OECD Skills Studies

Building a Skilled Cyber Security Workforce in Five Countries

INSIGHTS FROM AUSTRALIA, CANADA, NEW ZEALAND, UNITED KINGDOM, AND UNITED STATES

OECD

OECD Skills Studies

Building a Skilled Cyber Security Workforce in Five Countries

INSIGHTS FROM AUSTRALIA, CANADA, NEW ZEALAND, UNITED KINGDOM, AND UNITED STATES

OECD
BETTER POLICIES FOR BETTER LIVES

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Member countries of the OECD.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Please cite this publication as:
OECD (2023), *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/5fd44e6c-en.

ISBN 978-92-64-38124-7 (print)
ISBN 978-92-64-33839-5 (pdf)
ISBN 978-92-64-47591-5 (HTML)
ISBN 978-92-64-85405-5 (epub)

OECD Skills Studies
ISSN 2307-8723 (print)
ISSN 2307-8731 (online)

Photo credits: Cover © vs148/Shutterstock.com.

Corrigenda to publications may be found on line at: www.oecd.org/about/publishing/corrigenda.htm.

Foreword

Cyber security breaches continue to significantly threaten governments, businesses and individuals worldwide. The demand for cyber security professionals has increased significantly in recent years around the world and is expected to continue to grow, and this trend has created shortages in labour markets in several countries. The first step in addressing skills shortage in the cyber security sector is to understand the supply and demand dynamics of cyber security skills. This information can be used by governments and organisations to identify their vulnerabilities and determine where additional resources are needed. By analysing job postings, trends in demand for cyber security professionals and the skills for creating a secure organisational environment can be identified. Meanwhile, studying the provision of cyber security education and training programmes provides insights into how the cyber security workforce is being developed and the potential misalignment between demand and supply.

This report analyses the demand for cyber security professionals in five countries (Australia, Canada, New Zealand, the United Kingdom and the United States), and zooms in on the provision of cyber security education and training programs in England (United Kingdom). The report aims to provide a comparative analysis of cyber security demand in the five countries, with a detailed analysis of the education and training programmes and policies put in place in England to make the profession more attractive and diverse. The report is the first in a series of studies that aim to expand knowledge on the cyber security workforce and related education and training provision in various regions and countries.

This work has been carried out by the OECD Directorate for Employment, Labour and Social Affairs and the OECD Centre for Skills. The report was prepared by Diego Eslava (Chapters 1 and 2) and Iván Bornacelly (Chapters 1 and 3), under the supervision of Fabio Manca and Marieke Vandeweyer. Editorial assistance was provided by Natalie Corry. Valuable comments were given by Mark Pearson (OECD Deputy Director for Employment, Labour and Social Affairs) and El Iza Mohamedou (Head of the OECD Centre for Skills), as well as by Francesca Borgonovi (OECD Centre for Skills) and colleagues from the OECD Directorate for Science, Technology and Innovation.

The OECD is grateful to stakeholders in England for their invaluable input and feedback throughout the project, in particular the Department for Digital, Culture, Media and Sport and the Department for Education. Our warm thanks go to the many education and training institutions, businesses, research institutions, and other organisations who generously shared their knowledge and insights during bilateral discussions. The support from Microsoft Philanthropies is highly appreciated.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the OECD member countries or Microsoft.

Table of contents

FIGURES

TABLES

Abbreviations and acronyms

The following are the main abbreviations and acronyms cited in the report. Other abbreviations and acronyms cited occasionally are defined where used.

A-Level	Advanced Level
Beng	Bachelor of Engineering
BSc	Bachelor of Science
CAD	Computer-Aided Design
CAM	Computer-Aided Manufacturing
CO	Cabinet Office
CSIIF	Cyber Skill Immediate Impact Fund
CyBOK	The Cyber Security Body of Knowledge
DCMS	Department for Culture, Media and Sports
DfE	Department for Education
DSTI	Department for Science, Innovation and Technology
EPA	End-point Assessment Plan
FE	Further Education
FSM	Free School Meals
GCSE	General Certificate of Secondary Education
HE	Higher Education
HEIs	Higher Education Institutions
HTQs	Higher Technical Qualifications
ICT	Information and Communication Technology
IfATE	Institute for Apprenticeships and Technical Education
IoTs	Institutes of Technology
ISA	Income Share Agreement
ISCED	International Standard Classification of Education
IT	Information Technology
KSBs	Knowledge, Skills and Behaviours
L	Level
MAP	Mayor's Academies Programme
NCFE	Northern Council for Further Education
NCSC	National Cyber Security Centre
NLP	Natural Language Processing
OFS	Office for Students
OJPs	Online Job Postings
SDL	Sector Delivery Lead
SMEs	Small and mid-size enterprises
SOC	Cyber Security Operations Centre
SSBM	Semantic Skill Bundle Matrix
STEM	Science, Technology, Engineering and Math
UCAS	University and College Admission Service
UKC3	UK Cyber Cluster Collaboration
UKRI	UK Research and Innovation
VET	Vocational Education and Training
WIN	Workforce Integration Network

Executive summary

New technologies, such as Cloud Computing, Artificial Intelligence (AI) or the Internet of Things (IoT), offer great opportunities for societies to enjoy the benefits of an increasingly interconnected world. However, the use of digital technologies also implies greater exposure to the risks of cyber attacks. The number of cyber attacks is outstripping defence capabilities, and one reason for this is the lack of an adequately skilled cyber security workforce. Enterprises around the world are facing shortages of skilled professionals in this area, limiting their ability to contain threats.

This report analyses the evolution of the demand for cyber security professionals from January 2012 to June 2022 in five countries: Australia, Canada, New Zealand, the United Kingdom and the United States. The analysis in the report leverages the information contained in nearly 400 million job postings collected from the internet (online job postings, OJPs). The report also looks at the supply side, zooming in on the landscape of cyber security education and training programmes in England (United Kingdom) and the policies and initiatives to make these programmes more accessible and relevant.

Along with the fast-paced digital transformation observed in many OECD countries, the demand for cyber security professionals outpaced the growth in aggregate demand across the rest of the occupations in all countries analysed in this report. Notably, since 2021, the volume of OJPs in cyber security increased at a faster pace than in the pre-pandemic period, likely reflecting the challenges related to the expansion of remote working and a broader adoption of digital technologies.

The demand for cyber security professionals is heterogeneous. Cyber security architects and engineers stand at the core of the demand for cyber security professionals, recording the highest share of OJPs and the fastest growth in the period 2012 to 2022. Cyber security analysts also represent a large share of OJPs in the cyber security landscape, with particularly strong growth in Australia and New Zealand.

Most of the OJPs in the cyber security job market are for jobs located in main urban areas where major enterprise and government headquarters are found. However, the geographical concentration of cyber security OJPs in those areas has recently decreased, suggesting that, as the digital transformation permeates an increasingly larger number of economic activities throughout different geographies, the demand for cyber security professionals is also spreading out geographically.

The rapid adoption of new digital technologies is reshaping the skills that enterprises are demanding for their cyber security professionals. Data for 2021 indicates that the knowledge of cyber security-related frameworks (i.e. resources for the design and implementation of security systems) and “threat assessment” skills are highly relevant for the profession. Over time, new technologies are emerging, and these are increasingly mentioned as requirements in OJPs seeking to hire cyber security professionals. For example, the importance of knowledge in cloud computing has significantly increased in the last couple of years.

On the supply side, the case study for England shows that there can be various education and training pathways into cyber security roles, with opportunities for progression. The English further and higher education system provides multiple cyber security training programmes that lead to formal qualifications, including at the short-cycle tertiary level (or higher technical education) and bachelor’s level. Learners can also develop basic cyber security skills at lower levels of education, including through cyber security modules integrated in broader programmes and through dedicated cyber security programmes in further education. In addition to these classroom-based programmes, there are also apprenticeship opportunities in cyber security at various education levels – allowing learners to develop skills on the job.

Complementing these formal cyber security qualifications, young people and adults in England can also participate in non-formal training that typically leads to certificates. Such non-formal training is usually shorter and more flexible than programmes in the formal system. Bootcamps are one particular type of non-formal training that is available in the cyber security field, which can be offered by public or private education and training providers. The Department for Education offers Skills Bootcamps which can be fully funded by the government. These are flexible courses of up to 16 weeks to build up sector-specific skills and fast-track to a job interview with a local employer. While Skills Bootcamps are typically too short to prepare someone without a background in information technology to become a fully skilled cyber security professional, they provide opportunities for those with some relevant experience to specialise in cyber security and for those without experience to take their first steps in a longer cyber security training pathway.

Enrolment in cyber security education and training is relatively modest but on the rise for various types of programmes. Efforts have been made to improve the understanding of what a cyber security career looks like and the pathways to it. Moreover, programmes such as CyberFirst have been introducing young learners to the field to develop the next generation of cyber security professionals. As female learners are typically underrepresented in this field, various initiatives focus on bringing more girls and women into cyber security training and careers. More flexible training opportunities are being created (such as the Skills Bootcamps), and financial incentives are provided to make training more accessible.

