cyber Security Courses (Top 25)



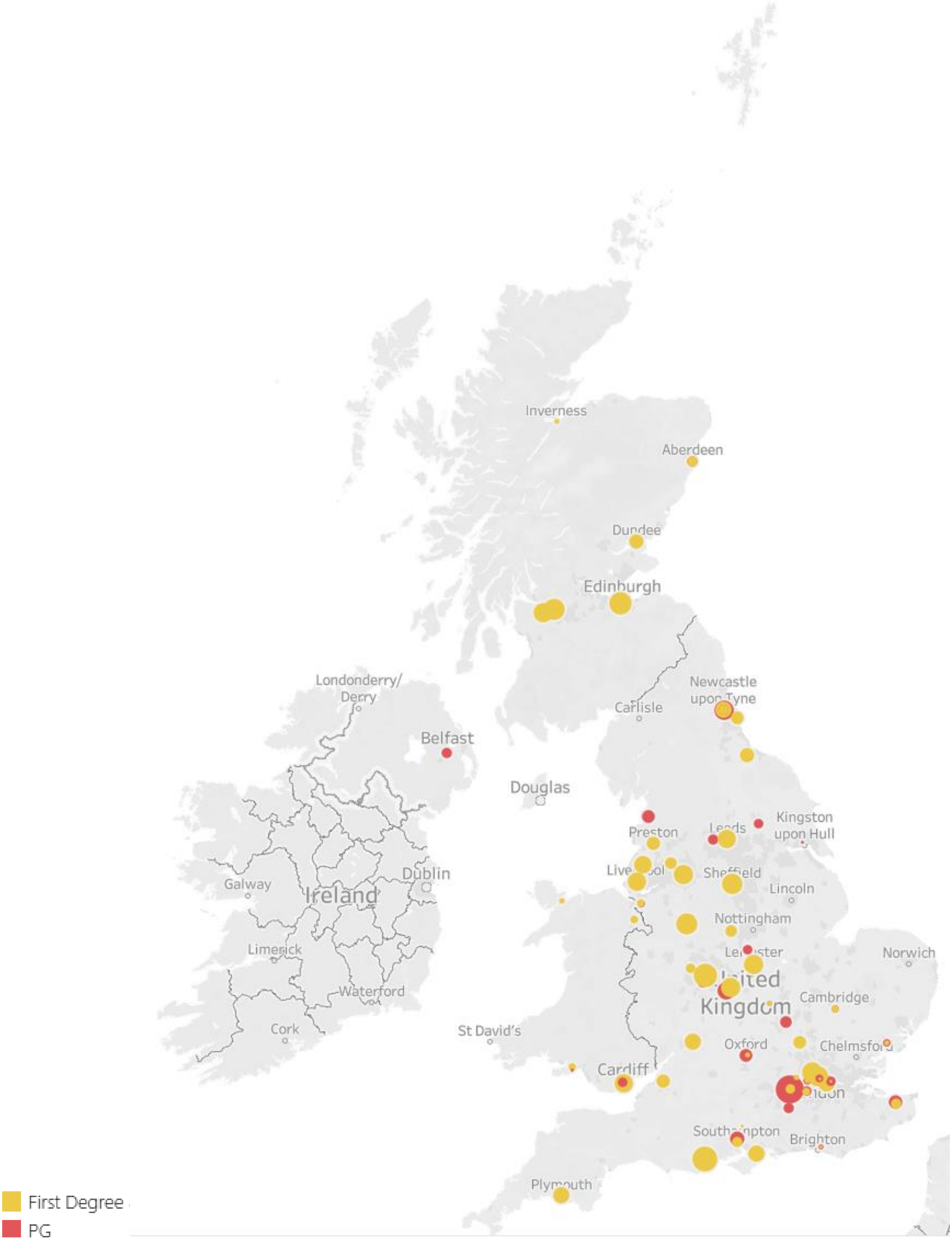
Source: Jisc / HESA (2018/19)

Figure 3.4: Number of Postgraduate Students Graduating in Cyber Security Courses (Top institutions by volume)



Source: Jisc / HESA (2018/19)

Figure 3.5: Location of Cyber Security Graduates



Source: Jisc / HESA (2018/19, n = 3,360): The size of the circle relates to the count of students.

3.3.3 Profile of Courses and Students

In 2018/19, there were:

- 3,360 students graduating from a cyber security related course (1,310 postgraduate and 2,060 undergraduate);
- 30,890 other Computer Science graduates (9,890 postgraduate, and 20,990 undergraduate); and
- There are currently 11,690 students registered on a cyber security related course (2018/19) – up from 9,890 in 2017/18. Of these, there are 3,020 at postgraduate level, and 8,670 at undergraduate level.

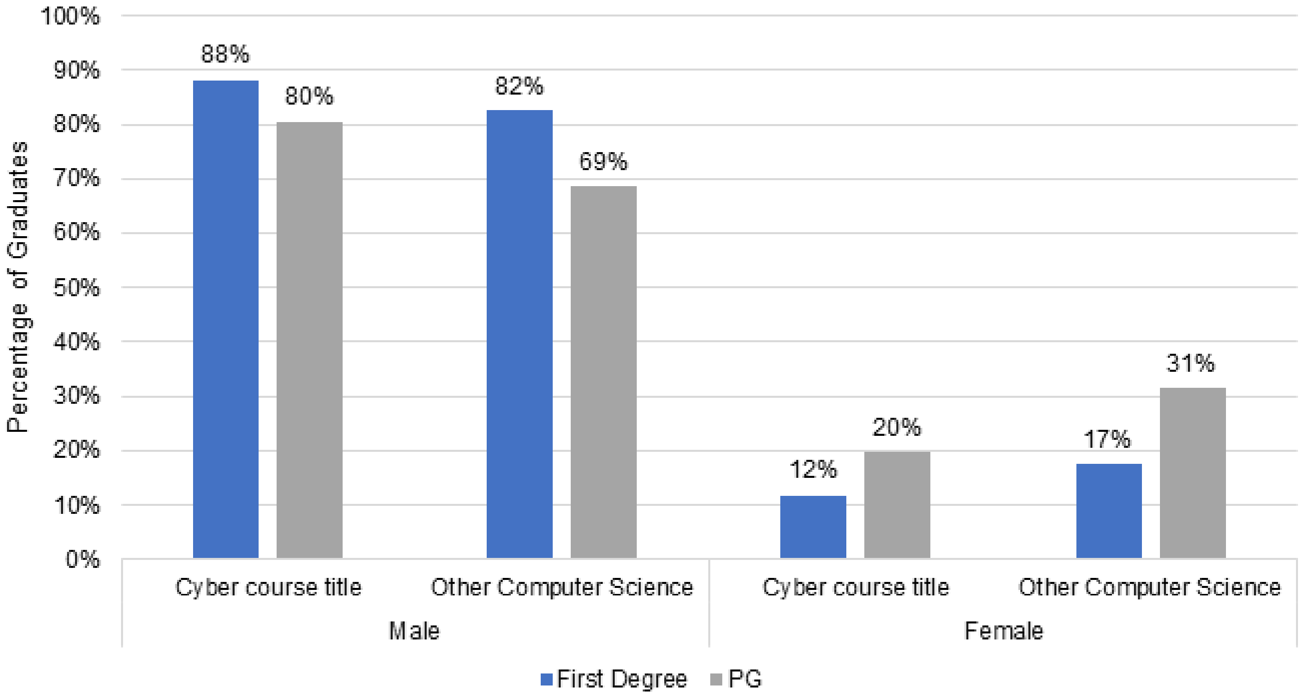
The following subsections provide a breakdown of 2018/19 graduates by respective demographic measures.

3.3.4 Gender Identity

As stated previously, the cyber security workforce is estimated to have a disproportionately low number of female staff. As such, tackling the gender gap will require a substantial increase in the new supply of female talent entering education, training and subsequently the workforce.

The HESA data highlights that only 12 percent of graduates in cyber security courses at undergraduate level, and 20 percent of graduates at postgraduate level identified as female in 2018/19. Comparing this to Computer Science courses in the UK (17 percent female at undergraduate and 31 percent at postgraduate level) suggests that there is still a substantive need to encourage and attract more females into cyber security courses and modules in UK higher education.

Figure 3.6: Gender Identify of Cyber Security and Computer Science Graduates (2018/19)



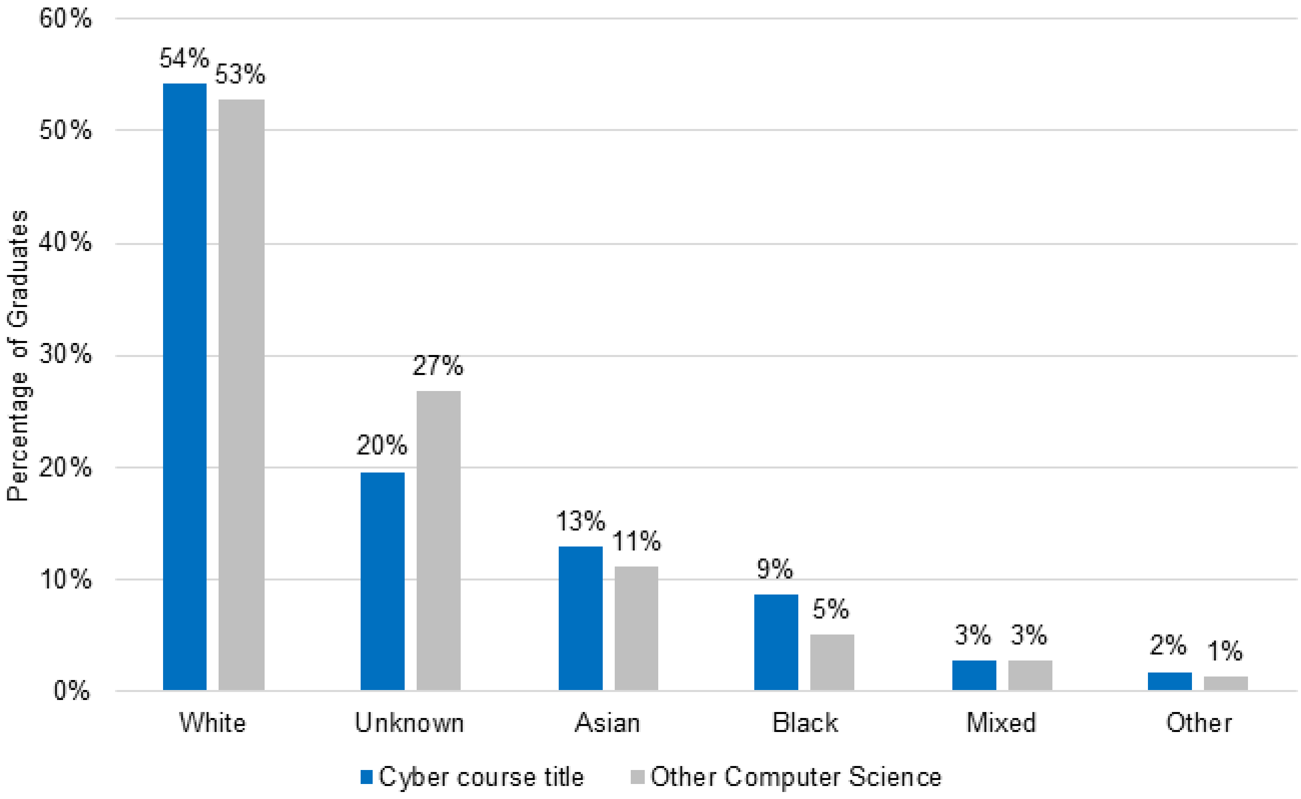
Source: Jisc / HESA (2018/19), n = 3,360 and n = 30,890

3.3.5 Ethnicity

Analysis of students enrolled in cyber security and computer science courses indicates that in 2017/18 and 2018/19, at least 24 percent of students enrolled in a cyber security course, and 19 percent of computer science students were from an ethnic minority background.

This is slightly higher than the current incidence of ethnic minority individuals (16 percent) identified within the Cyber Skills in the UK Labour Market report (2020). However, many of these students may be enrolled in a UK university for purposes of study, and subsequently leave the UK to study in other countries.

Figure 3.7: Ethnicity of Cyber Security and Computer Science Enrolled Students (2017/18 & 2018/19)



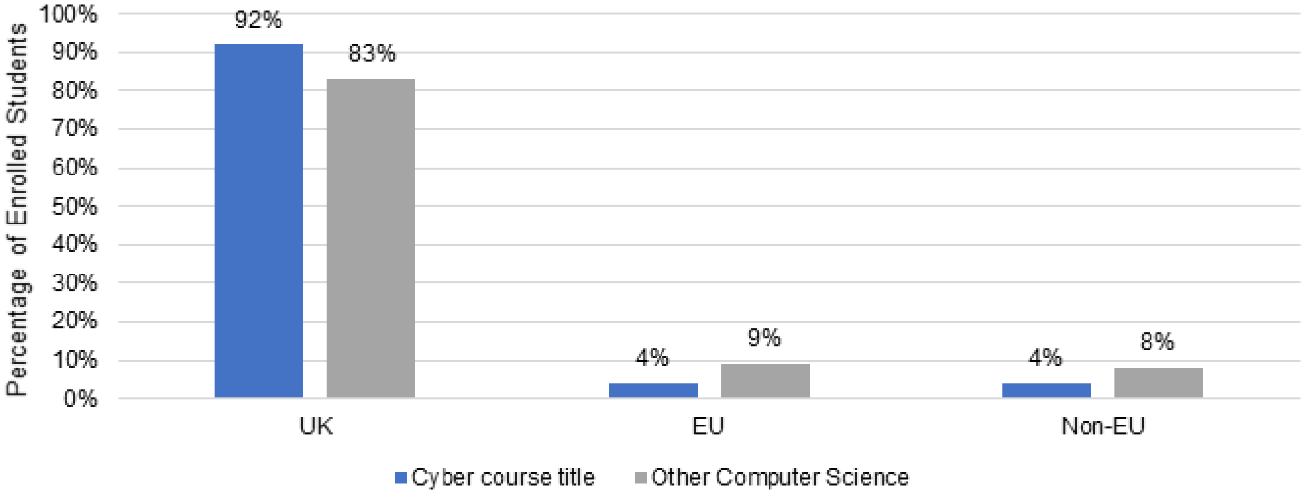
Source: Jisc / HESA (2017/18 and 2018/19)

3.3.6 Domicile

This refers to the country of the student's permanent home address prior to entry to their course. Across all undergraduate courses in the UK in 2018/19, an estimated 85 percent of students were from the UK, five percent were from EU countries, and 10 percent from outside of the EU (data).

For those enrolled in cyber security courses at undergraduate level, 92 percent were from the UK, compared with 83 percent for Computer Science courses.