Outcomes of cyber security programmes are positive overall, with on average, relatively high completion rates and progression into employment or further studies. As the cyber security field changes quickly, education and training programmes in this field need to adapt to stay relevant. Apprenticeships and skills bootcamps are designed in close collaboration with employers, and sectoral clusters facilitate co-ordination between employers and education and training providers. Various initiatives have been set up to certify cyber security programmes and providers to signal their quality to learners and employers, facilitating students’ choice of programmes and ensuring cyber security training content and delivery is consistent with best practices.

1 Key insights for building a skilled cyber security workforce

This chapter provides an overview of the report's objectives and rationale and summarises the main takeaways. It discusses the results from the analyses of the demand for cyber security professionals in Australia, Canada, New Zealand, the United Kingdom and the United States. It also summarises the main findings from the analysis of the landscape of cyber security education and training programmes in England (the United Kingdom). It concludes with actionable policy pointers.

Highlights

- As economies shift to digital and online models, cyber threats can quickly outpace traditional approaches to data security and threaten governments, businesses, and individuals worldwide. In response to this trend, the demand for cyber security professionals in Australia, Canada, New Zealand, the United Kingdom and the United States has shown a very robust growth. For instance, job postings seeking cyber security professionals in 2022 were five times larger than in 2012, with a particular acceleration in the demand since the COVID-19 pandemic.
- Within the cyber security profession, workers are employed in variety of roles. Cyber security architects and engineers stands at the core of the demand for cyber security professionals accounting for more than one-third of the online job postings seeking for professionals in this occupation.
- The rapid adoption of new digital technologies is reshaping the skills enterprises demand from cyber security professionals. For instance, In the United States, the number of job postings mentioning virtualisation applications (software-based cyber security solutions) as a skill requirement have increase by 50 times since 2018. Similarly, the number of job postings mentioning skill requirements related to cloud computing platforms in the United Kingdom increased by 20 times relative to 2018.
- Job postings for cyber security professionals typically demand three years or more of experience, leaving limited room for younger candidates to enter the profession. Policy intervention is needed to design comprehensive cyber security workforce development policies. Collaboration between the private sector, education and training providers, governments and social actors can help smooth the transition from school to work and expand the options for youth to access jobs in cyber security.
- Developing education and training programmes that are well aligned with the needs of the cyber security industry is crucial. This requires engaging employers in the design and delivery of programmes and, in the case of England, further strengthening cyber apprenticeships and Skills Bootcamps.
- Education and training options in the cyber security field and their associated career pathways need to be transparent and accessible. Solid careers information and guidance is needed to help individuals make informed choices and tackle stereotypes and misconceptions – which can contribute to making the cyber security workforce more diverse, including in terms of gender.

The relevance of cyber security skills in a more digitalised and interconnected world

Cyber security breaches continue to significantly threaten governments, businesses and individuals worldwide. As economies shift to digital and online models, threats can quickly outpace traditional approaches to data security. From supply chain disruptions to ransomware attacks, cybercriminals have become increasingly sophisticated and the threat landscape more diverse. The estimated economic cost of information and technology asset security breaches in 2020 was a staggering USD 4-6 trillion, equivalent to about 4-6% of the global GDP (UNCDF, 2022[1]). The United Kingdom and the United States have experienced the most significant cyber attacks[1] over the last two decades (Specops, 2021[2]).

A workforce shortage compounds these cyber security challenges. While the cyber security workforce has reached an all-time high, with an estimated 4.7 million professionals, a global shortage of 3.4 million workers is found in this field (ISC2, 2022[3]). The cyber security workforce is growing rapidly but still needs to catch up with the growing demand for workers in this sector. In the United States alone, there were more than 700 000 unfilled cyber security jobs in 2021 (Cybersecurity Ventures, 2021[4]). In fact, the labour shortage in the sector keeps growing: the global cyber security workforce gap has grown more than twice as strong as the workforce. The United Kingdom and Australia, together with France and Spain, are among the countries with the most substantial increase in the cyber security workforce gap between 2019 and 2021[2] (ISC2, 2022[3]).

The cyber security workforce faces a lack of diversity. Women represent only 24% of the global cyber security workforce (ISC2, 2022[3]). In the United Kingdom, women represent 36% of the cyber security workforce, and they are more likely than men to hold non-technical roles, such as compliance and risk assessment (NCSC & KPMG, 2021[5]). This gender gap not only highlights the need for greater equity in the industry but also presents a business imperative. By recruiting and retaining more women in the field, organisations can tap into a larger pool of potential talent and help to fill the shortage of skilled professionals in the industry.

Developing strategies and policies to prepare the workforce with the right cyber security skills is imperative, especially in the context of high cyber security workforce shortages. Cyber security professionals are crucial in safeguarding government and organisations' operations, sensitive information and digital resources. Cyber security professionals with the right set of skills improve organisations' capability to respond to threats affecting companies' productivity, adaptability to hostile environments, and further technological and digital adoption (Andrews, Nicoletti and Timiliotis, 2018[6]). Organisations seek cyber security talents to make the workplace more productive, efficient, and effective.

Strengthening the cyber security workforce requires co-ordinated action by international institutions, governments, enterprises, civil society, and individuals to train the workforce with the fast-evolving skills needed. Joint efforts from the private and public sectors have been taken, for example, through the development of cyber security skills strategies and skills frameworks. For instance, the United Kingdom and the United States Governments have established national cyber security strategies to align all the relevant stakeholders, increase the safety and resiliency of countries and overcome cyber security challenges, including the cyber security skill gaps (Box 1.1). Similarly, governments have established national cyber security centres to facilitate collaborations and information-sharing on cyber security and improve cyber security capabilities. For instance, the Australian Cyber Security Centre (ASCS) leads the government's efforts in strengthening national cyber security, including providing information and support to households and companies on becoming more resilient to cyber attacks and preparing the labour force with cyber security skills.

Box 1.1. Cyber security national strategies and cyber security skills frameworks

The speed of digital innovation and proliferation of cyber threats impact nations' safety, prosperity and resilience, pushing governments to develop national cyber security strategies (NCSs) to overcome these fast-evolving cyber security challenges. Several multinational organisations have also affirmed the importance of adopting comprehensive NCSs. In the last three years, there has been a 50% increase in countries adopting NCSs. But despite the recent progress, 60% of least developed countries still need strategies and most developing countries that have adopted a strategy struggle to implement it due to a lack of financial and human resources (Neto, Obiso and Baayen, 2022[7]).

National authorities have highlighted the lack of cyber security professionals as a relevant issue and have recognised the need for action. For instance, the **UK Government** established the National Cyber Security Skill Strategy in 2018 to develop the right cyber security capability by increasing the number of cyber security professionals and providing the skills needed across the general workforce to become the most secure digital economy (DCMS, 2018[8]). Similarly, through executive orders, the **US Government**, has recognised the need to strengthen the cyber security workforce and has developed strategies to overcome the cyber security skill shortage. Some strategies aimed at enhancing workforce mobility, developing cyber security skills and creating organisational and technological tools to maximise the existent cyber security talent (The White House, 2019[9]). The National Initiative for Cyber security Education (NICE) framework, for instance, is a fundamental resource for developing the cyber security workforce by describing tasks, knowledge and skills necessary to perform cyber security-related tasks (NIST, 2022[10]). In 2018, **Canada** developed its "Vision for security prosperity in the digital age", which includes a plan for improving cyber security knowledge and skills to prevent and overcome cyber threats (Public Safety, 2018[11]).

This report: Understanding the demand for and the supply of cyber security skills in a set of countries

What this report is about

Understanding what is happening on the supply and demand side of cyber security skills is a crucial first step to tackling skill shortages in the cyber security sector. This information can help organisations and governments identify the areas where they are most vulnerable and need additional resources. The information in job postings allows to uncover trends in demand for cyber security professionals and identify the skills currently essential for creating a cyber-safe organisational environment. At the same time, studying the provision of cyber security education and training programmes provides insights into how the labour force in this field is being developed.

This report is the first of a broader project to expand the knowledge on the cyber security workforce and associated education and training provision across multiple regions and countries (see Box 1.2). Each report is divided into two parts, one focusing on the demand for cyber security professionals and one looking at the landscape of cyber security education and training programmes:

- The demand-side analysis uses big data to study job postings for cyber security professionals, looking at the volume and content of the postings to uncover trends and detailed characteristics of employer demand. This first report analyses the demand for cyber security professionals in five countries: Australia, Canada, New Zealand, the United Kingdom and the United States.
- The supply-side analysis zooms in on cyber security education and training programmes and the policies and strategies implemented to expand and diversify the cyber security workforce. Each report focuses on one case study country for this supply-side analysis. For this report, England (the United Kingdom) is the country selected.