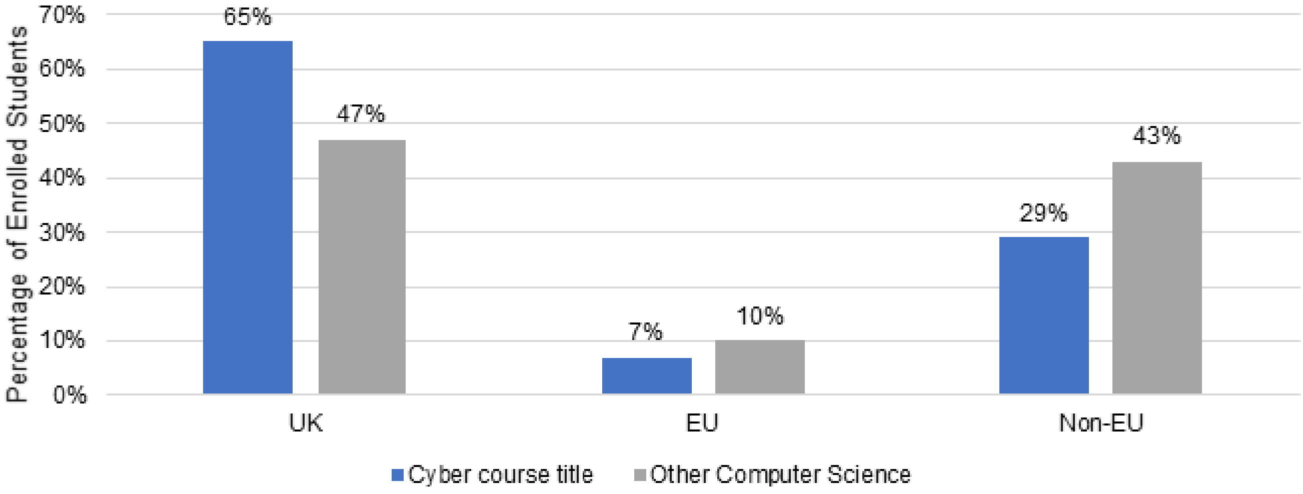
Figure 3.8: Domicile of Undergraduate Cyber Security and Computer Science Enrolled Students (2018/19)



Source: Jisc / HESA (2018/19)

Across all postgraduate courses in the UK in 2018/19, an estimated 63 percent of students were from the UK, 7 percent were from other EU countries, and 29 percent from outside of the EU, demonstrating the significance of international students at postgraduate level in the UK. For those enrolled in cyber security courses, the proportion of international student enrolment is comparable to the UK level.

Figure 3.9: Domicile of Postgraduate Cyber Security and Computer Science Enrolled Students (2018/19)



Source: Jisc / HESA (2018/19)

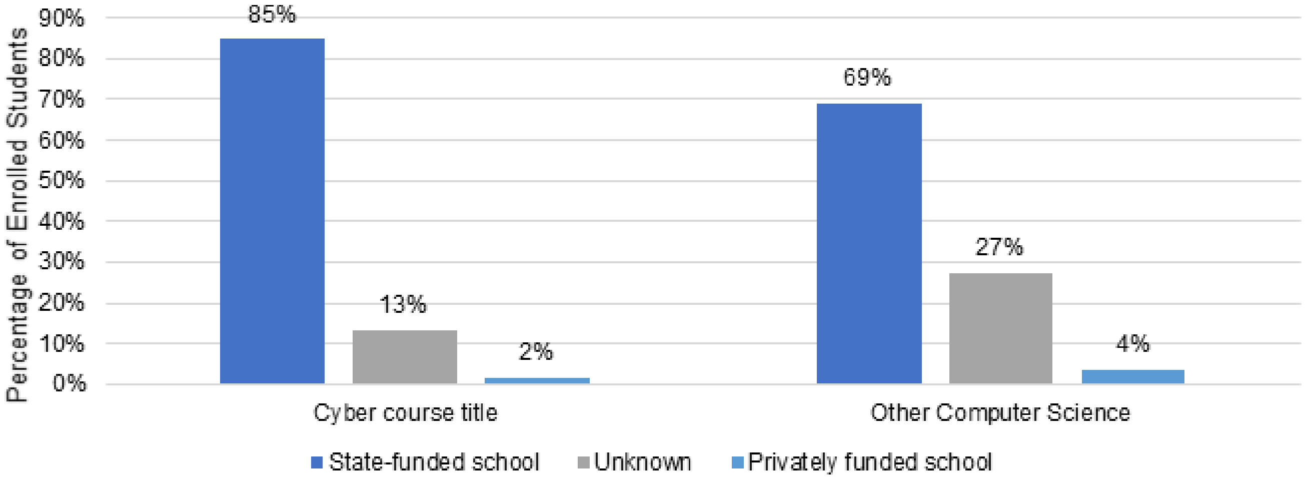
3.3.7 State School Marker

A key indicator for the performance of the UK's HE sector is that of widening participation. This is often measured exploring where the student previously attended a state school or privately funded school, or by those coming from a low participation neighbourhood.

Across all UK first degrees, 90 percent of students come from a state school or college. Across the UK regions, 87 percent of those enrolled in Scottish universities come from a state school background, followed by England (90 percent), Wales (92 percent) and Northern Ireland (99 percent).

Exploring this data for cyber security and other computer science courses highlights that two percent of students within a cyber security course are privately educated compared to four percent of computer science students. Whilst both courses contain some enrolled students with an unknown status (e.g. where the previous school was not in the UK), this indicates that participation within cyber security courses by those from state-funded schools is significant.

Figure 3.10: State School Marker – Undergraduate Cyber Security and Computer Science Students – Enrolled in 2018/19

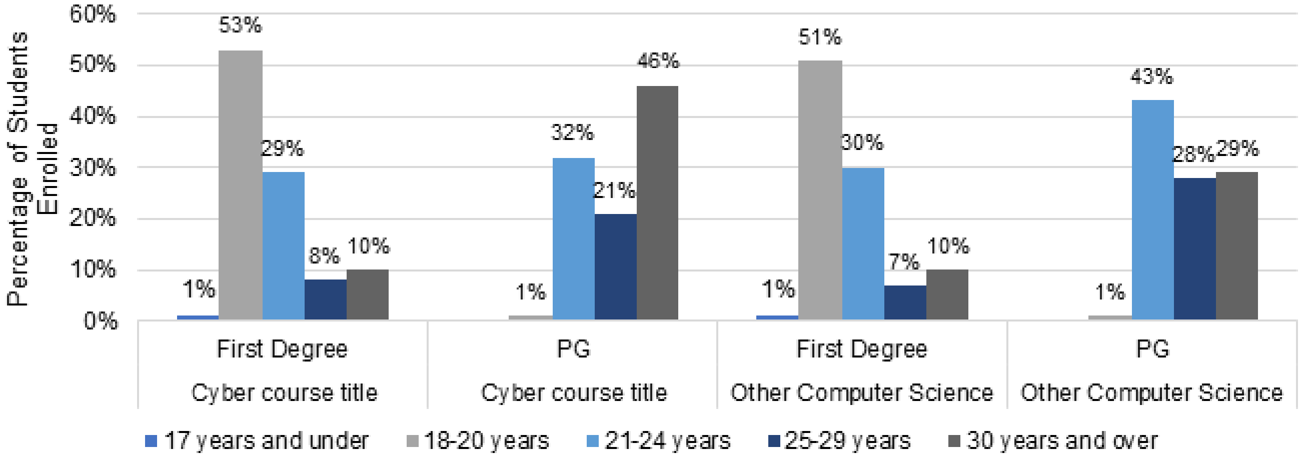


Source: Jisc / HESA (2018/19) n = 8,670 (Cyber), n = 89,760 (Other Computer Science)

3.3.8 Age

Whilst the majority of students enrolled in cyber security courses (83 percent) and computer science (81 percent) at undergraduate level are under the age of 24, there is evidence of a significant mature student demand for cyber security courses.

Figure 3.11: Age of Undergraduate Cyber Security and Computer Science Students – Enrolled in 2018/19



Source: Jisc / HESA (2018/19)

For example, as shown in Figure 3.11, 67 percent of those enrolled in postgraduate study in cyber security courses are aged 25+, with 46 percent over the age of 30. The enrolment of students over the age of 25 is higher at postgraduate study in cyber security courses (67 percent) than computer science (57 percent), and may signal a demand by mature students or those with existing qualifications and work experience to undertake further study at postgraduate level.

3.3.9 Full-Time / Part-time Enrolment

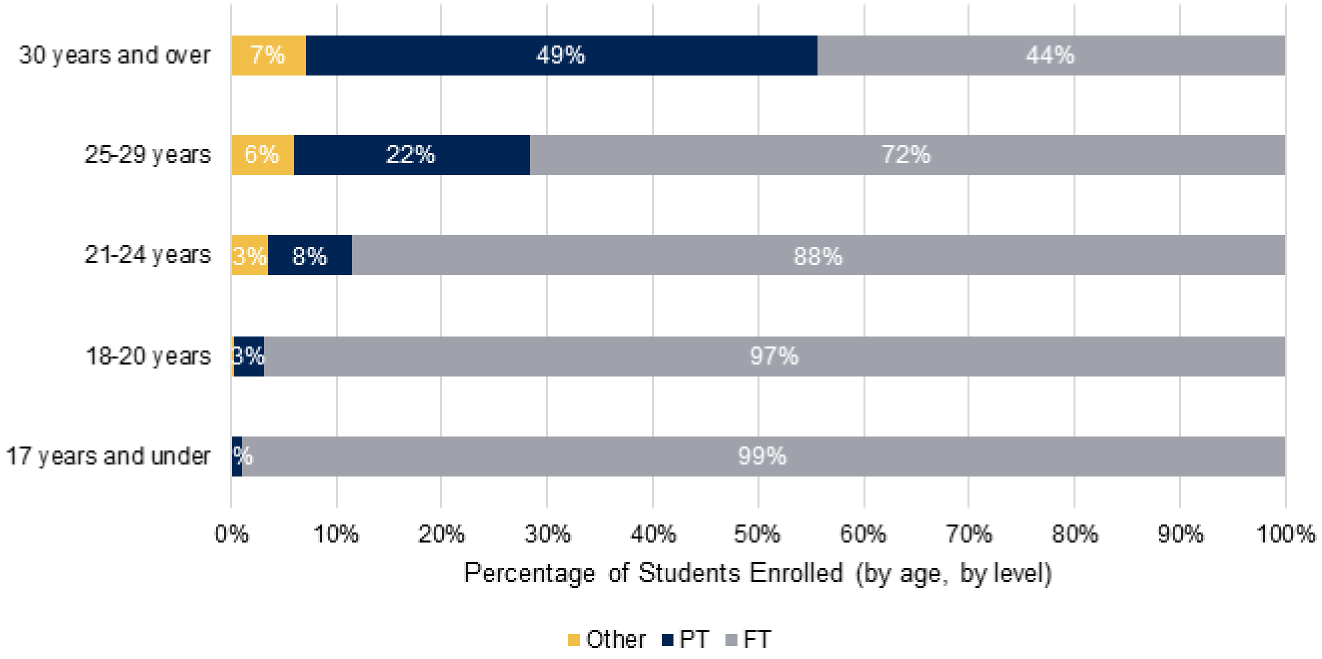
In 2018/19, 85 percent of undergraduate students and 61 percent of postgraduate students were enrolled on a full-time basis. For those enrolled in cyber security courses in the UK:

- 92 percent were enrolled full-time at undergraduate level; and
- 54 percent were enrolled full-time at postgraduate level, with 38 percent at part-time (and 8 percent other / unknown).

This highlights the proportional importance of part-time study at postgraduate level within cyber security courses in the UK. As demonstrated by the breakdown of courses and student locations, several UK universities often focus cyber security course provision at the postgraduate level, whereby students can undertake an undergraduate degree in Computer Science (or similar), potentially undertake a few years of work experience, and then return (part-time where available) to university to undertake an applied course in cyber security at postgraduate level.

As mentioned previously, 46 percent of postgraduate students in cyber security courses are over 30 years old, and of these, more than half undertake part-time study. This reflects the need for flexibility of provision, to help further encourage mature applicants into the field of study.

Figure 3.12: Age of Cyber Security Students – Enrolled in 2018/19 (all levels)

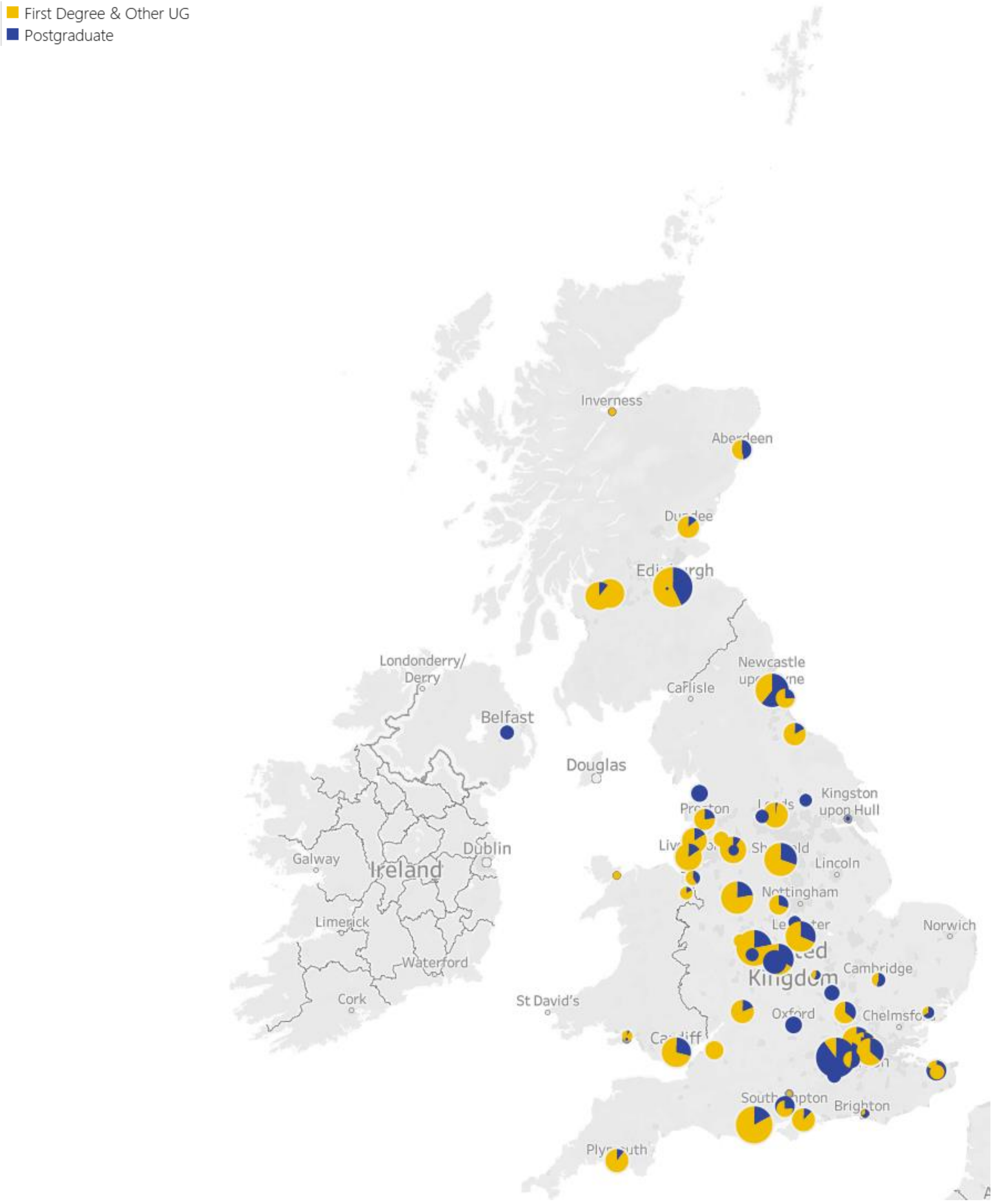


Source: Jisc / HESA (2018/19)

3.3.10 Graduate Outcomes

Further to current student data, it is also possible to draw upon graduate responses to the HESA Graduate Outcomes survey. This data covers those that had graduated in cyber security and other computer science courses in 2017/18, and have responded to the survey. Please note that as this reflects survey data – it is reflective of respondents, and may therefore underestimate or not fully capture the outcomes for groups less captured by the survey (e.g. those returning to another country following completion of studies in the UK).

Figure 3.13: Location of 'Cyber Security' Course Graduates (by location of HEI graduation outcome) (2018/19)

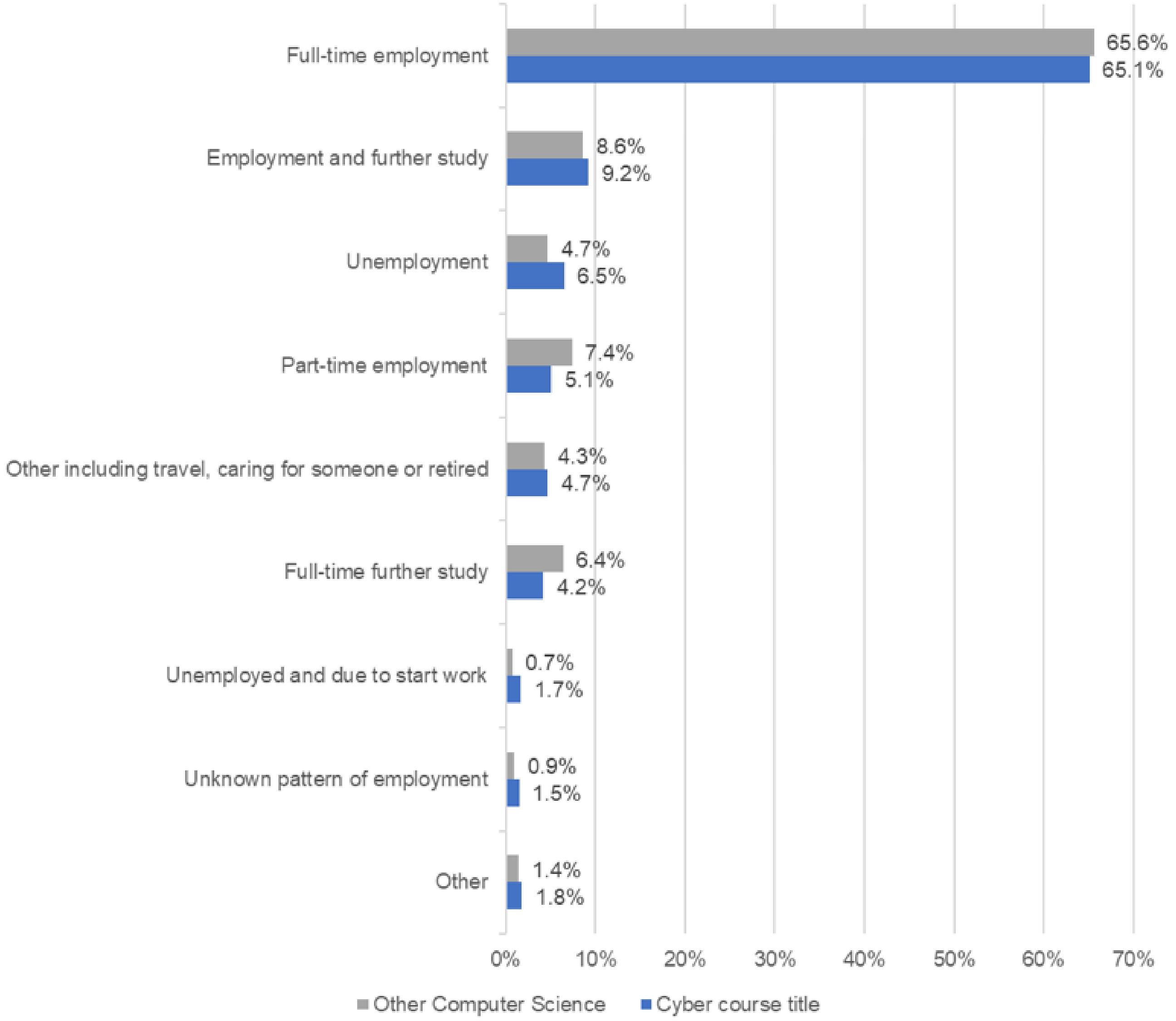


Source: Jisc / HESA Graduates (2018/19): n = 3,360

Within the Graduate Outcomes survey, graduates are asked information about their activities approximately 15 months after they complete their studies. Therefore, whilst the following data captures those that graduated in the academic year 2017/18, the responses received can range between December 2018 and September 2019.

For the students that reported their activity following graduation, the following breakdown was noted.

Figure 3.14: Graduate Outcomes (2017/18)



***Source:** Jisc / HESA Graduate Outcomes (2017/18 cohort) n = 1,370 (cyber), n = 14,570 (computer science)*

This indicates that approximately 65 percent of cyber security graduates enter full-time employment, with a further nine percent blending employment and further study. A further five percent entered part-time employment. This means that, of the 3,360 students that graduated within a cyber security course in 2018/19, we might expect that approximately 80 percent should enter or stay within employment within 15 months of graduation since their most recent degree award. These figures are comparable for other Computer Science courses.

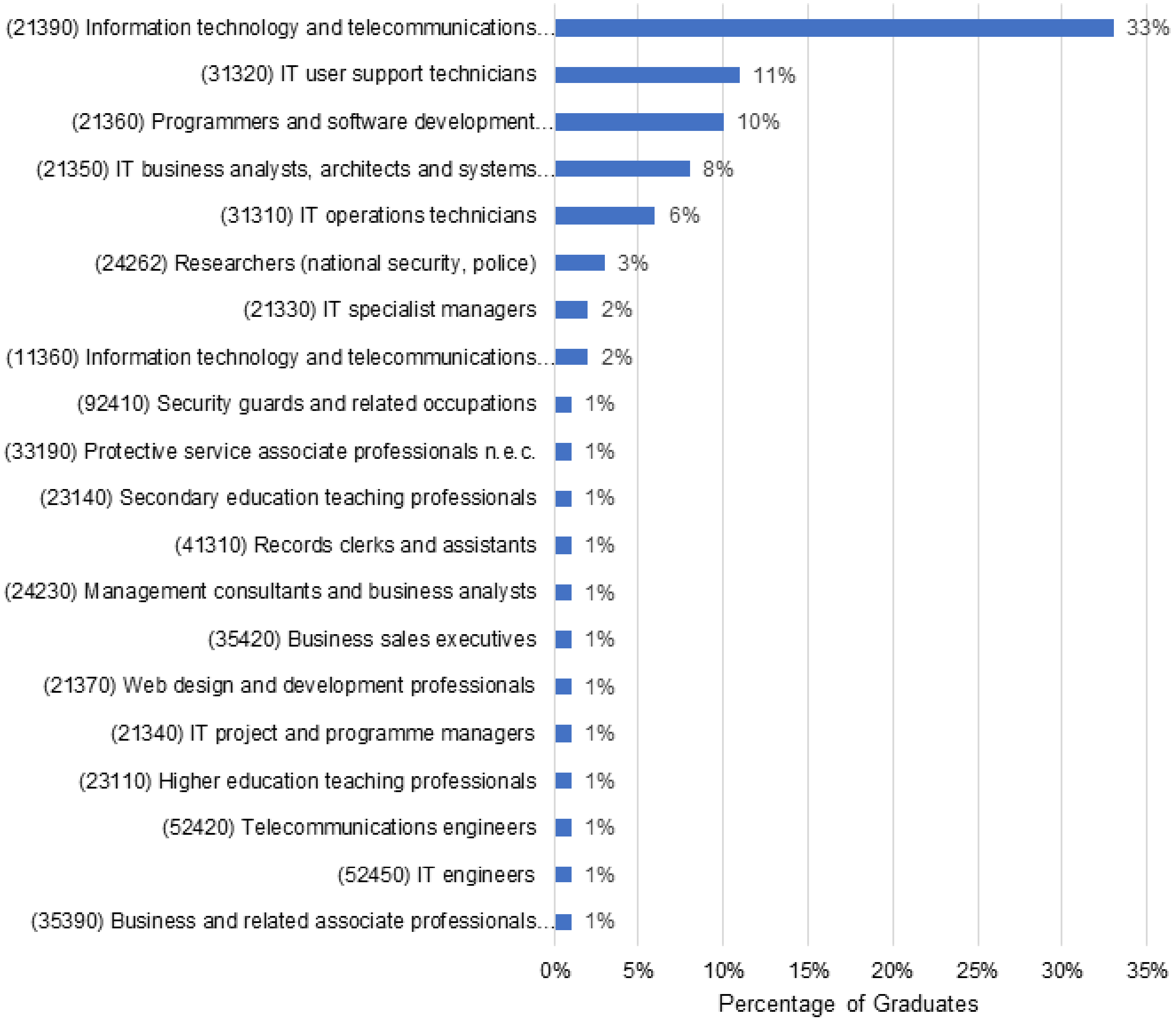
It is notable that seven percent of cyber security graduates are unemployed, without being due to start a new job or further study. This is higher than other Computer Science graduates (five percent), and is explored further within the qualitative findings.

Of those that enter full-time employment, we have identified their respective occupations. The Graduate Outcomes survey uses SOC2010 codes, which means there is no distinct identifier for being employed with a ‘cyber security role’.

However, as shown below, most graduates that move into full-time employment do tend to move into an IT related role. A small proportion (c. 10 percent) do not appear to move into IT based employment, however, this may be short-term following graduation.

The redefinition of IT occupations in SOC2020 by minor and unit group in the future should help to provide a more granular assessment of those cyber security (and other degrees) graduates moving into a cyber security role upon graduation. This is because 2139 ‘IT and Telecommunication Professional” will be segmented into 2135 Cyber Security Professionals, 2136 IT quality and testing professionals, 2,137 IT Network Professionals, and 2139 IT Professionals n.e.c.’.

Figure 3.15: Top 20 Job Roles (SOC2010) for Cyber Security Graduates (2017/18)



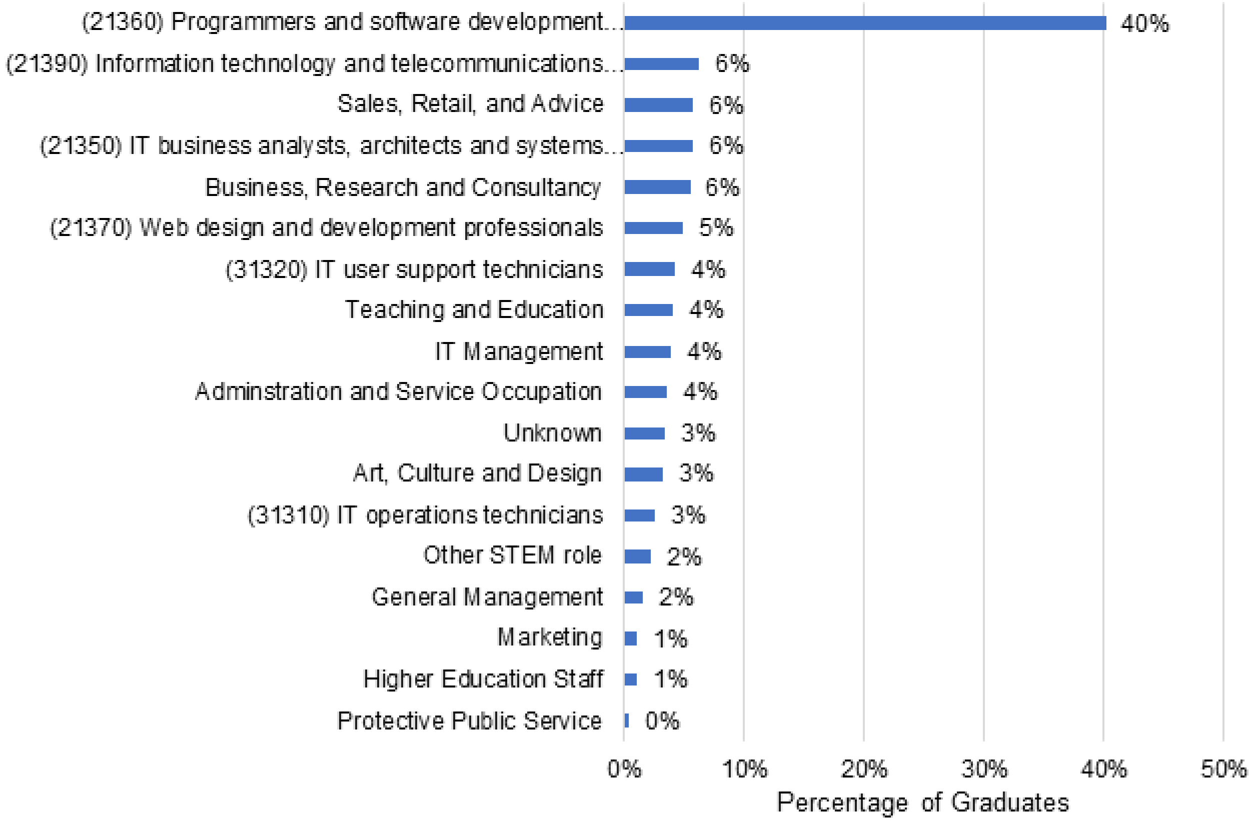
Source: HESA Graduate Outcomes (2017/18 cohort) n = 1,370

It is also estimated that 21 percent of these employees are in a supervisory position within the current job.

Exploring career outcomes for those graduating in other computer science courses indicates that nearly 82 percent secure full or part-time employment. Of those in full-time roles, the following breakdown of job roles is provided through the Graduate Outcomes survey.

For those graduating in computer science that have entered a full-time role, 40 percent report that they're involved in a programming and software development role. Whilst it is difficult to estimate what proportion of these are within 'cyber' roles, we can note that approximately 22 percent of these respondents are involved in roles potentially less likely to be IT / cyber related (e.g. sales, administration, art and culture, general management etc).

Figure 3.16: Job Roles (SOC2010)[13] for Computer Science Graduates (2017/18)



Source: HESA Graduate Outcomes (2017/18 cohort) n = 9,560

With respect to the cyber recruitment pool, we assume that the following proportion of higher education graduates may be likely to enter IT roles each year:

[13] Note: we have grouped some SOC codes in Figure 3.3 to better reflect the estimated proportion entering, for example, retail or administrative roles.