As such, the objective of this first report is to provide a comparative analysis of the demand in the five selected countries, looking at the evolution and characteristics of the cyber security profession, and through the English study case, look in-depth into what types of education and training programmes can prepare workers for cyber security roles and the policies that can contribute to making the profession more attractive and diverse.

Box 1.2. The "Building a skilled cyber security workforce" project

The rationale of the project

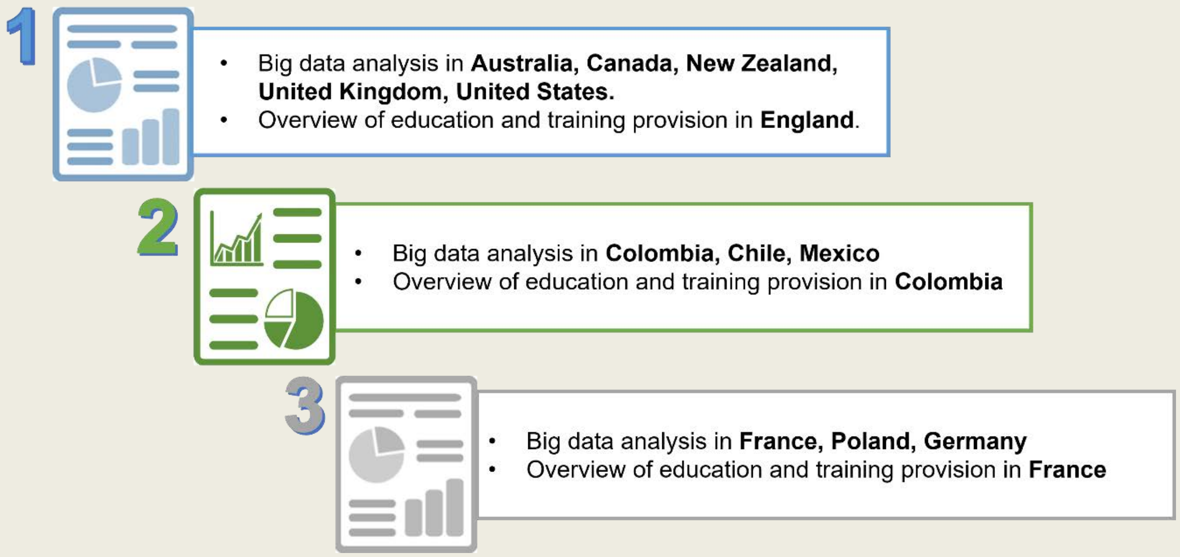
The demand for cyber security professionals has increased significantly in recent years and is expected to grow, and this trend has created shortages in labour markets in several countries. Given the high costs associated with cyber threats, policy makers and firms need detailed and timely information on the demand and supply of cyber security-related skills and learn from best practices from around the world.

This project leverages OECD-wide expertise to analyse the cyber security roles that are in demand in labour markets around the world and identify the set of skills that are currently considered to be key for creating a cyber-safe organisational environment. It also assesses how education and training systems in different countries are developing such skills. Lastly, the project also fosters an informal forum for discussion and dialogue on best practices and forecasted cyber security skill needs.

The structure of the project

The project is divided into three parts that combine big data and policy analysis to assess the demand for and supply of cyber security skills and the policies and strategies implemented to expand and diversify the cyber security workforce and overcome cyber security skill shortages. Each of the three parts is focused on different geographical areas (see Figure 1.1), covering three to five countries for the demand-side analysis and one case study country for the supply-side analysis. The analyses from the three parts will be summarised in three dedicated OECD reports (of which this one is the first).

Figure 1.1. Outputs of cyber security project



1
- Big data analysis in **Australia, Canada, New Zealand, United Kingdom, United States.**
- Overview of education and training provision in **England**.

2
- Big data analysis in **Colombia, Chile, Mexico**
- Overview of education and training provision in **Colombia**

3
- Big data analysis in **France, Poland, Germany**
- Overview of education and training provision in **France**

Methodology

Using big data to understand cyber security skills demand in five countries

To analyse the demand for cyber security professionals in a timely and detailed manner, this report uses data extracted from nearly 400 million online job postings collected from the five selected countries (Australia, Canada, New Zealand, the United Kingdom and the United States). Increasingly so, research on labour market dynamics relies on real-time big data to better capture recent trends and gain insights at a more granular level than is possible with more traditional data.

In particular, this report uses this high quantity of data points to analyse the main trends in demand for cyber security professionals from January 2012 to June 2022. Moreover, it leverages the texts contained in job postings to characterise the professional profile typically requested by enterprises, including a particular focus on the skills, competencies and abilities most relevant for the cyber security profession in each country.

A case study to zoom in on strategies for cyber security education and training provision

The types of cyber security education and training programmes available and their design differ strongly between countries, as do the policies and initiatives to make these programmes accessible and attractive. To provide insights into how education and training for cyber security roles can be developed, delivered and promoted, this report focuses on one particular country – England (the United Kingdom). The purpose of presenting a dedicated case study is to provide a detailed description of programmes, policies and initiatives that could serve as inspiration for other countries developing their cyber security education and training sector. The English case looks at the landscape of cyber security programmes, focusing on professionally-oriented formal education programmes at the undergraduate level or below and non-formal programmes (e.g. bootcamps). The case study also looks into the policies and strategies aimed at expanding the cyber security workforce in England, especially those that facilitate access to cyber security education and training programmes for newcomers in the field. The case study analysis builds on national data and literature, as well as insights gathered from interviews with various key stakeholders in the English education and training and cyber security sectors.

Main findings and policy pointers

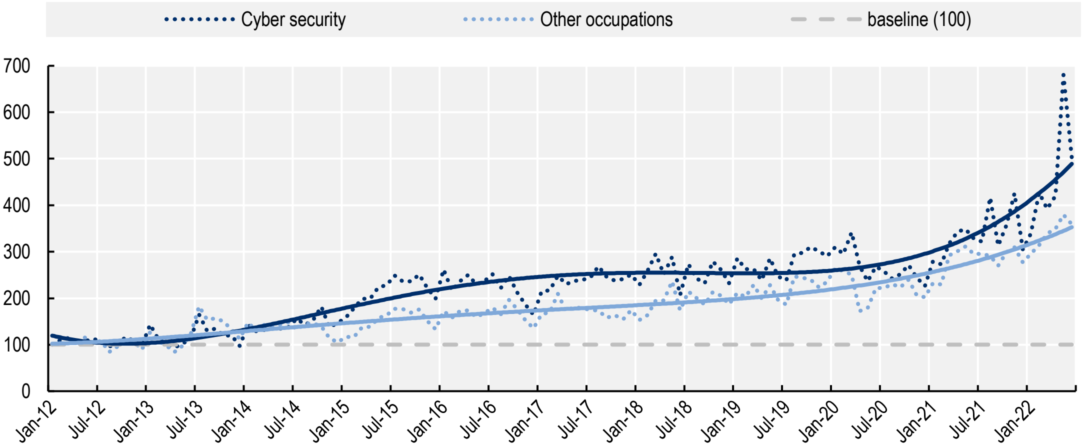
The demand for cyber security professionals is on the rise in the five countries

The demand for cyber security professionals shows a robust and increasing trend in all countries, especially during the period following the COVID-19 pandemic. Overall, the number of online job postings (OJPs) seeking cyber security professionals in the first half of 2022 was nearly five times larger than at the beginning of 2012 and twice as large than at the end of 2019 (Figure 1.2). Consequently, the share of cyber security job adverts over the total amount of online job postings has increased in all five countries. Results also show that smaller markets for cyber security professionals, such as New Zealand, have shown more robust growth than more developed markets, such as the United States, suggesting that the cyber security demand is expanding fast across countries.

The demand for cyber security professionals is heterogeneous. Among different job roles, cyber security architects and engineers (those professionals in charge of designing and modelling security solutions) stand at the core of the demand for cyber security professionals and have recorded the highest share of new online job postings (37%), as well as the fastest growth in demand between 2012 and 2022. Cyber security analysts (who provide insights to support planning, operations and maintenance of systems security) also represent a large share of OJPs in the cyber security landscape (26%), with robust growth in Australia and New Zealand.

Figure 1.2. Average growth in online job postings: Cyber security and all occupations

Evolution in demand in comparison to the month of reference (Jan-2012 = 100, average of the five countries)



Note: The average index for the five countries is weighted by each country's share in the total number of monthly cyber security OJPs. Data for NZL starts in January 2013. A polynomial trend line is included to show smoother results (solid lines).
Source: OECD calculations based on Lightcast data.

Most of the OJPs in the cyber security job market are for jobs in main urban areas where major enterprises and government headquarters are located. In Canada, for instance, 40% of the job postings advertised between January 2012 and June 2022 were for jobs based in Toronto, followed by Ottawa accounting for only 9% of the total demand. In the United Kingdom, London accounted for 38% of job postings searching for cyber security professionals, while postings for cyber experts located in Manchester only accounted for 5% of the total OJPs. However, the geographical concentration of cyber security OJPs in those areas has recently decreased. London's share, for instance, decreased 10 percentage points from 41% in 2012 to 31% in 2021. This trend suggests that, as the digital transformation spreads to diverse economic activities throughout different geographies, the demand for cyber security professionals is also spreading out geographically.

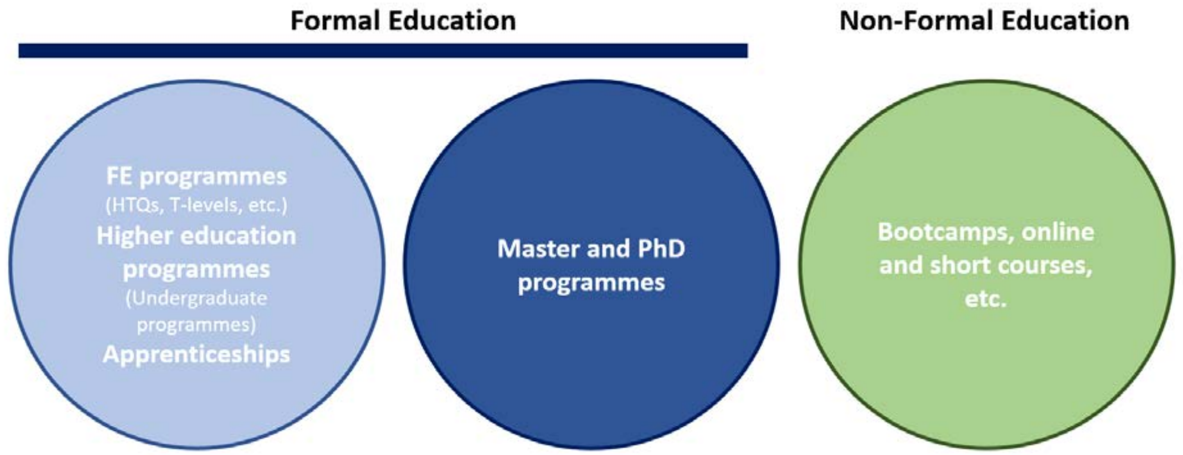
An analysis of enterprises' requirements shows that a typical candidate for a cyber security job needs a bachelor's degree and more than three years of experience. As such, data from OJPs suggest little space for younger and more inexperienced profiles to find cyber security positions. This is likely to contribute to broadening the workforce gap in the sector and policy initiatives are needed to boost the school-to-work transition of youth moving into cyber security roles.

The rapid adoption of new digital technologies is reshaping the skills enterprises demand from cyber security professionals. Data for 2021 indicates that, among others, the knowledge of cyber security-related frameworks (i.e. resources for the design and implementation of security systems) and "threat assessment" skills are highly relevant for the profession. Over time, new technologies are emerging, and they are increasingly mentioned as key requirements in OJPs for cyber security professionals. For example, in the period between 2019 and 2022, the mentions of cloud computing platforms in cyber security job postings have increased 60 times compared to the period in between 2012 and 2018. Similarly, the demand for specialised software for application virtualisation increased 30 times over the same time span. The demand for technologies in the cyber security space is expected to keep changing as new digital resources, and threats, keep emerging.

The provision of cyber security education and training programmes in England is diverse

On the demand side, the case study for England shows that there can be various education and training pathways into cyber security roles, with opportunities for progression (see Figure 1.3). The English further and higher education system provides multiple cyber security training programmes that lead to formal qualifications, including at the short-cycle tertiary level (or higher technical education) and bachelor's level. Enrolment in cyber security programmes in further and higher has been on the rise, but still remains relatively limited. Learners can also develop basic cyber security skills at lower levels of education, including through cyber security modules integrated into broader programmes. These education and training opportunities include classroom-based programmes, as well as apprenticeship opportunities in cyber security at various education levels – allowing learners to develop skills on the job.

Figure 1.3. Cyber security education and training programmes take many forms in England


Formal Education
Non-Formal Education
FE programmes
(HTQs, T-levels, etc.)
Higher education programmes
(Undergraduate programmes)
Apprenticeships
Master and PhD programmes
Bootcamps, online and short courses, etc.

Note: Formal education, which leads to formal qualifications such as bachelor's degrees, includes courses and programmes offered by Further Education (FE) and Higher Education (HE) institutions. For this study, programmes at the Master's level and above are excluded from the analysis. Non-formal education and training include courses outside the formal education system and not leading to formal qualifications (but awarding certificates in some cases), such as bootcamps. HTQs refer to Higher Technical Qualifications.

Complementing these formal cyber security qualifications, young people and adults in England can also participate in non-formal training. Such non-formal training is usually shorter and more flexible than programmes in the formal system. Bootcamps are one type of non-formal training available in the cyber security field that the Department for Education (DfE) and private training providers can offer. Particularly, the DfE offers Skills Bootcamps programmes fully funded by the government. The Skills Bootcamps are flexible courses of up to 16 weeks to build sector-specific skills and fast-track a job interview with a local employer. In 2022, 890 digital Skills Bootcamps have been offered of which 77 were in cyber security, with further expansion planned in the coming years. While bootcamps are typically too short to prepare someone without a background in information technology to become a fully skilled cyber security professional, they provide opportunities for those with some relevant experience to specialise in cyber security and for those without experience to take their first steps in a more extended cyber security training pathway. Multiple online courses are also part of the non-formal supply in the digital field. In cyber security, almost 6 000 courses were offered among the most popular e-learning platforms in the United Kingdom.[3]

Cyber security is a rapidly growing profession in England, but unfortunately, it suffers from a lack of diversity. Only 22% of the cyber security workforce is made up of women, dropping to 13% when looking at senior cyber security roles (DCMS, 2022[12]). According to data from the UK Government, only 18% of students enrolled in computer science courses at universities and colleges are women. The lack of gender diversity in cyber security can be attributed to various factors, such as a lack of female role models, unconscious bias during recruitment, and a general lack of awareness of the opportunities available in the industry. It is crucial to address this issue to ensure that the cyber security profession is more representative of the population it serves, and to benefit from the diverse perspectives and ideas that a more inclusive workforce can bring.

Multiple policies and strategies have been implemented in England to expand and diversify the cyber security workforce in an effort to attract young and adult learners from different backgrounds to the field. Efforts have been focused on providing clear information about cyber security education and training and careers and guidance on how to engage with the distinct learning pathways available to pursue a career in the field. Similarly, financial incentives and subsidies have been provided to increase participation in cyber security education and training, especially targeting the most disadvantaged young people and adults. In particular, multiple initiatives have been put in place to expand women's representation in cyber security and address skill needs by providing learning experiences and information focused on overcoming gender stereotypes. The government has also played an essential role in facilitating the interaction between the education sector and the world of work so that the education and training provision is more aligned with the concrete needs of the cyber security sector both nationally and regionally. Initiatives have been implemented to encourage companies to offer cyber security apprenticeship opportunities and provide support in delivering them. Box 1.3 provides examples of interesting practices in England, which are further documented in Chapter 3.

Policy pointers for building a skilled cyber security workforce

Analysing the demand for cyber security professionals in Australia, Canada, New Zealand, the United Kingdom and the United States and the case study on cyber security education and training in England highlight opportunities to tackle shortages in the sector. These includes:

Providing information and guidance on cyber security careers and training

- The cyber security profession has diverse roles, facing different demand and requiring different skill sets. The demand also differs between geographical areas. Moreover, as cyber threats rapidly evolve, the skills and technologies required to fulfil security needs constantly change. Employers, as well as education and training providers, need to have a good understanding of these different roles and their skill demands to reduce labour market mismatches. As such, solid skills intelligence needs to be produced and disseminated across the various labour market and education actors.
- As numerous cyber security career options are available in various industries, this requires supporting students to navigate them. Effective career guidance enables people to develop informed, critical perspectives about the relationship between education and employment in the sector. This is especially relevant for newcomers in the field who may find it hard to understand the entry requirements and the competencies needed.

Overcoming barriers to expand and increase diversity in the cyber security field

- Raising awareness of cyber security careers should start early to create a pipeline of talent and break possible misconceptions and stereotypes about the sector. Particular efforts are needed to diversify the workforce. Career guidance is crucial, as are programmes targeting underrepresented groups that incorporate particular efforts to tackle barriers commonly faced.
- Making cyber security education and training more attractive and accessible for women can help address their significant underrepresentation in the industry and simultaneously fill the workforce needed. Role models in industry and policy making can contribute to breaking gender stereotypes and broaden perspectives and aspirations of girls and women.