Table 3.6: Estimated number of graduates in IT related roles

Course Type	Number of Graduates (2018/19)	Proportion in FT Employment (within 12 months)	Proportion of those in IT roles (estimated)	Implied Population
Cyber Security	3,360	65%	c. 90%	2,000[14] (rounded)
Other Computer Science	30,890	65%	c. 80%	16,000 (rounded)

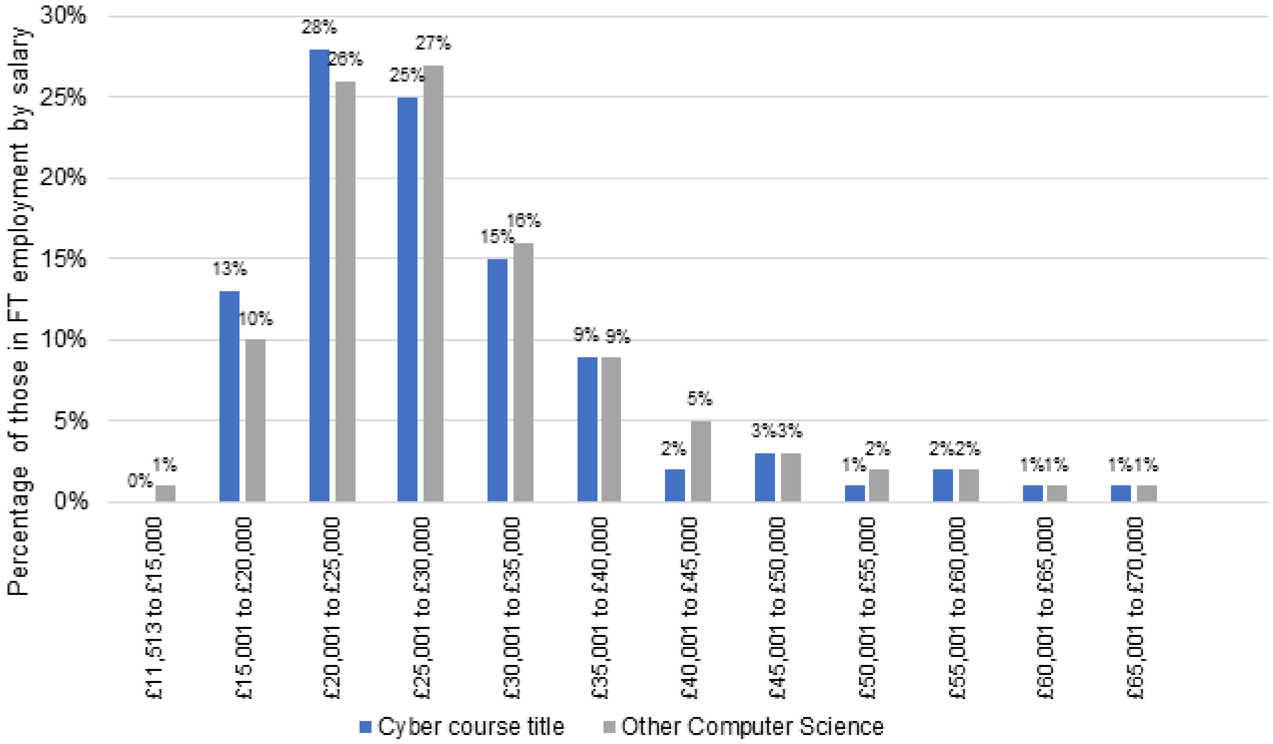
Source: HESA Graduate Outcomes Data (Estimates, PE)

However, only a small proportion of these students will enter a **cyber security role** (given the breadth of industry and sectors whereby these skills are applicable) which is explored in further detail in Section 3.8.

3.3.11 Salaries

Analysis of Graduate Outcomes data also indicates salary bands for those in full-time employment. This shows that the earnings of graduates from cyber degree courses broadly matched the earnings of graduates from computer science courses (see figure below). The majority of graduates for both courses (around two thirds) were earning less than £30,000 within fifteen months of graduating.

Figure 3.17: Reported Salaries by those in full-time employment (2017/18)



Source: HESA Graduate Outcomes Data (Cyber, n = 500 // Computer Science, n = 5,170)

[14] Number of graduates x Proportion in FT employment x Proportion working in IT roles = Estimated Population (rounded to nearest hundred)

3.4 Role of Apprenticeships / Degree Apprenticeships

The number of individuals undertaking degree apprenticeships in cyber fields in England is presented in the table below. This shows that although the actual numbers of degree apprenticeships are still relatively low (just over 600 in 2018/19), there has been a large increase in degree apprenticeships in cyber in the past three years, with the largest increase (and largest proportion of degree apprenticeships in cyber) being for the Cyber Security Technologist apprenticeship. This increase has largely been driven by organisations such as BT, QA, KPMG and Firebrand Training, all of whom are utilising degree apprenticeships.

Table 3.7: Number of degree apprenticeships in England, 2016/17 to 2018/19

Framework/Standard Name	2016/17	2017/18	2018/19
Cyber Intrusion Analyst	10	18	24
Cyber Security Technologist	96	284	557
Cyber Security Technical Professional (integrated degree)	0	0	25
Total	**106**	**302**	**606**

Source: Department for Education

3.5 Role of Certification and Training Providers

3.5.1 Introduction

In addition to qualifications obtained through further and higher education, several employers will also look for potential employees with relevant skills often affirmed through certification and training providers.

In recent years, there has been increased emphasis on how certifications and training models can rapidly upskill people to move into or increase knowledge of cyber security roles. Further, the provision of innovative training models such as cyber security academies and bootcamps, and enhanced access to low-cost online training platforms has also driven enhanced interest in cyber security training.

The following sections explore the role of the certifications and training providers in increasing and size and capabilities of the cyber security recruitment pool.

3.5.2 Certifications

Within the 2020 Cyber Skills in the UK Labour Market study, a survey of 205 cyber sector businesses found that among qualified staff:

- 33 percent of staff held a general computer science / IT degree;
- 27 percent of held a specialist degree in cyber security;
- 11 percent were qualified through a cyber or other apprenticeship role; and
- 51 percent of staff held some form of other technical accreditation.

Among these 51 percent of staff, there were recurring mentions of staff holding Certified Information Systems Security Professional, or CISSP (38 percent), Certified Information Security Manager, or CISM (14 percent), CREST-approved training (12 percent), Certified Ethical Hacker accreditation (12 percent) and ISO 27001 Certified Information Security Management Systems, or ISMS (11 percent). This indicates the relative importance of technical accreditation for cyber security staff in the UK. However, this study also recorded over thirty cyber security accreditations held by cyber security staff, indicating a high level of fragmentation within the market for cyber security training.

Within the UK, as of January 2021, there are approximately 7,900 (ISC)² members in the UK holding the CISSP certification, and 148,000 globally. In other words, approximately 5 percent of CISSP certifications are held in the UK.

CompTIA is also a prevalent certification provider, offering Network+, Security+, PenTest+ and more. In 2019, CompTIA announced that over 500,000 individuals had earned the CompTIA Security+ certification globally.

The qualitative findings within the following sections explore the role and perceived importance of certifications within the cyber security recruitment pool and includes a case study on CompTIA.

3.5.3 Role of Retraining for a Cyber Security Role

Range of Interventions

The impact of the COVID-19 pandemic in recent months has arguably provided a renewed emphasis on the potential of reskilling and retraining individuals into cyber security roles. This might include, for example, retraining and placing unemployed or underemployed individuals into cyber security training bootcamps with the potential for an employer interview as a cyber security analyst.

It may also include a focus on individuals that could benefit from support to enter or re-enter the labour market. For example, in 2019 DCMS led the Cyber Skills Immediate Impact Fund (CSIIF) which provided funded government support to a range of pilot initiatives to increase the volume and diversity of individuals entering into cyber security.

In recent months and years, there has also been an increased focus by devolved administrations and Local Enterprise Partnerships (LEPs) to fund such initiatives as employer-led cyber security skills academies, and support access to online funded training courses[15].

As set out in the Cyber Skills in the UK Labour Market research, this provision can be a highly effective way to address access barriers involved in entering the cyber security recruitment pool. For example, within CSIIF, the development of a pilot Neurodivergent Digital Cyber Academy highlighted how neurodiverse individuals could be in a best position to train and undertake applied SOC experience.

[15] Examples include Scotland’s Digital Start Fund (https://www.scotlandis.com/digitalskills/) and the Microsoft Cyber Academy in Northern Ireland supported by the Department for Economy (https://www.nidirect.gov.uk/articles/assured-skills-training-programme)

Case study – Microsoft

Funded by the Department for the Economy NI, the Assured Skills pre-employment programme provides an upskilled workforce which facilitates new inward investors, and provides existing employers with the resource to enable business expansion and growth.

Belfast Metropolitan College (Belfast Met) have delivered over 100 Assured Skills academies since 2013, with 1300+ graduates now in careers with leading global and local firms based in the greater Belfast area. Before completing the programme many of the graduates were unemployed, underemployed or people wishing to change career.

In March 2020, Belfast Met commenced the inaugural Cyber Security Assured Skills Academy with Microsoft. This 12 week academy began on campus at Belfast Met's e3 building. By the end of the first week, the college had to transition to remote delivery due to lockdown restrictions of the COVID-19 pandemic.

Twenty-five students successfully completed the academy which included brand new Microsoft Azure qualifications which had previously only been delivered as part of a pilot with students in Sydney Australia. The academy curriculum was designed in collaboration with Microsoft to upskill participants for roles as cyber security consultants.

The students completed the following qualifications and training:

- MTA Security Fundamentals
- MTA Networking Fundamentals
- AZ-900: Azure Fundamentals
- AZ-500: Microsoft Azure Security Technologies
- AZ-104: Microsoft Azure Administrator
- FRESH - Design thinking programme
- Human Skills including commercial awareness, leadership styles, EQ, networking and resilience.

On completion of the academy twenty-three students moved into roles as cyber security consultants in the Microsoft Belfast Cyber Security Centre.

Online Training Models

In addition to direct funded support to undertake training or programmes, there is also a wide range of low-cost or often free online modules and courses that individuals can undertake in their own time. These include platforms such as FutureLearn, which is part-owned by the Open University, or proprietary platforms such as Coursera, EdX, and Udemy that offer online modules in IT, networking, cyber security and more. Whilst these modules may not always contain direct certification, they provide a highly useful platform for skills development and access to further training.

In recent years, there has also been an increase in the volume of online training provision focused on how to use and become experienced in securing particular platforms among existing users. For example, Microsoft offers training in how to implement security controls in Microsoft Azure (Azure Security Engineer Associate pathway), as does Amazon Web Services (e.g. the AWS Certified Security specialty) and Google Cloud. Often these pathways are accessible through a third-party training provider e.g. Cloud Academy.

A number of certification bodies have also invested in developing online-based pathways to enable users to learn and achieve relevant certification, which can complement and augment other forms of in-person training. For example, CompTIA Security+ offers a range of interactive labs, study guides and videos.

Further, there are also a range of dedicated cyber security training organisations that have been set up in the UK in recent years to help address the size of the cyber security recruitment pool. For example - Immersive Labs provides an interactive training platform for cyber security skills, with hands-on gamified labs that enables both new and experienced individuals to learn new capabilities. Capslock offers a cyber academy model for re-training individuals into a new cyber security career, with an Income Share Agreement in place which means individuals do not have to repay their tuition costs until they earn over £27k per annum. This model requires a 16 week full-time, or 26 week part-time bootcamp. In 2021, Capslock intend to reskill 200 adults into cyber security.

Case study – Immersive Labs

Immersive Labs provides a fully interactive, gamified and on-demand cyber skills platform. It delivers training based on continuous and real-time threat intelligence, meaning that it can be used by users of all levels (from those starting out in cyber security, to those experienced staff wanting to know more about how to tackle the latest threats).

Immersive Labs offers a range of targeted Digital Cyber Academies including:
Students' Digital Cyber Academy: This is free to those in part-time or full-time study in the US, UK, Australia, Singapore, Canada, Poland, Germany, the Netherlands and Switzerland. Students must have a university or college email address to register.

Veterans' Digital Cyber Academy: This enables veterans from any military background to develop hands-on cyber skills and earn recognition from leading cyber employers. Immersive Labs have partnered with TechVets to deliver this academy.

Neurodivergent Digital Cyber Academy: This academy is open to those within the neurodivergent community, and offers both a learning environment, and promotes job opportunities from businesses seeking to take on neurodiverse talent. Immersive Labs has partnered with the National Autistic Society / UK Cyber Security Forum to deliver this, including recently supporting IASME to develop and support a number of neurodiverse individuals to gain employment within the Worcester Community Security Operations Centre (SOC).

Further, the platform also enables upskilling of existing teams, and allows employers to uncover hidden potential cyber security talent within their teams. Some of the clients include the NHS, Falanx, and BT – where Immersive Labs has helped to support cyber security training.

Case study – Capslock

CAPSLOCK enables adults to re-train through cyber security bootcamps, delivered entirely online. It provides cyber security education through the CAPSLOCK curriculum, which covers a number of real-world cyber problem areas and teaches adults how to solve these in the workplace.

This includes problem areas such as People and Processes, Security by Design, Identity and Access Management, Offensive and Defensive Security, and Incident Response and Business Continuity, in addition to providing career coaching and impact skills.

In order to help students gain employment in cyber security once they have completed the training, it works in collaboration with a number of the UK's largest cyber security employers, including BT, BAE Systems, Deloitte, Dell, and Lloyds Banking Group. They also have an employer network and mentors representing over 60 UK cyber employers.

Further, Capslock also works closely with a range of certification bodies, and will support students receive up to five cyber security certifications through its training, including CompTIA Security+, ISO 27001 Foundation Certificate, CCSK (Certificate of Cloud Security Knowledge), BCS CISMP (Certificate of Information Security Management Principles) CE-CSP (Certified Cyber Security Practitioner), as well as memberships to the Chartered Institute of Information Security Professionals, and the British Computer Society.

In 2021, Capslock plan to re-skill 200 adults in cyber, through a 16-week intensive re-training course, delivered entirely online.

Armed Forces

Over 14,000 skilled and experienced personnel leave the Armed Forces every year. In total. 8,000 of these use the Career Transition Partnership which supports the transition from military to civilian life.

In 2018/19, of these personnel, 665 entered a Science, Research, Engineering and Tech Profession (SOC2010). Whilst it is not possible to estimate how many of these were in a cyber security role, the military is often viewed as one of the best sources of talent for the cyber security sector given the skills and expertise built up in service.

Initiatives such as SaluteMyJob have partnered with IBM to train ex-military personnel in cyber security fundamentals, and Security Operations Centre (SOC) overviews. The Defence Academy of the United Kingdom also offers a Cyber Foundation Pathway, which offers courses on practical networking and strategic cyber awareness for Ministry of Defence (MOD) civil servants and military personnel.

Attracting International Talent

In addition to upskilling the population, the cyber security recruitment pool can also be increased through exploring the UK's capacity to attract international talent, and encourage global knowledge transfer.

The Exceptional Talent (Tier 1) Visa previously enabled hundreds of tech talent from outside the UK to join cyber / tech firms (via Tech Nation). The Global Talent Visa has no formal cap, and includes cyber security experts.

3.6 Estimating the Size of the Cyber Security Recruitment Pool

3.6.1 Current Workforce Estimates

As highlighted in subsection 2.2, there are varying estimates of the size of the cyber security workforce, subject to definition and scoping.

However, using the data available to this research, we can provide a current estimation of the size of the current UK cyber security workforce, and use this estimate to help policy-makers and industry understand the scale of interventions that might be required to help address the perceived skills gap.