- Cyber security training should be available at various levels, consistent with the multiple existing roles. Formal and non-formal programmes can complement each other. Moreover, clear progression pathways between the programmes should exist.
- The demand for cyber security professionals is no longer concentrated in a few hubs, and increasingly employers outside of these usual hubs are hiring cyber security professionals. Young people and adults should have easy access to cyber security education and training – irrespective of where they live. Online training programmes are valuable in this regard.
- Developing cyber security technical skills demands strong foundations in digital skills. This requires that young people and adults, especially the most disadvantaged, should have opportunities to develop essential digital skills before engaging in any cyber security-specific training.
- Skill requirements in cyber security evolve rapidly, and formal education may struggle to provide individuals with the sector-specific skills required in a changing labour market. Skill-based recruitment (which promotes hiring workers based on skills instead of degree requirements) can reduce entry barriers for younger and less experienced individuals while closing the workforce gap in the sector.

Boosting employer participation in the design and delivery of cyber security programmes

- Employer engagement in the design of cyber security programmes is crucial to ensure that they reflect the needs of the labour market. In order to expand provision and respond to cyber security skills needs beyond the technology sector, stronger links between the education sector and firms in non-technological industries such as financial services and advanced manufacturing should be developed – including with small and medium-sized enterprises.
- Apprenticeship can be a valuable training form in this sector, especially when apprenticeship standards are co-designed with employers and the quality of work-based learning is guaranteed. Apprenticeships can be delivered at various levels, aligned with the diversity in cyber security roles.
- Short non-formal programmes that are designed with employers have the ability to respond quickly to changing skill needs in the cyber security sector. However, such short programmes might not be sufficient to develop the required knowledge and skills for specific roles. As such, to improve the relevancy of education, these programmes should be better linked to the cyber security roles they target and should exist at various levels to provide clear career pathways.
- Bringing employers from different sectors and other relevant stakeholders together is key for developing cyber security skills strategies, as it helps to identify common challenges and opportunities and strengthen collaboration between the private sector, education and training providers, governments and social actors. Cyber security skills strategies can set a roadmap to design comprehensive cyber security workforce development policies beyond policies targeting only the education and training system.

Investing in the quality of cyber security education and training programmes

- Information on teacher shortages by sector is typically not readily available. To enhance cyber security training provision, comprehensive data on teachers should be collected regularly and systematically to understand teachers' shortages in the field.
- Ensuring a high quality of cyber security education and training is imperative to generate a skilled workforce and improve organisations' cyber security capabilities. Certification mechanisms for education and training programmes or providers can help students and employers recognise quality approved institutions/programmes and strong graduates in the cyber security field.

Box 1.3 highlights interesting practices put in place in England aimed at expanding and diversifying the cyber security workforce.

Box 1.3. Interesting practices from England

Several interesting initiatives and strategies have been implemented in England to expand the cyber security workforce through strengthening the provision of cyber security education and training programmes and providing information and incentives to engage with education and training in the field. Some of these practices are listed below:

- **Apprenticeships in the cyber security field** (Find Apprenticeships, 2022[13]) combine practical training on the job with off-the-job training, allowing apprentices to gain job-specific skills while working alongside experienced staff from the sector in addition to the more theoretical aspects of cyber security. They are available at different levels of qualification. Enrolment in cyber security apprenticeships increased strongly in the last five years.
- **CyberFirst** (NCSC, 2022[14]) is a programme led by the National Cyber Security Centre (NCSC) which aims to develop the United Kingdom's next generation of cyber security professionals through bursaries, free courses for 11-17 year-olds and competitions. The programme provides opportunities for young people to explore their passion for tech applied to the fast-paced cyber security sector.
- **CyberFirst Girls** (NCSC, 2022[14]) is a complementary programme to CyberFirst focused on demystifying the idea that only boys can succeed in IT, especially in the cyber security sector. The programme includes a CyberFirst Girls competition which aims to support girls interested in a career in cyber security. Additionally, NCSC offers the CyberFirst girls' development day, where girls can have interactive learning experiences and witness inspirational speeches from women leaders in the cyber industry. This event helps girls to have a better understanding of the learning and aspirational possibilities.
- **Department for Education Skills Bootcamps** (Department for Education, 2022[15]) are free, flexible courses of up to 16 weeks at various levels, available in England, allowing people to build up sector-specific skills and fast-track to a job interview with a local employer once the training is completed. The courses are open to adults aged 19+.
- **Cyber security career route map** (UK Cyber Security Council, 2022[16]) is a website developed by the UK Cyber Security Council that provides detailed information about the different areas of specialisation in cyber security. It also suggests learning pathways for individuals interested in a specific field. The information shown for each area of specialisation includes characteristics of the role, skills and knowledge required and helpful information to enter the specialisation.
- **NCSC certification** (NCSC, 2023[17]) is a certification of cyber security apprenticeships, bachelor's, master's and integrated master's degrees with well-defined and relevant content delivered to an appropriate standard. Working in partnership with the DCMS, Cabinet Office, and UK Research and Innovation, the NCSC certifies programmes across higher education institutions that better respond to cyber security standards established by CyBOK and the national cyber security priorities. This certification should help students differentiate between the many cyber security degrees on offer and employers distinguish between applicants' qualifications.

References

Andrews, D., G. Nicoletti and C. Timiliotis (2018), “Digital technology diffusion: A matter of capabilities, incentives or both?”*, OECD Economics Department Working Papers*, No. 1476, OECD Publishing, Paris, https://doi.org/10.1787/7c542c16-en. [6]

Cybersecurity Ventures (2021), *Cybersecurity Jobs Report: 3.5 Million Openings In 2025*, https://cybersecurityventures.com/jobs/. [4]

DCMS (2022), *Cyber security skills in the UK labour market 2022*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf. [12]

DCMS (2018), *National Cyber Security Skills Strategy: increasing the UK’s cyber security capability*, https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views. [8]

Department for Education (2022), *Skills for life, skill bootcamps*, https://skillsforlife.campaign.gov.uk/courses/skills-bootcamps/. [15]

Find Apprenticeships (2022), *Cyber security apprenticeship*, https://www.findapprenticeships.co.uk/cyber-security-apprenticeships/. [13]

ISC2 (2022), *ISC2 cybersecurity workforce study*, https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx. [3]

NCSC (2023), *NCSC certification*, https://www.ncsc.gov.uk/section/products-services/ncsc-certification. [17]

NCSC (2022), *CyberFirst overview*, https://www.ncsc.gov.uk/cyberfirst/overview. [14]

NCSC & KPMG (2021), *Decrypting diversity: Diversity and inclusion in cyber security*, https://www.ncsc.gov.uk/files/KPMG-and-the-NCSC-Decrypting-Diversity-2021-report.pdf. [5]

Neto, I., M. Obiso and M. Baayen (2022), *How tailored national cybersecurity strategies enable safe, inclusive and sustainable digital development*, https://blogs.worldbank.org/digital-development/how-tailored-national-cybersecurity-strategies-enable-safe-inclusive-and. [7]

NIST (2022), *National Initiative for cybersecurity Education (NICE)*, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center. [10]

Public Safety (2018), *National Cyber Security Strategy - Canada’s vision for security and prosperity in the digital age*, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf. [11]

Specops (2021), *The countries experiencing the most ‘significant’ cyber-attacks*, https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/. [2]

The White House (2019), *Executive Order on America’s Cybersecurity Workforce*, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/. [9]

UK Cyber Security Council (2022), *Cyber security career pathways. Routes into and through the profession*, https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/. [16]

UNCDF (2022), *The role of cyber security and data security in the digital economy*, https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/62082f066a25c62651a9ae40/1644703527175/EN-UNCDF-Brief-CyberSecurity-2022.pdf. [1]

Notes

[1] Significant cyber attacks refer to any cyber attacks on a country's government agencies, defence and high tech companies, or economic crimes equating to loss of more than 1 million USD.

[2] Among 16 countries for which the cyber security workforce gap was estimated.

[3] Courses available at the moment of the search in September 2022 in Coursera, EdX, LinkedIn Learning, Udemy, FutureLearn and Skillshare.

2 Tracking the demand for cyber security professionals

This chapter discusses the main trends in the demand for cyber security professionals across Australia, Canada, New Zealand, the United Kingdom and the United States. The analysis is based on millions of online job postings collected throughout January 2012 and June 2022. Results show that the demand for cyber security professionals outpaced the growth in aggregate demand across the rest of occupations. This chapter also points out the heterogeneity within the demand for cyber security workforce, recognising those roles most demanded on each country. Finally, as a consequence of the quick adoption of new technologies across the world, the chapter discusses the rapid change in the skills enterprises in the cyber security sector are looking for.

Introduction: Filling the cyber security workforce gap

Technologies, such as Cloud Computing, Artificial Intelligence (AI) or the Internet of Things (IoT), offer great opportunities for societies to enjoy the benefits of an increasingly interconnected world. New digital tools allow businesses to expand their operations worldwide, increasing productivity and economic gains. However, the use of digital technologies pairs this range of new opportunities with a greater exposure to the risks of cyber attacks,[1] since digital platforms and the use of digital tools allow – and need – to share data with third parties, increasing business and organisations' exposure to potential cybercriminal activities (World Economic Forum, 2022[1]).

The COVID-19 pandemic also brought new challenges for enterprises as they started implementing remote work arrangements on a large scale to mitigate the effects of lockdowns on economic activity. While many jobs were saved during the lockdowns by teleworking arrangements, working from home can potentially increase the risk of cyberattacks since residential networks have less protection from cyber attacks. According to the 2022 Global Risk Perception Survey from the World Economic Forum, cyber security failures are one of the top 10 risks that have worsened the most since the pandemic and the first within the technological risks group (World Economic Forum, 2022[1]). These are just examples of how the accelerated adoption of new digital technologies during the last few years has considerably increased the risks of data security breaches.

In such a rapidly evolving landscape, economic actors need to be prepared to face new cyber-related challenges that require improved physical resources (i.e. hardware resources for running the specialised software) and protocols for data security but also to develop a skilled workforce that can create, analyse and manage cyber security solutions. Despite the increasing importance that cyber security has gained in recent years, enterprises around the world are still facing a significant shortage of skilled professionals in this area, limiting their ability to contain threats. The (ISC)^2 organisation, for instance, recently estimated a world's cyber security workforce gap of 2.7 million people ((ISC)2, 2021[2]).

Against this backdrop, analysing the most recent trends in the demand for cyber security professionals and understanding the profile of cyber security professionals in high demand can support policy makers in planning adequate education and training policies able to fill the emerging shortages and avoid future shortages across labour markets. Tracking the demand for cyber security skill demands is also key to anticipate future bottlenecks and for businesses and individuals to make informed workforce and training decisions going forward.

This chapter monitors the evolution of the demand for cyber security professionals from January 2012 to June 2022 in five countries: Australia, Canada, New Zealand, the United Kingdom, and the United States. This chapter leverages the information contained in nearly 400 million job postings collected from the internet (online job postings, OJPs) by Lightcast[2] to fill the knowledge gaps of analyses that relied on traditional labour market statistics, these latter are usually patchy and highly aggregated when it comes to the assessment of the demands for cyber security professionals and skills.

Using the information contained in online job postings has many advantages over traditional data sources such as labour force surveys or national accounting data (Box 2.1). First, OJPs data allow to track the emergence of skill demands in a timely manner as OJPs are collected daily from available jobs posted online. Second, information on skill demands in OJPs is far more granular than in other data sources, allowing to be much more detailed on the specific technologies and skills that are in high demand across the cyber security landscape. OJPs, however, also have some limitations as they may provide less comprehensive coverage of some occupations and sectors where vacancies are not typically advertised through online platforms (see (OECD, 2021[3]); and Cammeraat and Squicciarini (2021[4])). These limitations, however, are likely to be small in the current study as it investigates a specific part of the labour market demand that is typically channelled by online job postings.

The remainder of this chapter is organised in two sections. The first section provides an analysis of the demand for cyber security professionals from different perspectives. On the one hand, it compares the evolution and geographical distribution of cyber security OJPs across countries and reviews within each country how this demand compares to the aggregate demand for the rest of occupations. On the other hand, it exploits the granularity of OJPs data to address other relevant questions. Specifically, it explores the relation between the demand for cyber security professionals and that for other digital professions in a context of rapid digital transformation. Moreover, it identifies specific cyber security roles and reviews their demand across time. The second section, instead, provides insights into the main characteristics of jobs for cyber security professionals, leveraging information contained in firms' requirements to access the job. The section provides insights on the qualifications and education levels typically required to access the profession and the bundles of skills most relevant for cyber security professionals. It also provides information about earnings offered to potential applicants across countries as reported in OJPs.

Box 2.1. Methodological note: Interpreting the results from online job postings

The wealth of information contained in job postings can offer a very detailed overview of the demand of enterprises for cyber security profiles. This box summarises the main methodological approaches used to leverage these data in order to improve readability of the results and insights shown below. More details are also contained in Annex 2.A and in the footnotes to each figure.

Using OJPs to track the evolution of demand

- **Trends in the volume of OJPs:** To show the evolution in the amount of OJPs throughout the period of analysis, this report uses a standardised index of the monthly count of job postings. This index takes the value of 100 in January 2012, except for New Zealand where it starts in January 2013 due to data availability. A polynomial trend is calculated on this index to reduce noise.
- **Cyber security roles:** Using the job titles available in OJPs, this chapter identifies different cyber security roles (*Analysts, Architects and engineers, Auditors and advisors, Managers)* and tracks the evolution of their demand. Job titles are used in a first stage as an input to get the most frequent keywords used by recruiters to name the positions offered and then, in a second step, these keywords are used to define role groups in which each job posting is classified.
- **Groups of digital, engineering and math related occupations:** The analysis provides insights on more than 40 occupations used to compare the trends in their demand with the demand for cyber security professionals. The 40+ occupations were classified in four occupational groups: Chief Information Officers, Computer-based professions, Math-related professions and Engineers and technicians.

Using OJPs to infer skill demands

- **Skill bundles:** Using Natural Language Processing (NLP) approaches, the analysis in this chapter identifies the most relevant skills in employer's demands for cyber security positions collected through OJPs. As detailed also in Box 2.3, this "skill relevance" index should be interpreted as a measure of relevance of a given skill in the cyber security profession. In this context is also important to notice that keywords collected from OJPs do not only represent skills *strictu sensu*. Some of them, for instance, are technologies or tools (i.e. Python or Microsoft Azure), while others identify knowledge areas (i.e. Network or Information Security). For the sake of simplicity, this study pools all keywords together under the term "skills" and only differentiate between them if necessary.

The demand for cyber security professionals

The impact that the digital transition is having on labour markets is a reality that has attracted a lot of attention in recent years. A recent study (OECD, 2022[5]), for instance, shows the significant increase in demand for digital professionals across labour markets as well as the increasing pace by which digital technologies are permeating workplaces, spreading across an increasing number of different sectors and occupations. Cyber security professionals are one amongst the many digital occupations that have shown strong growth recently, reflecting the fast-paced adoption of digital technologies in the workplace and in productive processes.

The cyber security profession[3] encompasses a wide variety of different roles and jobs. Most professionals in this area are in charge of securing data, systems, infrastructure and other cyber resources from failures, hazards and cyber threats that affect an organisation mission and operation (World Economic Forum, 2022[6]). This section focus on tracking the demand for professionals in this area in each country using the online job postings classified in this occupation following the Lightcast taxonomy.

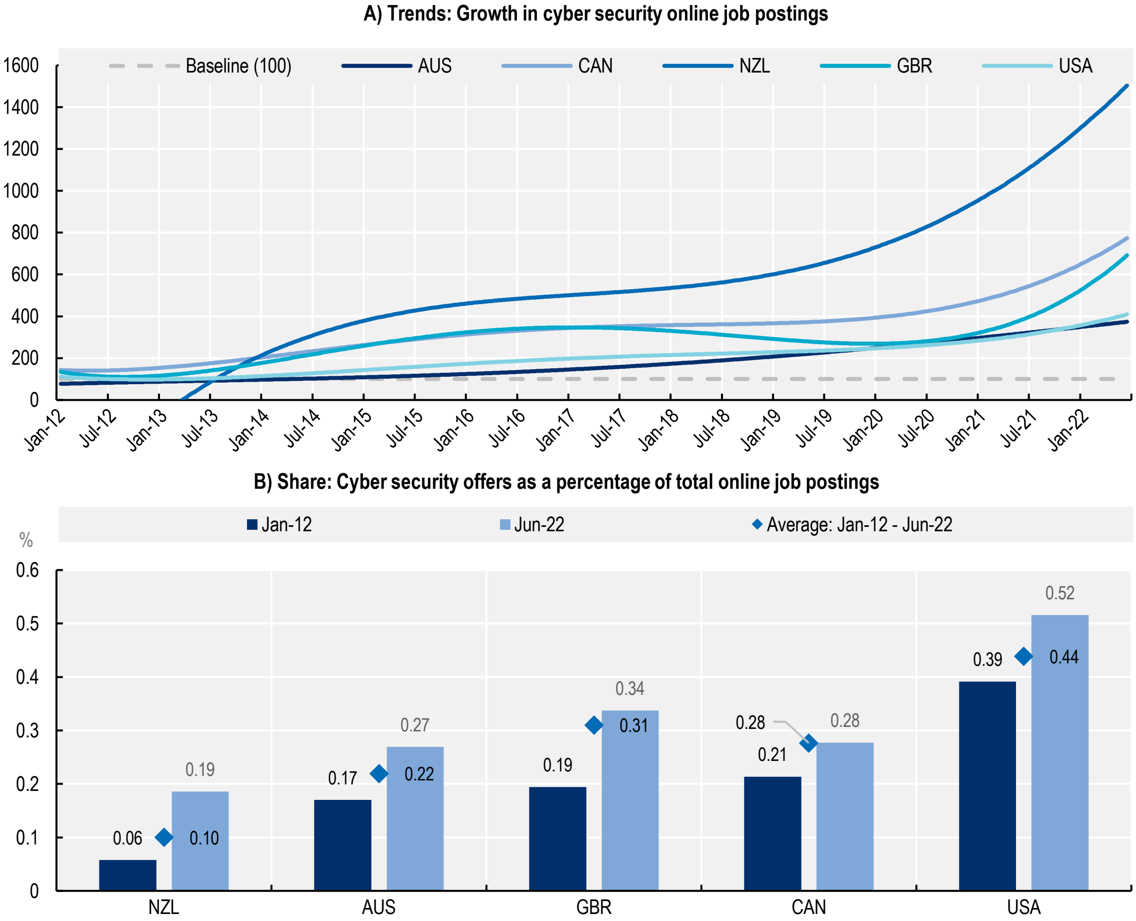
What has been the evolution of the demand across countries?