We draw upon the following sources to inform this estimation:

DCMS Cyber Security Sectoral Analysis

Since 2017, DCMS has tracked the size and scale of the UK's cyber security sector. Whilst this only covers Full Time Equivalent (FTE) employment related to cyber security roles, it provides a useful indicator of the scale of the number of jobs within the private sector related to the sale of cyber security products and services.

Table 3.7: Number of FTE employees within the UK cyber security sector

Year	Value	Increase	Annual Growth
2017	31,339		
2018 (Estimated as there was no study in 2018)	*36,000*	4,661	15%
2019	42,855	6,855	19%
2020	46,683	3,828	9%

Source: DCMS Cyber Security Sectoral Analysis

From this, we can identify that in the most recent year, **employment in the cyber security sector has grown by nine percent**, and has experienced double-digit growth in previous years.

ISC^2 Cyber Security Workforce Study

As stated previously, (ISC)^2 estimated in 2019 that the UK cyber security workforce had 289,000 professionals, and that this has increased to 365,823 in 2020 (an increase of 27 percent). The 2020 study has also estimated that the size of the cyber security workforce gap has decreased globally from 4m to 3.1m, and estimates a current UK workforce gap of c. 27,408 professionals.

However, DCMS estimates that in the UK, in 2019, there were 1.6m people employed in the 'Digital' sector. This would suggest that, if the ISC^2 estimate for the number of cyber security roles was used, approximately up to 1 in 5 digital roles would be in cyber security. It is the view of the research team that this figure may over-estimate the scale of cyber security employment in the UK workforce, and **we therefore treat the 365,823 figure with caution.**

Tech Partnership

In 2017, the Tech Partnership published that the UK cyber security workforce had reached 58,000 professionals by the end of 2016 – a significant increase from 22,000 in 2011 (an increase of 160 percent over the five year period.

Further, this research reflected those in salaried employment across the public and private sectors, and Tech Partnership estimated that approximately 12 percent of cyber security roles were within the UK public sector. This compares to 16 percent of all people in paid work being in the public sector, possibly suggesting that cyber security roles in the UK may be slightly more private sector facing.

Whilst this figure is a few years old, it provides a useful indication of the estimated size and scale of the sector in 2016.

If we assume that this workforce figure has grown by 14 percent per annum since then (i.e. the average annual growth reported in the UK Cyber Security Sectoral Analysis), then **it can be estimated that the cyber security workforce may have reached c. 98,000 by the end of 2020** using the Tech Partnership baseline. This figure is lower than the ISC^2 estimate, but captures private and public sector roles (i.e. a broader overview of the UK's cyber security workforce, rather than just the private 'cyber security sector' employment.

Cyber Skills in the UK Labour Market

This study explored the number of core (technical) cyber security job vacancies advertised in the UK, and the number of cyber 'enabled' vacancies in the UK using Burning Glass data.

Whilst there is some monthly variation within this data, the research identified that in the UK, there were approximately 3,000 core cyber security job postings, and a further 8,000 broader roles advertised online each month between 2016-2019[16].

In other words, for every core cyber security job vacancy posted in the UK, there are a further 2.67 'enabled' cyber security vacancies. However, it should be noted whilst many of these enabled vacancies may have some application to cyber security, it does not mean they are necessarily 'cyber security' roles in each case e.g. an 'IT analyst' with some responsibilities for information security.

If we apply this ratio to the number of FTEs working within the core cyber security sector, this might however imply a 'maximum' estimated cyber security workforce in the UK of c. 171,000.

Overall Workforce Estimation Scenarios

In absence of Standard Occupational Code data, it is challenging to identify the number of people working within a cyber security role within the UK. However, the previous data suggests the following:

- The core cyber security sector in the UK employs an estimated 46,683 FTEs (2020);
- The ISC^2 Cybersecurity Workforce Study estimates a UK cyber security workforce with 365,823 people;
- The Tech Partnership estimated a cyber security workforce of 58,000 for 2016. Applying an average industry growth rate of 14 percent (2016-2020), suggests that the cyber security workforce may be in the region of 98,000 by the end of 2020; and
- Exploring the Cyber Skills in the UK Labour Market data, whilst focused on demand, highlights that a broad definition of a 'cyber security role' can affect the number of roles in scope. We suggest that the number of job vacancies highlighted in the Burning Glass data may imply a maximum cyber security workforce in the UK of 171,000.

[16] In 2020, whilst there was a fall in job vacancies in Spring/Summer given the coronavirus pandemic, this has broadly recovered in the latter stages of the year.

On this basis, we estimate that the UK cyber security workforce is most likely to be in the region of 98,000 – 171,000 people. The mid-point estimate is therefore c. 134,500 individuals currently working in the UK cyber security workforce.

This would imply that there may be:

- Approximately 46,700 working within cyber security firms (offering a cyber security product or service to market);
- Approximately 11,800 – 20,500 working within cyber security roles in the public sector (assuming 12 percent of the cyber workforce are in the public sector); and
- Approximately 39,500 – 103,800 working within cyber security roles in private roles outside of the cyber security sector (e.g. CISO functions in finance firms) and academia.

Further, applying the most recent growth estimate (for employment, 9 percent) to the mid-estimate figure suggests that the workforce would need to take on c. 12,000 individuals per annum to meet increasing demand (from 2021 onwards). However, we do recognise that current labour market conditions may impact this growth estimate, and should be revisited in late 2021.

3.6.2 Inflows and Outflows to the Cyber Recruitment Pool

It is generally viewed that the cyber security labour market has a number of issues with respect to labour shortages, and challenges in identifying and securing talent. Further, the importance of cyber security to national prosperity and security means that workforce planning (i.e. understanding the current size, inflows, and outflows into the sector) can help policy-makers and industry understand the scale of the issue, and design interventions accordingly.

Inflows

In order to address the need for additional workers in the cyber security labour market, individuals need to undertake routes that demonstrate sufficient understanding and knowledge of cyber security to be employable within the field (i.e. inflows).

Whilst it is possible that there are several hundreds of thousands of people in the UK that could have the aptitude to undertake cyber security training or re-skilling (e.g. participate within a cyber security bootcamp), it is important to recognise that encouraging individuals to train in cyber security will also take time, and should ideally illustrate employment outcomes for those involved. In other words, there is a need to improve supply, we should be aware of the absorptive capacity of businesses and organisations to take on new cyber security talent in a sustainable way to help address the shortage over time.

With this in mind, we focus on the typical current estimated inflows into the cyber security labour market within a twelve month period. These include individuals that we consider have a likely potential to commence within a cyber security role.

Please note these figures reflect ‘new’ annual supply. For many organisations recruiting ‘experienced’ staff, they may be hiring from within the existing workforce estimates (or from aligned or similar digital sectors).

We estimate that these inflows include:

- **2,000 cyber security graduates (UK)**: As set out in Section 3.4, in the most recent year, there were 3,360 graduates from a cyber security focused undergraduate or postgraduate course in the UK. Based on Graduate Outcomes, we estimate that the labour market will attract c. 2,000 of these graduates to join the cyber security workforce.

  However, the number of enrolments in cyber courses increased 18 percent between 2017/18 and 2018/19, therefore this number is expected to rise in the future. We would also expect that, for many of these graduates, their outcomes will change from further study to employment at a later date, and we would anticipate that another 1,000 graduates (from the 2018/19) are likely to enter the cyber security recruitment pool at a later date, following further study.

  For analysis purposes, we use the 2,000 figure as a conservative estimate, but expect this could increase to over 3,000 per annum subject to supply of graduates.

- **2,000 Computer Science (and other similar) graduates (UK) entering cyber security roles:** As also set out in Section 3.4, in the most recent year, there were 30,886 Computer Science graduates (UK). Further, within the Cyber Skills in the UK Labour Market report, these qualifications are often requested by cyber security employers.

  It is not known what proportion of Computer Science graduates enter the cyber security labour market (given limited SOC data coverage). However, we estimate that of these graduates, approximately 16,000 will enter IT / digital related employment within a year of graduating.

  There will be a number of sectors competing for this talent; however, we assume that at least 10 percent[17] are entering cyber security related roles each year i.e. 1,600 individuals.

  As above, for analysis purposes, we round this figure to c. 2,000 as a conservative estimate, but expect this could also increase to over 3,000 - 4,000 per annum subject to supply of graduates, and increased demand from cyber security employers within the broader digital labour market.

- As set out within some of the case studies, cyber security employers can also recruit potential workers from the wider population, either directly or through the use of retraining or conversion courses. There is limited data on this route, but we estimate that it is possible that **up to 1,500 individuals** may currently enter the recruitment pool through this route. This is based upon knowledge of a number of initiatives identified across the UK e.g. Assured Skills Academies, pilot initiatives through CSIIF, Career Transition Partnership etc. There is considerable potential to scale this provision, as well as demand, particularly through the provision of funded opportunities to grow such initiatives.

- More than 600 individuals have started Degree Apprenticeships in 2018/19 (in England), and this number has been growing over the past three years. We estimate that, based on this growth, it is possible to anticipate **approximately 1,000 degree apprentices** in the UK could enter the cyber security recruitment pool each year in future, and these routes should be further encouraged.

- There are a number of case studies identified with respect to other initiatives targeted to attract workers into the UK cyber security recruitment pool, including attracting international talent (e.g. the Global Talent Visa), and also privately funded re-training initiatives (such as Capslock), or self-taught

[17] Based on the cyber security workforce range (i.e. 98,000 – 171,000) as a proportion of the DCMS Digital Sector Economic Estimates (Employment) c. 1.6m.

online training. Whilst there is limited data, we assume such initiatives could currently provide c. **1,000 additional individuals** to the cyber recruitment pool per year.

In total, these estimates would suggest there may be approximately 7,500 new individuals entering the cyber security recruitment pool each year (with a realistic likelihood of receiving an employment outcome).

Outflows

DCMS Cyber Skills in the UK Labour Market (2021) suggests that up to six percent of the current cyber workforce leave their employer each year for any given reason. This could also potentially include employer to employer movement.

We further estimate an outflow figure (to the industry) of c. four percent for this analysis (i.e. at least one in every 25 working in the cyber security labour market leave each year due to retirement, migration, or moving to another non-cyber security related role).

Applying this estimate to the workforce range suggests that between 4,000 – 7,000 (mid-point, 5,500) staff could be exiting the cyber security workforce each year.

Further, some literature and survey data suggests that, more could be done to alleviate this figure, which could have the potential to rise in the future given that as the industry grows, there is considerable pressure exerted on senior staff within cyber security – particularly CISOs. The Nominet CISO Survey (2020) sets out that 88 percent of CISOs are ‘moderately or tremendously stressed’, with 48 percent reporting a negative impact on their mental health.

In addition, often cyber security is viewed as a ‘young industry’. However, only 37 percent of cyber security staff are estimated to be under the age of 35 (ISC^2 estimate, 2019). An estimated 29 percent of the workforce are over the age of 45 – and the average age of a cyber professional is 42.

Longer term, increased demand alongside increasing retirement could be challenging for the growth and sustainability of the sector – particularly when ensuring experience and knowledge of legacy systems / processes can be shared.

This indicates that there is an even greater need to increase the inflows into the cyber security recruitment pool.

3.7 Estimating the Cyber Workforce Gap (Key Findings)

The Cyber Skills in the UK Labour Market research (2021) has indicated that despite the economic impact of COVID-19, there remains strong demand in the UK for cyber security professionals. Indeed, COVID-19 has placed a renewed emphasis upon existing employers to consider their approach to recruitment, training, and roles for new staff (and upskilling of existing staff).

This research paper suggests that, taking the mid-point of the estimates for the current cyber security workforce, inflows and outflows, there is a quantified gap between the number of new staff demanded by the UK cyber security labour market, and the volume supplied by existing education and training provision.

Overall, this research suggests that:

- The current UK cyber security workforce currently has an estimated 98,000 (low) – 171,000 (high) employees. We take the mid-point for modelling purposes (i.e. 134,500 individuals).

- The demand for cyber security professionals has grown by an average of 14 percent per annum since 2016. In the most recent year, it has grown by nine percent. This implies that the UK cyber security workforce would need to grow by approximately 12,000 people per annum (to meet demand). However, we do recognise that this assumes a direct relationship between demand and employment (which may be partially affected by processes such as automation and labour costs).

- The cyber security workforce is also losing approximately 4,000 – 7,000 (mid-point of 5,500) people each year.

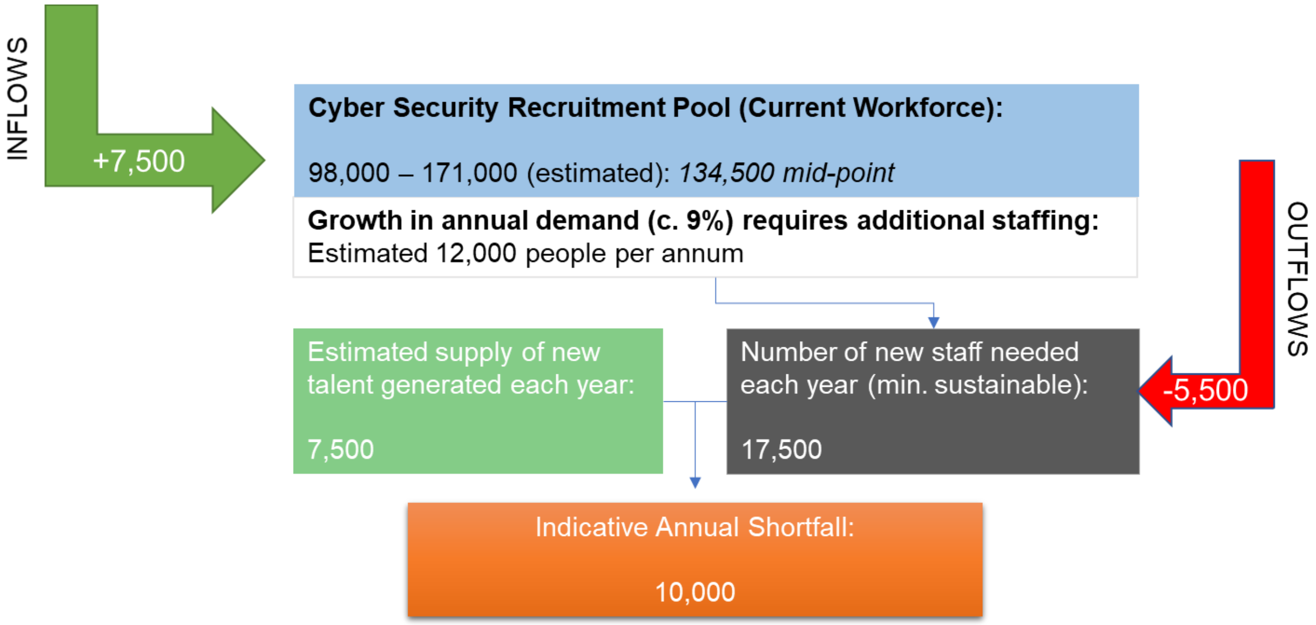
- In total, this implies that the UK cyber security workforce needs to attract at least 17,500 people each year to meet new demand and replace lost workers. This broadly aligns with the Cyber Skills in the UK Labour Market research, which indicates there were 33,662 online job vacancies posted by employers in the UK seeking core cyber security talent.