Figure 2.1 (Panel A) shows the trends exhibited by a standardised index calculated on the monthly count of job adverts. This index allows for easier comparison across countries over the time. In line with the fast-paced digital transformation of labour markets (OECD, 2022[5]), the analysis of OJPs in Figure 2.1 (Panel A) shows that the monthly demand for cyber security professionals has been significantly increasing in the last decade in the five countries covered in this report. In June 2022, for instance, the volume of new job adverts in the cyber security domain was between three to 16 times the number of recorded job postings at the beginning of 2012, almost double the speed of expansion recorded for all new job postings in the same period. The pace by which the demand for cyber security professionals has grown, however, differs by country.

While growth in demand has been positive across all geographies, results in (Figure 2.1, Panel A) seem to suggest that the COVID 19 pandemic may have partially affected the demand for cyber security professionals in early 2020. Since 2021, as economies started to open up again after the severe economic shock imposed by the pandemic, the demand for cyber security professionals has started increasing again significantly and at a much faster pace than in the pre pandemic period. This result is likely reflecting the expansion of remote working activities around the world, which imposed new technological challenges for enterprises that faced increased cyber security threats. Results for the United Kingdom, in particular, show a decreasing trend in OJPs for cyber security professionals between January 2017 and July 2020, earlier than in other countries. This is likely to reflect the effects of the political developments happening in the United Kingdom during the Brexit negotiations that led to increased uncertainty in the transition phase as the reduction in OJPs starting in 2017 is widespread and not exclusive to the cyber security jobs (see Figure 2.2, Panel D).

Figure 2.1. Cyber security Online Job Postings: Trends and shares

Polynomial trends calculated on a standardised index (Jan-12 = 100) of the monthly count of job postings



A) Trends: Growth in cyber security online job postings

B) Share: Cyber security offers as a percentage of total online job postings

Note: For Panel A, polynomial trends are calculated on a standardised index (Jan-12 = 100) for the monthly count of job postings. This index shows the evolution in the demand for a given profession in comparison to this month. Data for NZL starts on January 2013.
Source: OECD calculations based on Lightcast data.

Overall, results in Figure 2.1 (Panel A) suggest that the growth in demand for cyber security professionals in New Zealand and Canada has been the strongest in the period between January 2012 and June 2022, followed by the United Kingdom, the United States and Australia. While this figure suggests a slower growth in the demand of cyber security professionals in the United States relative to other geographies, this result can be partly explained by the largest size of the United States' cyber security market in 2012 relative to that in other countries.

In January 2012, the job postings seeking cyber security professionals in the United States accounted already for roughly 0.4% of total job postings in the same month (Figure 2.1, Panel B). This figure is almost twice the share of postings in the United Kingdom market and more than 6 times that in New Zealand. Results indicate, in other words, that the United States was already a much more mature cyber security labour market in 2012 and, while the growth in the following years has still been positive and above the average of other professions, this was slower than in other countries where the market started to develop much more strongly in later years. Differences in the size of the cyber security market at the beginning of the period are likely to explain some of the differences in the rate of growth in more recent years, where countries that were lagging in absolute volume of cyber security vacancies have started to catch up with more mature economies like the United States. Other factors, however, may be playing important roles in the overall evolution of the demand across countries. These are analysed in the following sections.

How does the demand for cyber security professionals compare with other occupations?

A particularly relevant question relates to how the demand for cyber security professionals compares to the rest of professions and to the overall dynamics of job vacancies. Figure 2.2 shows the standardised indexes capturing the demand for cyber security professionals and compares the trends with that for the rest of occupations. In the countries covered, the growth in demand for cyber security professionals significantly outpaced the aggregate demand across other occupations. Different patterns, however, can be observed across countries.

In the United States (Figure 2.2, Panel E), for instance, the demand for cyber security professionals has closely followed the evolution in other occupations, although it has grown faster in most of the period. The most notable differences, in favour of cyber security demands over the total economy, can be observed in the period 2016-19 and, particularly, in 2022 where the demand for cyber security professionals has been relatively stronger. Demand for cyber security professionals only slowed in the United States during the pandemic, with a strong dip in May 2020 despite a rapid rebound afterwards.

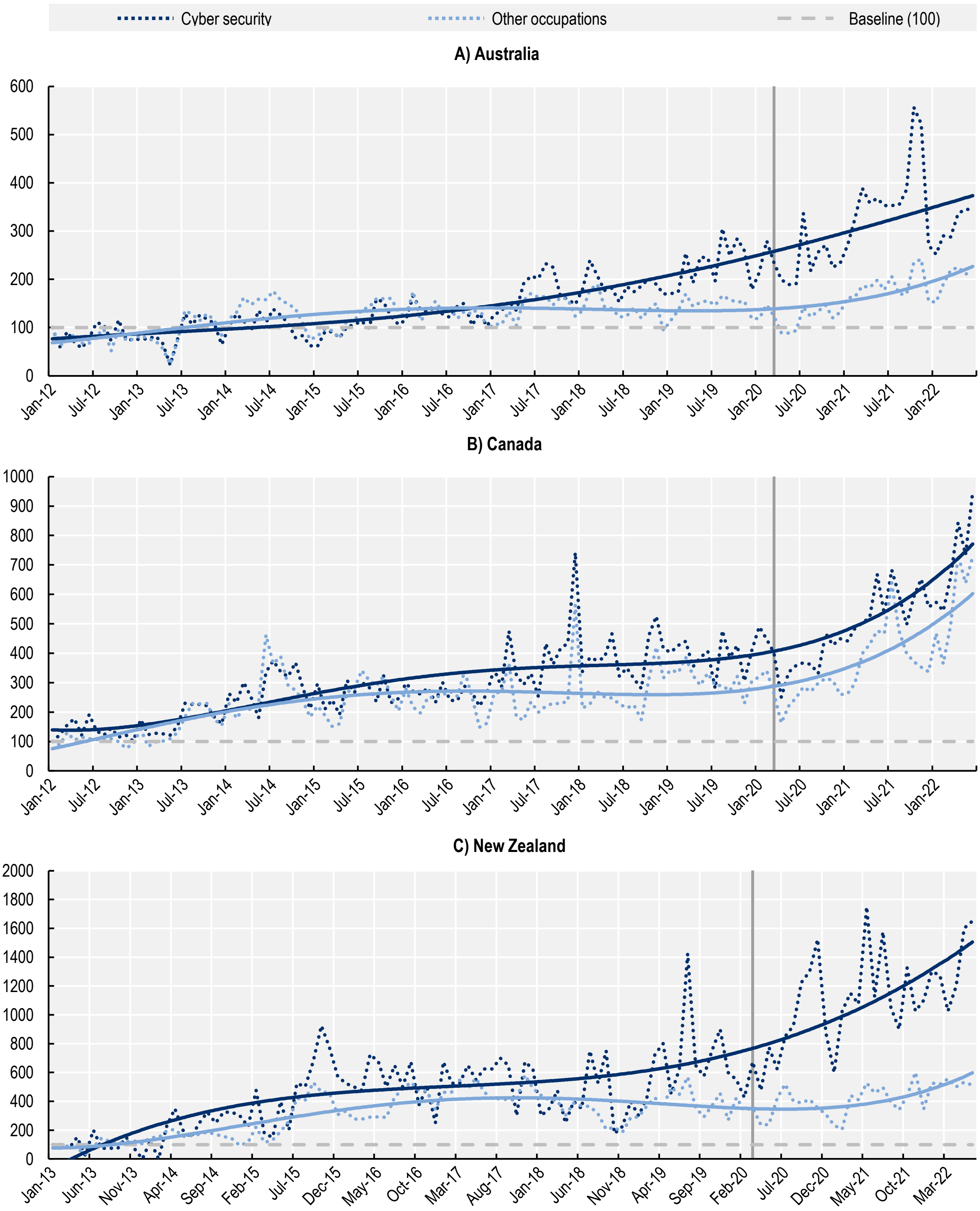
In Canada and the United Kingdom, the growth in demand for cyber security professionals significantly exceeded that of other occupations. Starting in early 2014 (2015 for Canada), the demand for cyber security roles increased faster than in the rest of the occupations in both countries. Analyses of cyber security sectoral demand carried out in the United Kingdom in 2021 confirm that, during the period 2017 19, the sector experienced double digit growth with an estimated employed workforce growth of nearly 50% (Ipsos MORI, Perspective Economics, CSIT, 2021[7]). Despite this remarkable growth in the United Kingdom, it is also noticeable that the gap between the growth of job postings for cyber security professionals and those for the rest of professions shrunk during the 2017-20 period. As pointed out before, the declines in the volume of cyber security job postings can reflect the uncertainty related to political developments such as Brexit's negotiation process as well as the most recent and unprecedented shock related to the COVID 19 pandemic. Figure 2.2 suggests that these events could have had a stronger effect on the demand for cyber security professionals than for the rest of the occupations.