- With respect to inflows, we estimate that there are approximately 7,500 **new** individuals entering into a cyber security career each year. This figure could be increased through re-training initiatives, support with certifications and skills, and potentially expansion of the volume enrolled in higher and further education courses.

- This implies that the UK should be attracting c. 17,500 new people each year into cyber security employment to meet demand, but is only generating c. 7,500 in new supply. **This suggests an annual shortfall (2021) of c. 10,000 people**, and this is in addition to existing perceived shortage of talent currently, as well as potential for further demand to increase in future. In other words, this highlights that the cyber skills shortage is an ongoing challenge, that needs to be addressed rapidly in order to mitigate some of the resulting issues (e.g. loss of talent and experience, challenges in staff retention and productivity, risk of staff burnout etc.).

- This also suggests, left untreated, the extent of the shortfall will continue to worsen, as cyber security remains an area where demand for talent exceeds supply.

Figure 3.18: Summary of Inflows, Recruitment Pool, and Outflows


INFLOWS
+7,500
Cyber Security Recruitment Pool (Current Workforce):
98,000 – 171,000 (estimated): *134,500 mid-point*
Growth in annual demand (c. 9%) requires additional staffing:
Estimated 12,000 people per annum
Estimated supply of new talent generated each year:
7,500
Number of new staff needed each year (min. sustainable):
17,500
-5,500
OUTFLOWS
Indicative Annual Shortfall:
10,000

Source: Perspective Economics (Summary of Recruitment Pool estimates)

However, this should also provide an opportunity for public and private sector organisations to identify the scale of the challenge ahead, and to fund and deliver interventions that can meaningfully address these shortages.

Within the UK, the current working age population contains approximately 36.3m people. There can be a renewed emphasis on how reskilling in cyber security offers people an opportunity to attain a rewarding career, whilst also supporting wider ambitions for Levelling Up, and supporting people to upskill over a life-long period.

We therefore suggest that this research indicates, with an annual shortfall of an estimated 10,000 people per annum (and likely to grow with demand), targeted interventions should be explored to help rapidly increase the supply of potential cyber security talent. Further, this figure suggests that interventions to the scale of generating an additional c. 300 people per 1m of working age population (on top of existing supply) would help to address this annual shortfall.

Indeed, the learning from the Cyber Skills Immediate Impact Fund projects and a range of devolved and local LEP skills plans suggests that a blend of regional, national, and online interventions may be best suited to help tackle the workforce gap. For example, providing a three month cyber security bootcamp backed by a regional employer may result in hundreds of new employment outcomes for those starting out in cyber security. These staff will then learn on the job, can continue to upskill, and will provide the experience needed in the years ahead.

Overall, investment in enabling current re-training initiatives to scale in the coming years will be critical to increasing the tangible supply of cyber security talent. Further, the current economic climate means that a number of training providers have reported that there is much greater demand for engaging in retraining initiatives. This offers a route for the UK to increase digital skills and productivity in the next 12-18 months and should be utilised rapidly.

4 Qualitative Findings

4.1 Introduction

The research team have undertaken 25 in-depth interviews with relevant UK-based stakeholders (six employers, six recruitment agents, six employees, and seven training providers). These discussions have focused on providing a greater context and understanding of the recruitment pool, with indicative quantitative and qualitative insights to better inform the reliability of the estimates from the secondary data.

4.2 The makeup of the recruitment pool

4.2.1 Current views on the pool

This subsection provides views about the size and quality of the recruitment pool and how this has changed in the past few years. It also provides evidence of the motivating factors which could explain these changes.

As evidenced from the quantitative study, employers felt that it was challenging to match a candidate's skills and experience to the requirements of the role.

"I think those that balance cyber security skillsets with genuine cyber security experience, they're slim to none. There's plenty of IT people, but it's difficult to find cyber defence experts. There's a small pool of people we can recruit from."
Employer, Large multi-national firm

However, they felt that the number of candidates applying for roles had increased over the past few years. They were keen to stress that this did not necessarily lead to an increase in the quality of candidates. This view was reinforced by recruitment agents.

"You get a lot more 'blag artists' that try to exaggerate their cyber security experience. A lot of candidates have IT leadership experience, but you've got to understand what they're doing with regards to security specifically. You've got to really understand the market to be able to weed out those candidates."
Recruitment agent

Recruitment agents felt that the pool had changed in recent years. They felt that there had been a rise in demand from employers for roles relating to training and awareness. They also felt that candidates were quite specific with their job requirements. The company had to remunerate generously, be committed to the ethos of cyber security, offer career progression and also offer a role that gave candidates the opportunity to sit exactly where they saw themselves within the sector.

"In a company candidates value progression, that they understand cyber security as an enabler rather than a cost, not held to one particular expertise to get a broader perspective."
Recruitment Agent

Though employers struggled to fill roles, training providers have seen huge demand for people to reskill, particularly since the coronavirus pandemic, with candidates looking for a secure form of employment:

"Having looked at the recruitment campaigns they have done for CSIIF programme to attract people from a non-IT background into cyber, the audience is huge there. For one of the CSIIF programmes we had 30 places but 1,500-2,000 applicants and still get them coming through

because of links on government websites. There is never a fear that we won't have enough candidates, we are swamped."
Training Provider

4.2.2 Identifying candidates

To identify suitable candidates, employers need to engage with the labour market through multiple routes. This included working with specialist recruiters, encouraging employee referrals, and ensuring that the next generation are aware of their organisation as a potential location to join and develop.

Recruiters' approach to identifying candidates depended on the role they have been asked to recruit for. For more senior roles personal networking at tech or security events was most effective and allowed recruiters to suitably match candidate and organisation. For more junior roles, particularly those at entry level, keyword searches via tools such as LinkedIn and candidates directly registering with the recruiter were most effective.

4.2.3 Indicative Candidate Success Ratios

Within the consultations, employers were asked about the ratio of applications they received for a role. The responses varied from 10:1 to 33:1, demonstrating there is a high volume of applications, but employers noted the difficulty in finding suitable applicants. However, consultees noted a balance needed to be struck. One consultee stated that there was no perfect candidate and that training would always be required:

"There's always a balance, the work needs to be done and someone needs to be hired. We can't hold out for the golden candidate, but then I'm not willing to take a bigger risk."
Employer, Large multi-national firm

Further, a consultee noted that there is a need for businesses to consider and reflect upon their demand for talent:

"There is a tossup of expectations and experience. People with 10 years of cyber security experience might not exist when recruiting for senior roles. However, it's only going to get better [in next five years]. There's three jobs for one candidate, it will become more prevalent, and the universities will catch up with what a cyber info sec person looks like, they'll build a more rounded candidate."
Employer, Large multi-national firm

4.2.4 Enablers and barriers of getting into cyber roles

Employers were asked what characteristics, qualities or attributes they required from those coming through the recruitment pool. They tended to cite complementary skills as most important, believing candidates could be trained in more technical skills. This was particularly the case for junior candidates.

"We want those who are reliable, knowledgeable, who can work in a team, with a background in what they are asking them to do (if mid/senior role). If it's a junior role, with no experience, we are looking for aptitude more than particular qualifications."
Employer, Large multi-national firm

"We've had good luck with reskilling and upskilling people who have an IT background into cyber security. We used branded software in many cases, so we have to teach them about that software even if they are familiar with the technology."

Employer, Large multi-national firm

However, they were keen for candidates to have some cyber experience (at least 3 to 5 years). This was driven by customer demand. They were several other factors which limited their recruitment pool:

- A strict definition of what cyber security meant. Employers were not often keen to recruit IT professionals more generally.
- Some subsectors, such as defence and security, require extensive vetting and clearance before hiring candidates.
- Employers would be biased towards their head office location (often London). They may then be able to hire other candidates from elsewhere to improve geographical diversity once they had opened other premises.

Recruitment agents felt that good cyber security candidates needed a range of skills and accreditations in order to be accepted into roles. There was a sense that employers were often looking for 'unicorns' to fill cyber roles.

"Cyber security is not one of those areas within tech that you typically associate with sitting on your own and coding, for example... with cyber you need that element of interpersonal skills as well."
Recruitment Agent

They felt that highly skilled candidates were being rejected because they did not have the right accreditations, despite having demonstrable technical capability.

"CISSP (Certified Information Systems Security Professional) is a barrier - some of the most capable people don't have it. But it's such a straightforward thing for an employer to put on a post as a filter. It's a lazy way of recruiting because employers don't have time. Others are CISM (Certified Information Security Manager) - again need to have a number of years of experience. ISO 27001 as well. Maybe also CRISC (Certified in Risk and Information Systems Control) are consistently banded into job roles. This is not letting up because the education of HR people hasn't changed."
Recruitment Agent

4.2.5 Groups entering the pool

At entry level there is a heavy graduate focus on those entering the pool. Employers and training providers felt this could be widened with more focused apprenticeships and NVQ Level 4 qualifications.

Those entering the pool from other sectors tended to come from a variety of areas:

- Professional services: Those in generic leadership roles were also able to transfer to cyber consultancy firms.
- Public services: These came from defence and security areas such as the police or military. Skills were transferred from protection and conflict resolution. Candidates from the teaching profession also entered the pool. Complementary skills relating to communicating complex information clearly were transferable to cyber security.

- Trades: Though not as common as the above two areas, these included professions such as mechanical engineering and plumbing. They tended to be self-employed. Employees entering the pool felt their problem-solving skills were transferable into cyber security.

Employees tended to be motivated by a desire for change, an interest for cyber security, and feeling their complementary skills matched their role.

"I set up alerts and this training one just came in... I tended to really quickly flick through them... and that's when I started to read into it. Training was non-committal and you hear cyber security sounds interesting and fascinating... if nothing else I'll have a new qualification and that will never go to waste."
Employee

Training providers stated that entrants on their courses came from a variety of backgrounds, and tailored their content as such.

"I've seen in recent months pilots, because of what has happened, air hosts and hostesses, carpenters. You name it, we've seen it."
Training provider

They also noted that they had candidates from IT and technical backgrounds who would sign up to intermediate to advanced courses with a view of looking to go into cyber security roles.

A low proportion of candidates applied from diverse groups. One London based recruiter noted the following when it came to candidates they were trying to place into roles:

- Proportion of candidates they speak to that are from ethnic minority backgrounds: 20-25 percent.

- Proportion of candidates they speak to that are female 30 percent.

- Proportion of candidates they speak to that have a neurodiverse condition: 5-10 percent.

There were various factors which determined whether a candidate was suitable for a job role. Primarily, training providers felt their qualifications highlighted talented and driven candidates and supported them in gaining an entry level role without prior cyber experience. They felt this was particularly the case for women. Employees interviewed also noted how training courses had helped them into cyber roles. However, it was noted that for those going into non-graduate roles, prior work experience was essential (and more important than qualifications).

"Female candidates have done extremely well. Had a single mother of 4 who got a part time cyber job role, she did extremely well. Six months after graduating from the course she was on a Black Hat panel."
Training Provider

Employers tended to focus on a mix of technical and complementary skills among potential employees. Those employers with a greater focus on complementary skills would invest in the technical training of candidates. Those focusing on candidates with particular technical skills tended to struggle to find suitable candidates.

Employees mentioned their networks with cyber security professionals as a key route into cyber. For those in leadership roles, an additional factor in securing a job role was their experience in senior positions, as opposed to technical skills.

There were barriers that limited the number entering the pool, and the key barriers mentioned by consultees were:

- **Awareness of cyber as a career:** Training providers felt that not all candidates were aware that cyber was a viable career option. This was particularly the case amongst women, consultees from ethnic minority backgrounds, and those without a university degree. This led to candidates not understanding what skills they needed before applying to a role.

- **Perceptions of cyber:** There was a misperception of what cyber security careers entailed. Employers felt that education leavers regarded cyber security either as a typical coding job and was male orientated. This discouraged candidates, particularly females.

- **Cost of training programmes:** This was a barrier to those trying to get more technical cyber accreditations such as CISSP. Some training providers felt this was a barrier and stated it led to free programmes being oversubscribed. Recruitment agents also noted that some candidates paid for training courses with less reputable providers.

"It has got to go mainstream and the first step in that is stopping the artificial barriers which are these very expensive high-end qualifications. You don't actually need someone to be a top Penetration testing expert to pen test the power grid."
Training providers

- **University courses:** Training providers felt that university courses did not adequately prepare candidates for cyber roles. They felt courses did not teach candidates how to apply the knowledge they had gained.

- **Employer attitudes:** This was a perceived barrier. Some employers mentioned a need for extensive technical and cyber security experience before they would consider a candidate appropriate.

- **Recruitment processes:** A barrier to diversity in the pool. Neurodiverse specialists mentioned the process was not suitable for neurodivergent groups. They felt the job advertisements were complex, did not define the expectations of the role, and just listed a series of skills and qualifications. The interview process was regarded as too formal and structured. It was often male dominated, which made it challenging for suitable female candidates to be hired.

"A cyber security job advert is a long list of skills and knowledge and certifications. It is obscenely horrible!"
Training provider

Employers felt there were ways to overcome challenges of encouraging education leavers into the recruitment pool:

- **Breaking down stereotypes:** Employers felt challenging the stereotype of a cyber worker and making those in education aware of how varied a cyber security career was would help increase the candidate pool.

- **Engaging with the curriculum and extra-curricular activities:** Employers felt that there could be better cyber security engagement with and from schools. They felt if schools understood schemes better (such as CyberFirst) they could give better careers advice.

"My son is studying GCSE computing and the syllabus for that isn't good. He did the NCSC's summer school which he thoroughly enjoyed and asked why aren't they teaching that on the GCSE curriculum"
Employer, Small UK based cyber firm

4.2.6 Career Progression and Outflows

A typical route through cyber security tends to start with a wide exposure to different facets of cyber, with employers training employees in specific technical skills and relevant soft skills, such as presentations and communicating with non-specialist staff. They will then progress into a specialism, such as penetration testing, or systems architecture, before widening their role as they move into leadership positions, where softer skills become more important.

Career progression is facilitated by the employer and candidate qualifications. Employers will create career pathways via training and will then hire external providers to further enhance specialist technical skills. Some encouraged candidates to gain further qualifications. However, there are numerous barriers to career progression:

- **Specialism conundrum:** As leaders needed a diverse set of skills, becoming an expert in a specialism risked becoming a ceiling to leadership.

- **Diversity beyond entry level:** Diversity was high in terms of ethnic minority backgrounds and neurodiversity on pathway training courses and at entry level. This decreased with seniority. This was exacerbated as recruiters stated they found it challenging to directly make case for talented ethnic minority background and female staff due to lack of experience.

- **Networking**: CISOs have quite a closed network and can be hard to break into a role from the outside. Once in a role, cultural issues mean it can be a challenging working environment for women, which leads to outflows.

Despite these barriers, outflows are rare in cyber security. This tends to happen as candidates progress from mid to leadership level. One of the main reasons for outflows was suggested to be a toxic working environment for women, causing them to leave the profession, or through them not being taken seriously as suitable senior candidates for roles such as CISOs. This also affects ethnic minority candidates:

"I have seen minority candidates pushed out of the industry because it's too difficult to progress. People end up in roles they're overqualified for, they accept this, then they're no longer eligible for cyber security roles because they've been away from it for so long. This leads to a skills gap."
Recruitment Agent

Another cause of outflow stems from those in leadership roles wanting to remain technical specialists. This leads to them to leave their organisation and become freelancers or contractors.

4.3 Skillset within the pool

4.3.1 Types of skills within the pool

Consultees mentioned a varied and diverse set of skills within the cyber recruitment pool. These can be broadly categorised as technical and softer skills.

Technical skills employers and recruitment agents regarded as essential related to the ability to understand networks and systems, and the ability to implement such systems. They also felt that a cyber security degree or accreditation was important. Employers would then look at the more specific experience or qualifications presented by those in specialist roles, such as security architecture and penetration testing.

Softer skills were varied. Those working in more technical roles needed to have good analytical skills, an ability to solve problems, and a sense of determination. It was noted that those working in consultancy or in leadership roles had strong communication and interpersonal skills which were desirable to employers in the cyber sector. Good project management skills as well as an ability to communicate complex information simply were desirable across all roles within cyber security.

It was highlighted by consultees that it was not essential for individuals to have extensive technical and softer skills. Rather, it was crucial for organisations as a whole to have the full range of required skillsets found within the pool amongst their wider body of staff.

“There are some technical people with an absolutely massive EQ (Emotional Quotient) and then some socially clunky people who are exceptionally good technically, but their people skills leave some room for improvement.”
Employee

4.3.2 Level of technical expertise within the pool

Consultees felt that the level of technical expertise varied by career stage. At entry-level there tended to be low technical expertise. To alleviate this, employees are trained on their skills gaps before selecting a specialism. One exception was for those entering the pool with a cyber security specific degree, where technical expertise was high, but complementary skills were lacking.

The highest level of technical expertise comes within mid-level roles, where specialisms such as network engineering were more prevalent. At more senior levels, such as CISO or an MD of a cyber specialist business, the role tends to broaden. Recruitment agents specialising is senior hires felt the focus was more on softer skills, such as managing people, communication and decision making. However, demonstrable technical expertise was still essential, even if at a high level.

"Obviously if I need a reverse malware engineer, I will scrutinise their qualifications in that field. If I'm looking for a managerial position, I'm looking at their leadership. The higher the position I'm looking at managerial skills. Different skillsets on soft skills."
Employer, large multi-national firm

Employers felt that there was a skills gap when it came to mid-level specialisms, particularly for engineering, penetration testing, or architecture roles. They felt it was difficult to find employees who could clearly demonstrate that they had the core skills to undertake these roles, meaning the candidate pool was too limited.

"If the position has 'engineer' in the title, those take the longest to fill. Where you are really looking for deep subject matter expertise and a bit of work experience… a network security engineer, a firewall engineer, encryption or key management engineer."
Employer, large multi-national cyber firm

However, training providers and employees felt that employers were being too specific when it came to recruiting suitable candidates. Employees felt that a stronger focus on relevant soft skills by employers would help increase the supply. For instance, employees with problem solving and analytical skills felt they developed technical skills through in-depth on the job training. Training providers felt that employers wanted too much in terms of both work experience and qualifications, when only one of the two would allow them to source a suitable candidate.

"Soft skills count massively and in our programme we do try and make sure people are answering questions, feeding back. It is a key component to working in cyber because if you can't work as a team, how can you function in that job role?"
Training provider

4.3.3 Developing skills

In order to broaden the skills of individuals in the pool, improve its quality, and increase suitable new entrants, candidates' skills were developed through a number of means:

- **On the job training:** Employers acknowledged that cyber security was a fast-evolving area. Therefore, they upskilled their technical staff to become proficient in managing new types of risk. **Secondly**, they would train highly technical staff on softer skills such as managing others and presentations with a view to promoting them to senior roles. Entry level candidates were trained via graduate style schemes to give them exposure to the technical aspects of their role.

"My entire career, a lot of it has been learning on the job. Especially in cyber security as it is moving so fast. And the more I learn, the more I understand what I don't know."
Employee

- **Gaining further technical accreditation:** For those that wanted to move into more senior or specialist role, further accreditation was essential. CISSP was frequently cited by consultees as a qualification that employers would regard as desirable on job adverts.

"CISSP is seen as a top qualification but that doesn't give the true picture. People see CISSP as for people who have been five years in the industry, but what we need is to get more people into the industry."
Training Provider

- **Online courses**: There were a variety of online courses for entry level candidates to self-teach and gain technical skills in cyber security. This is a growth area with a high level of demand. The COVID-19 pandemic has exacerbated this. However, consultees noted that those enrolled in free online courses were unlikely to complete the course, particularly when compared with those who were on a paid course.

- **Specialist training**: In order to encourage greater diversity in the pool, there are specialist training options. For instance, there are dedicated training providers for those with neurodiverse conditions. There are also online course providers who targeted under-represented groups such as women and those from deprived areas. Groups were recruited via FE colleges and charities and communities. Training providers also tailored their content based on level of experience within cyber or IT.

There were also suggestions amongst employers that they should look to retrain generalist IT staff internally, in order to increase the pool and satisfy demand. However, challenges were noted in trying to encourage those with more generalist IT skills to retrain into cyber. One training provider noted the following:

"Industry's frustration is that there isn't a pool of experienced tech people, in broad brush terms, who are willing to completely refresh their skills. There appears to be an age and an attitude limit and are happy to gracefully end their careers without doing that big push to reskill. Both people in IT who could move into cyber and people in cyber whose skills are going out of date."
Training Provider

Case study – CompTIA CyberReady

CompTIA's Cyber Ready programme takes graduates and IT technicians thorough a six months training towards a cyber analyst role and other cyber security related employment. On top of market observation, training pathways are developed in close partnership with cyber organisations (mostly SMEs) and security experts.

The range of their programmes covers all levels of seniority, however they stated that the focus needs to be on entry-level roles – *"what we need is to get more people into the industry".* For these, premium qualifications such as CISSP are regarded as being too advanced. As a result, they have developed a range of beginner and intermediate courses aimed to facilitate entry to more junior roles. They feel demand for this has been substantial and they are oversubscribed.

Despite oversubscription, poor awareness of cyber security can make it challenging to find talented graduates and suitable learners. Especially from a re-skilling perspective, many applicants are lured in by the prospect of high pay. This is especially the case for those who recently lost work and income because of the coronavirus pandemic. Here, people seem to lack basic understanding of what a career in cyber entails and thus fail the key examinations. On the other hand, those who do pass the exams and are awarded the qualifications, have the knowledge and ability to gain a competitive advantage and fill roles they apply for.

On diversity, they think there is little they can do as an organisation. The focus must be in the early years of people's education to establish a solid interest towards cyber across a more varied range of demographics. They appreciated the work done by CyberFirst, but they believed there is more to be done. For example, they mentioned an initiative CompTIA runs in the USA called TechGirlz, which inspires secondary school girls to explore careers in technology - "There's no point in saying let's have more girls when girls are thinking that it is a geeky subject or not for them."

Finally, in terms of geography, they are conscious of diversifying the pool away from the South East of England. One of the issues, for now, is the lack of work opportunities in the North East for example. This limits the diversity of the geographical spread.

4.4 Diversity within the recruitment pool

Consultees tended to agree that a diverse group of candidates was critical to a high-quality recruitment pool. It was emphasised that employees needed to be from a range of backgrounds and methods of thinking for employers to be able to have robust cyber security in place. Consultees noted that whilst some improvement had been made in recent years, there were challenges placing employees from diverse groups in roles and this required improvement.

"We cannot continue to target red brick 2.1 cyber degrees. We need to go non-linear, we need to look at all kinds of backgrounds and figure out ways to appeal to people from all those backgrounds rather than when a job comes up just taking it to your usual recruitment consultant. We need to be much more creative than that."
Employee – with hiring responsibilities

4.4.1 Neurodiversity

Placing candidates from neurodiverse backgrounds in roles was noted as an important challenge for the cyber security sector to address. Increasingly, the notion of coming up with diverse solutions to problems as a result of employing neurodiverse candidates was regarded as important within the sector.

"Neurodiversity brings some exceptional skills and having a better grasp around that is going to be important for industry. Getting neurodiversity into the workplace is going to raise the quality of our output. But it needs to be treated differently, don't just treat neurodiverse people the same as other employees. It is a different style of leadership and management."
Employee

Neurodiversity specialists and neurodivergent individuals interviewed noted some challenges:

- The recruitment process generally was aimed at those from a neurotypical background. Consultees felt that the traditional interview approach was ineffective in demonstrating the skills and experience of neurodivergent candidates, with them often feeling uncomfortable during the process. Job advertisements could be more accessible to neurodiverse candidates, with the extensive list of experience and qualifications being overwhelming. There was also a sense that employers could be more lenient towards neurodiverse candidates on their previous work experience. This was because they may face challenges to adapt to certain roles if the employer does not create a suitable working environment for them.

- Once in roles there was a risk that neurodiverse employees would not remain there for a sustained period of time. Consultees felt employers could do more to create suitable working environments for neurodiverse employees. There was a sense that employers did not always understand the needs of those from neurodiverse backgrounds, particularly those with more complex conditions. They felt employers could create links with autism charities to help alleviate this. Employees noted that employers that had been successful in this had a bespoke induction process for individual employees.

- Training providers felt that their offering could be more accessible in terms of how they teach neurodiverse candidates. Online training providers noted that they were improving their accessibility to neurodiverse candidates, though did not detail methods used.

"My experience with neurodiversity is that people say they want to employ neurodiverse people and are open to neurodiverse people but they only want the easy ones. They want neurodiverse people who can pretend not to be. As soon as you get to the really difficult problems and barriers, then they don't want it. The relationship can break down. That is why it is so important to have someone who can communicate between the individual and employer."
Training Provider

However, there were opportunities to help overcome challenges. Specialist neurodiverse training providers have been set up to encourage neurodiverse candidates into cyber security roles. They tailor training methods to upskill neurodivergent candidates in technical skills. They then offer a more bespoke programme where neurodivergent candidates are advised on how to approach job applications and interviews in a neurotypical environment. However, training is currently localised dependent on the provider, and providers felt it was therefore important for them to build links with large employers. They could then use these links to potentially put neurodiverse candidates into placements.

4.4.2 Demographic diversity

Consultees mentioned that minority groups and women are under-represented in cyber security, but there are opportunities to alleviate this.

Consultees stated there was low female representation across all levels. They felt this was caused by the perception cyber careers had amongst women, with it being regarded as a masculine profession. A lack of female representation was particularly prevalent at leadership levels. Recruitment agents felt that this was because of a cultural issue, where cyber leaders' networks were too tight-knitted, leading to an 'old boys' attitude to hiring new leaders.

"It is possible to break into the industry but if we don't give girls the belief that it is an industry for them then we are never going to break that mould."
Employer, small UK cyber firm

Ethnic minority candidates were also seen to be under-represented at leadership level. There was a sense that this was because of promotion and recruitment processes not being transparent enough. It was perceived that white and male candidates were better able to develop relationships with senior leaders, who were likely to also be white and male. There was also seen to be too much focus on education and qualifications in recruitment and progression, which candidates from middle-class backgrounds, who were more likely to be white, were better able to afford. However, it was mentioned that the pool was more representative at entry level.

Employers, employees and recruitment agents all noted that those leaving education with FE qualifications were under-represented. They felt this was caused by a mix of course content not preparing candidates to find a role and employer believing degrees were essential.

There also seemed to be some resistance to change from employers in fully addressing having a cyber workforce more representative of the wider population. Recruitment agents also felt this was the case. Employers felt that as their recruitment process were open to anyone for application, they did not feel any fundamental issues to their processes needed addressing.

"I think there's a massive gap in the UK, I don't think it's going to change anytime soon because of the internal cultures."
Recruitment Agent

4.4.3 Opportunities to improve diversity

Consultees noted there were opportunities and solutions to improve demographic diversity. Firstly, they felt that employers were too minded to hire from Russell Group universities, where graduates were more likely to be from white, male and middle-class backgrounds. They felt that if schools and FE training providers adapted and future-proofed courses there would be more candidates suitable for employment leaving education. Increasing cyber engagement in schools would help alleviate the *"boffin image"* surrounding cyber security, with entry-level candidates clear on what they can expect from a cyber security role.

“We hosted a CyberFirst event, with 50 girls in the facility. “When I had those girls hold up their hand if one of their parents worked in IT, nearly every hand went up. Kids aren’t necessarily hearing about roles in IT and cyber security from their schools, they are hearing about it from their parents.”
Employer, large multi-national cyber firm

There were also suggested solutions for improving the chances of female and ethnic minority candidates making it to interview and being offered roles. Recruitment agents felt that more personal relationships with hiring managers would help solve this. They felt that talented individuals were being denied the chance to interview, because they did not match all of the criteria on job advertisements, having not had the opportunity to gain experience or qualifications. They stated that had they been able to make the case directly to hiring managers, then candidate CVs would not have been filtered out by HR departments.

As mentioned previously, job descriptions were criticised by consultees. They felt employers were looking for unrealistic candidates, which discouraged those that did not have the opportunity to gain extra qualifications from applying. This meant consultees felt more focused job advertisements would encourage applications from a more diverse range of candidates.

“It really is a wish list for employers. I know they are trying to make things easier by putting things that are desirable but they really need to make it very clear that these are added things rather than you need to have that. The job ads need to be looked at.”
Training Provider

Employees and recruitment agents felt that blind recruitment would help improve diversity in the pool. By limiting what employers knew about candidates outside of skills, experience and qualifications, there would be less chance of affinity bias from hiring managers. In leadership positions, this would help mitigate the issue of old boys’ networks being used to secure job offers.

"We should be pushing for more blind recruitment. Doing something like this may really help create a more diverse workforce. Now, there isn't any blind recruitment going on.”
Recruitment Agent

Training providers were also seen to have a role in improving diversity. Face-to-face training is centred around areas with a high proportion of cyber employers, such as London or Cheltenham. This acts as a barrier to skilled candidates not local to those regions. Therefore, there is an opportunity to expand regional offerings, or undertake more virtual training.

Along with neurodiverse specialist providers, more general training providers had taken steps to improve diversity of entrants. One provider stated they are improving the accessibility of their training by linking with women’s charities and targeting areas with high socio-economic deprivation.

“Our whole thing is to try to get completely free training with volunteer support to target people who are unemployed but particularly to target ethnic minorities, but also neurodiverse people, women to some extent but there are lots of organisations that are doing that for women.” *Training Provider*

4.5 Impact of the coronavirus pandemic

The coronavirus pandemic had had both positive and negative impacts on the cyber recruitment pool. In general, employer sentiment was that the impacts of the coronavirus pandemic on the cyber security employment landscape have been more limited than in other sectors.

4.5.1 Opportunities presented by the coronavirus pandemic

Consultees believed that the quantity of the pool had increased as a result of the pandemic.

Employers and recruitment agents thought that candidates had recently been made redundant or furloughed from industries such as aviation, finance, engineering, and telecoms had expanded the pool. Therefore, individuals with such experience could feasibly be retrained with the right support. Recruitment agents estimated tenfold increases in the number of applications they had seen.

"There are generally more candidates in the market from particular industries like airlines which have downsized or gone under. It's really impacted the number of jobs as well. There's a higher demand for technical skills and there's certain areas that have definitely had an increase in demand, e.g., SecDevOps; engineers; incident response and digital forensics, cloud security architects."
Recruitment agent

Candidates previously working in other sectors had also hypothesised this, with one employee interviewed stating that they had moved roles from a large retailer into cyber security because of a perception of improved job security. There was also a sense that cyber security was both an industry likely to be set up well for remote working, and also a growth industry because of the nationwide increase in remote working. Further, employers had noted there was less turnover of existing cyber security staff:

"People hunker down and wouldn't necessarily change jobs so we haven't had to recruit as much as normal."
Employer, large multi-national firm

The increase in remote working has given those outside of traditional cyber security centres, such as London and Cheltenham, the potential to enter the pool and improve its geographical diversity. An employer noted that whilst location was previously a challenge (where staff needed to relocate etc), they viewed that remote working could become more prevalent across the UK in future. This was perceived to increase numbers in the pool by making the sector more accessible to suitable entry-level candidates.

4.5.2 Challenges presented by the coronavirus pandemic

Though opportunities had been presented, consultees noted challenges too. Firstly, training providers felt they had struggled to adapt their methods to train entrants remotely. Training providers felt that this meant candidates would not be well enough prepared to then secure employment in cyber security.

"Corona has been a good driver, but e-learning has its limitations - humans learn from humans. A Warwick study on MOOCs (Massive Open Online Courses) found that only 13 percent of people actually complete the course. There's no motivation to complete it. It's a bit scary to be going down that route [e-learning] and expecting people to be competent at the end of it."
Training provider

The second challenge employers raised related to their own recruitment methods. They felt that the risks posed by the coronavirus pandemic meant they would be more risk-averse in hiring staff who did not exactly fit the job description. Smaller employers were reluctant to hire outside of their own personal networks. One employer noted that they were currently more likely to hire freelancers as they could not hire permanent staff because of the uncertain economic situation. They mentioned that freelancers would more likely be experienced, white, male and neurotypical. This would exacerbate a problem in hiring candidates who would need some on-the-job technical training once in their role. It would also limit opportunities at entry level and to a more diverse range of candidates. The lack of opportunities may see greater outflows from the pool.

Thirdly, some recruiters have noted a potential risk that some regions in the UK with lower salaries / GVA (e.g. Northern Ireland, Wales) could lose existing talent to other regions as a result of this process – for example, a Threat Analyst leaving a £40,000 per annum role in Cardiff to work for a London firm remotely for £60,000.[18]

4.6 Future of the recruitment pool

Despite the challenges outlined, consultees felt that the industry was moving in the right direction and felt the quality and quantity of the pool would improve in the future. Employers felt that a number of interventions such as CyberFirst are working well, and society is better grappling the need for new forms of training and re-training. This presented a huge opportunity when it came to reskilling. There was also a sense that they would be able to broaden the educational backgrounds they hire from, as well as lead to a more diverse pool. Educational interventions and reskilling would mean that the comparative value of a university degree would lessen, and that they would better be able to hire women and manage those on parental leave with increased remote working.

"Reskilling opportunities with many people losing their jobs, what greater time to do this for people who are interested in moving into a career in cyber. Promoting the fact that you don't have to have a technical background. Technical roles are needed but you name it, cyber security has a job for everyone."

Employer, large multi-national firm

4.7 Role of government

Consultees caveated their optimism for the future and felt it only be maintained through sustained government help. They had several ideas to help increase quantity, and improve the quality and diversity of the pool.

4.7.1 Education and training

There was a strong desire to continue to invest in skills, education and training. There was positivity about the impact of previous investments and interventions to try and improve access to cyber security with one employer saying the following:

"What I like about CyberFirst is that they have training material that is targeted for each age group, it is very well thought out, a lot of research has gone into it, it is very professional. It is very popular here. This year we have seen a 25 percent increase in the number of students applying to do these courses virtually. It has also helped increase the number of girls which is really positive."

[18] GVA stands for Gross Value Added. According to the ONS, this is defined as "the value generated by any unit engaged in the production of goods and services" - https://www.ons.gov.uk/economy/grossvalueaddedgva.

Employer, large multi-national firm

Employers felt this could be built upon further through communication in school. Consultees felt that education on cyber security should start at primary level. It was also perceived that not enough schools picked up programmes such as CyberFirst and that the curriculum did not sufficiently educate pupils on GCSEs. One noted the NCSC summer school as a good scheme for schools to replicate. They also felt the government could do more in secondary schools to make students aware of cyber careers. This would allow more students to gain relevant qualifications and experience at an early career stage, especially if they were not inclined to go to university.

"The government could do a lot more in terms of explaining career options. We should also act at school level telling students that it's not necessary to go through a STEM subject to join cyber."
Employer, large multi-national firm

Employees entering the pool and employers felt it was important to diversify routes into the market and make it less degree dependent. They felt the government could do this via two main routes in Further Education. Firstly, they could fund and help colleges create or improve cyber specific NVQ Level 4 courses. Secondly, employers felt the government could help get more further education students into apprenticeships, whereby they would be certified and given a permanent role at the end of the course.

“There is clearly some real talent out there. To fall foul of the Computer Misuse Act properly and get prosecuted, you’ve got to be doing something quite technically sophisticated. There are a lot of people out there crying out for those kinds of skills. This talent is going to waste because we haven’t provided a pathway for people who do think differently.”
Employee

Employers and training providers both felt that the government could help raise awareness to help alleviate negative perceptions of cyber security. They felt currently talented candidates were discouraged from a career in the sector because of a lack of clarity of what a cyber career truly entailed. It was suggested that government could communicate to the public that cyber security roles entail a variety of different skills. One consultee felt breaking this down into three specific areas could encourage a greater quantity into the pool with a relevant set of skills.

"There are the people who like to solve the puzzle, they are interested in the clever attack and how to circumvent the clever attack… Then you have those who see the social responsibility to protect the integrity of data… The third group are the people who are in IT who have found their way into almost by accident and it became a branch in their career.”
Employer, large multi-national firm

Training providers felt that the government could provide more funding to help them satisfy excess demand from free and low-cost training courses. There are high levels of over-subscription and the coronavirus pandemic exacerbated this. Course access was particularly important to ensure candidates from regions with a low cyber security presence, or those from deprived backgrounds.

“I had over 400 people apply and was only able to help 45 people. What’s happened to the other 400 people? What can we do for those individuals?”
Training Provider

Employers and recruitment agents echoed this, and felt it was important for the government to set aside funding for reskilling and retraining initiatives. This was seen as critical should unemployment rise in the next twelve months.

"Government have to support reskilling. If we're staring down the barrel of job losses and people being unemployed, they should be doing that. Retraining people to become digitally capable and digitally competent is the way forward."
Employer, small UK based cyber firm

Individuals from a military background felt that the government could help reskill those leaving the military to work in cyber. Suggestions ranged from help in CV writing to encouraging and funding individuals to sign up to relevant training programmes.

4.7.2 Co-operation between stakeholders

Consultees felt that greater co-operation between different stakeholders and government would help encourage more candidates into the pool and improve diversity.

Firstly, employees and training providers felt that government could improve relations with employers in order to increase the range of candidates in the pool. An employee from an ethnic minority background felt that ethnic minority communities needed more support in finding roles in the industry. They felt that government could help support employers on how to manage blind recruitment or quotas on minority candidates. Recruitment agents and employers noted that government could lead the way in improving diversity. A recruitment agent stated they could do this by setting an example, stating that GCHQ had been successful:

"GCHQ have a fantastic neurodiversity quota. If more employers demanded quotas, if they were serious about it, then the CVs would rise up. They need to commit to this on a company wide basis."
Recruitment agent

A training provider felt that government could set diversity criteria in contracts to ensure their suppliers were hiring from a diverse range of candidates:

"Just the very fact that government talks about diversity keeps it at the forefront of company's minds. We get lots of large organisations that have big contracts with government that go further to trying to be more diverse than others. Just influencing their supply chain makes a big difference."
Training Provider

Neurodiversity specialists felt the government had a role to play with employers in supporting them to hire neurodivergent employees. There was a suggestion for government to help enable relationships between employers and autism charities. This would allow charities to contact neurodivergent employees and discuss any issues that they would not be able to discuss with their employer. The charities can also discuss issues with employers they may otherwise ignore, such as lights in the office being too bright, or that their interview techniques need adapting to make neurodivergent candidates feel comfortable. In turn this would ease challenges employers face regarding recruitment and working environment and enable more neurodivergent candidates finding employment.

"It has to be made easier for industry and having organisations that support neurodiverse people for free is the key. Just telling them 'oh employ neurodiverse people and support them' is never going to work. We have to provide the support structures."
Training Provider

One consultee also noted that different government departments could improve co-operation when delivering initiatives to drive employment in cyber security. They cited a neurodiversity course as an example, whereby multiple government departments and the Police all had an interest in developing a course and had agreed roles in doing so. However, they could not come to an agreement on who should fund it, meaning no department took ultimate responsibility for the course.

Local government can help with or sponsor initiatives to encourage more people into the cyber recruitment pool within their authorities. An example where this could benefit would be the Women in Cyber initiative in Bristol. Its purpose is to attract women into cyber roles from any background (with candidates coming from a variety of backgrounds, such as arts or STEM). Candidates were given technical and non-technical training in cyber security. One employer stated they helped close the gender gap in their business by hiring 10-12 women from this. Government involvement in this would help expand networks nationwide, and create a series of female role models.

Consultees also felt it was important for the government to communicate success stories and share best practice where stakeholders were able to improve quantity, quality and diversity within the recruitment pool.

5 Recommendations

This section provides the key recommendations from the research into the cyber security recruitment pool. These are based on the quantitative and qualitative research undertaken.

These recommendations should be read in conjunction with the recently published Cyber Skills in the UK Labour Market 2021 report, which explores a number of similar and important themes in the cyber security workforce. However, the recommendations below focus on improving supply and wider aligned themes:

Theme 1: Boosting the supply of new talent, and recognising the role of cyber security roles in driving economic recovery

- **Recommendation 1:** This research highlights that the traditional cyber recruitment pool (e.g. graduates and experienced staff) is much smaller than some employers might recognise. In order to address the shortage of cyber security talent, we recommend that alternative and innovative routes to a cyber security career need to be clear, funded and accelerated. These should also be targeted to a diverse range of individuals.

- **Recommendation 2:** The economic impact of the COVID-19 pandemic has demonstrated the critical role of retraining and upskilling. The current economic conditions mean that there is much greater demand for engaging in retraining initiatives, particularly among individuals that have faced redundancy or reduced hours of working in existing roles. There is a window of opportunity for the UK to rapidly invest in cyber security retraining initiatives, courses, and learning models to increase future productivity.

- **Recommendation 3**: Leading by example. Throughout this research, we note several examples of good practice in increasing the supply of new talent into the cyber security industry. We recommend further activity should be undertaken to better promote the understanding and take-up of such initiatives. This could include greater public sector uptake of such schemes (including retraining) where possible, and the sustained promotion of 'what works' across industry.

Theme 2: Supporting pathways into cyber security employment

- **Recommendation 4:** Time to scale up. As noted, there are several pilot and early-stage initiatives that appear to have gained traction in improving diversity and access to cyber security training and entry-level employment. There is now a strong mix of examples across further and higher education, private training initiatives, bootcamps, employer-led training models, and academies targeted at retraining particular groups such as neurodiverse and former Armed Forces. We recommend that further support to help successful pilot initiatives scale-up faster (and to do so across the UK) would be particularly welcome given the identification of the current cyber security skills gaps.

- **Recommendation 5:** We further recommend that in addition to supporting supply-based initiatives, government and training providers should work closely with industry at a regional level to help match skills with local demand. For example, these models should ideally have a clear outcome whereby those supported can enter a role with a local employer in need of such skills. We note that this should also be considered as an important component of the Levelling Up Agenda, as the type of demand for cyber security professionals can vary across the UK, and there is significant potential to increase regional productivity given the longer term salary premium associated with cyber security roles.

- **Recommendation 6:** The nature of cyber security roles has expanded in recent years. We recommend that addressing the cyber security recruitment gap will also require providing and supporting other digital skills pathways, and supporting individuals move into highly complementary roles such as Governance, Risk and Compliance roles. In this respect, improved segmentation, and definition of what skills (including less technical') and type of 'cyber security career' an individual could have may help to ease some of the shortage, and better improve allocation of resources.

Theme 3: Undertaking workforce planning to meet the needs of the cyber security industry today, and into the future

- **Recommendation 7:** We recommend that government further explores a Capacity Review of Higher Education Institutions (HEIs) in the UK with respect to cyber security provision. Whilst this study has explored the number of students graduating within 'Cyber Security' and Computer Science courses, a capacity review of undergraduate and postgraduate cyber provision may be useful to understand if and how HEIs may be able to increase supply (if at all, and without impacting quality) of cyber security teaching, and to further understand the prevalence of cyber security modules across all degree pathways.

- **Recommendation 8:** Building on this theme, we would also recommend that a 'workforce planning' approach should be explored at regional and national levels, particularly by Local Enterprise Partnerships (LEPs) and devolved equivalents. This research has estimated a UK based shortfall in the number of new entrants to the recruitment pool. However, this availability of supply will vary regionally, as will employer demand. Improving alignment between regional skills supply and employer demand, and understanding regional growth ambitions should help regions to make informed decisions and investments to support retraining.

  This research has suggested that across the UK, interventions to the scale of generating an additional c. 300 people (in cyber security) per 1m of working age population (in addition to existing supply) would help to address this annual shortfall. We recommend that each region, particularly those with high density of cyber security employment explore this in further depth.

Theme 4: A strong focus on improving diversity in supply

The Cyber Skills in the UK Labour Market (2021) explores themes of diversity within the cyber security labour market. However, the following recommendations are included below:

- **Recommendation 9:** Retraining initiatives to support individuals get into cyber security can be life changing. They can allow people to learn new skills, meet new people, and increase their earning power. However, we recommend that such initiatives should place a sustained emphasis where possible, on improving accessibility to all extents. Whilst many individuals may want to retrain, the barriers to undertaking such initiatives such be continually explored. For example, this might include provision of financial support (e.g. direct, or support with child-care) to enable the take-up of the training place.

- **Recommendation 10:** As set out in the research, whilst there have been a number of initiatives aimed at improving diversity within the industry, there are still significant issues reflected in the inflows of new talent (e.g. female take-up of cyber security courses remains low). We recommend that these figures are closely monitored in future years, alongside the continued promotion of schemes such as CyberFirst.

Our standards and accreditations

Ipsos MORI's 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 market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos MORI was the first company in the world to gain this accreditation.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation. We were the first company to sign up to the requirements and self-regulation of the MRS Code. More than 350 companies have followed our lead.

ISO 9001

This is the 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

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

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

Ipsos MORI is required to comply with the UK GDPR and the UK DPA. It covers the processing of personal data and the protection of privacy.

HMG Cyber Essentials

This is a government-backed scheme and a key deliverable of the UK's National Cyber Security Programme. Ipsos MORI was assessment-validated for Cyber Essentials certification in 2016. 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.

Fair Data

Ipsos MORI is signed up as a "Fair Data" company, agreeing to adhere to 10 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-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI Public Affairs

Ipsos MORI 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.