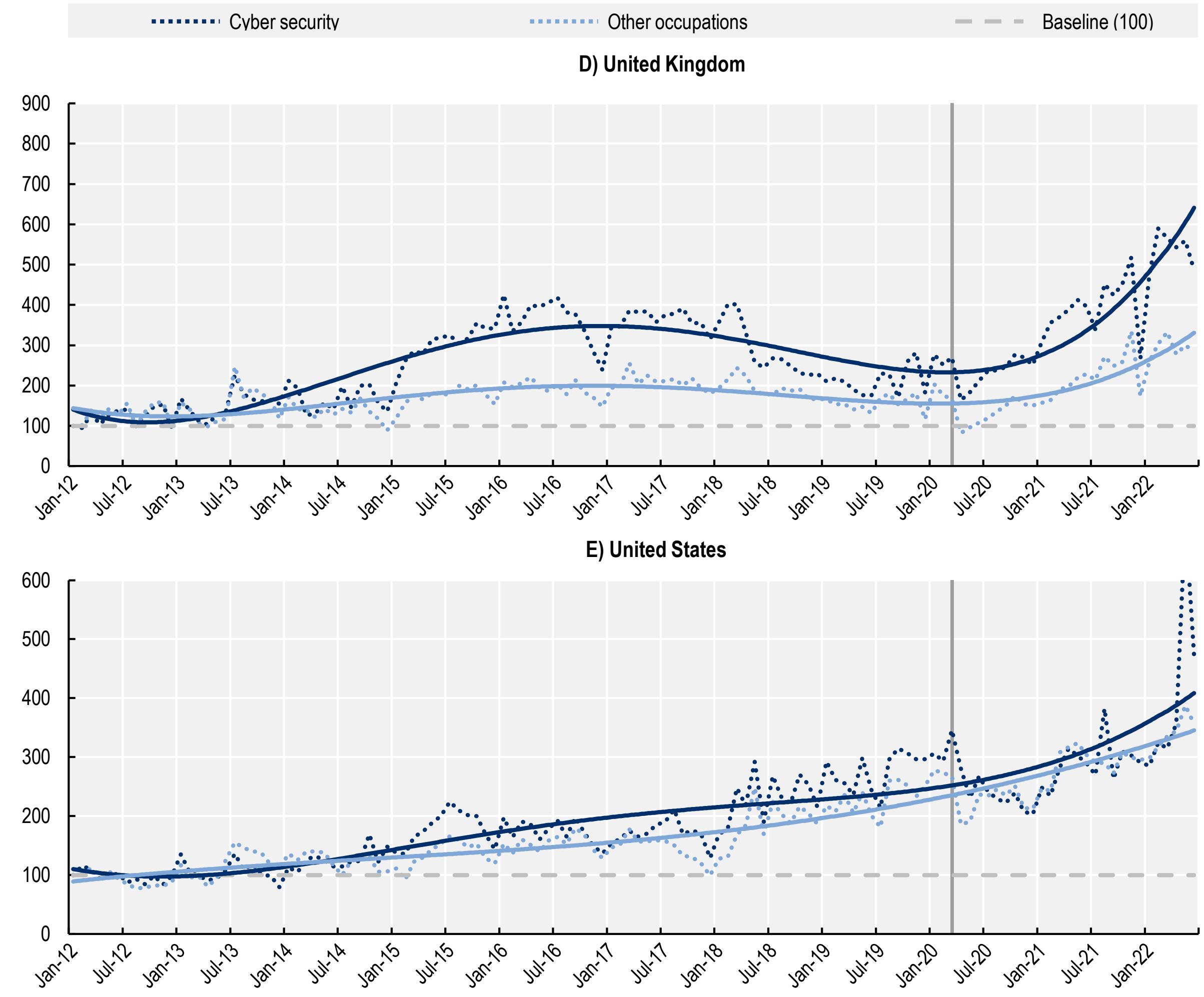
During Brexit, in particular, concerns about the negative impacts on the cyber security sector emerged due to the uncertain consequences on corporation's investment decisions in the United Kingdom and the potential reduction in the number of cyber security professionals willing -and able to arrive to work in the sector (Stevens and O'Brien, 2019[8]). In fact, according to the EY Financial Services Brexit Tracker, between March 2017 (after the triggering of Article 50) and March 2021 the proportion of firms that announced plans to move some operations or staff from the United Kingdom nearly doubled, from 24% to 43%. Additionally, 24 firms declared they will transfer more than GBP 1.3trn of UK assets to the EU (EY, 2022[9]). This context potentially affected the hiring decisions of companies looking for cyber security professionals.

In Australia and New Zealand, the number of new job postings for cyber security professionals has steadily increased since 2017, continuously widening the growth gap with the rest of professions. Notably in these countries, the pandemic in 2020 does not seem to have affected the demand. On the contrary, in the period following the declaration of the pandemic the differences in the demand for cyber security and other occupations has increased. This trend can be explained, to a certain extent, by the expansion of remote work arrangements during the pandemic which led to an increasing demand for cyber security solutions across a wide range of businesses. The Australian Cyber Security Growth Network indicates, for instance, that during 2020 medium-sized cyber security providers recorded significant increases in their revenues (+21.6%), while small-sized enterprises reported moderate decreases (-5.1%) and large companies revenue remained unaltered (0.1%). In the same survey, only 13% of the enterprises reported a decrease in their workforce, while 18% reported an increase (Australian Cyber Security Growth Network, 2020[10]).

Figure 2.2. Growth in online job postings: Cyber security and all occupations

Polynomial trends (solid lines) calculated on a standardised index (Jan-12 = 100) of the monthly count of OJPs





Note: The standardised index shows the evolution in the demand for a given profession in comparison to the month of reference. Data for NZL starts on January 2013. Vertical line reflects the declaration of COVID-19 as pandemic (March 2020).
Source: OECD calculations based on Lightcast data.

A geographical view of the demand for cyber security professionals

The granularity of job postings data offers a unique opportunity to assess the geographical dimension of the demand for cyber security professionals by investigating the distribution of cyber security-related job postings within a country and assessing the degree of geographical concentration of such demand. In particular, data on job postings allows an assessment of how the geographical distribution of cyber security demand has evolved in recent years and whether the concentration in the demand has increased or, else, spread out even further, with lagging regions catching up in the demand.

Using the geographical location available in OJPs, Figure 2.3 to Figure 2.7 show two maps for each country examined:

1. Map A shows the average share of job postings for cyber security professionals in each geographical area (see Box 2.2) relative to the country's total number of cyber security OJPs over the period between January 2012 and June 2022.[4]
2. Map B captures the evolution over time and geographies by showing the change in percentage points of the share of cyber security OJPs, relative to the total country's volume of cyber security OJPs, during the periods 2012-19 and 2020-June 2022 to distinguish between older and more recent trends in the geographical distribution of the demand for cyber security professionals.

Generally, across countries, results show that most of the jobs postings for cyber security professionals are in large urban areas or economic centres where also major enterprises and governments agencies' headquarters are located. In these areas, global interconnectivity in financial, industrial, government and other sectors increasingly require the availability of secure IT services and infrastructure, as well as of a talented workforce that can protect their businesses.

Figure 2.3 (map A) shows the share of OJPs for cyber security professionals across the Australian territory divided by statistical areas Level 4 (SA4). Areas located in the southeast of the country gather most of the job postings for cyber security professionals over the period of analysis (January 2012-June 2022). Sydney, as the financial and economic centre of Australia, stands out as the area with the highest share of cyber security job postings with roughly 40% of the total. Melbourne and the Australian Capital Territory (ACT), where the headquarters of the Australian Government are located, follow with 22% and 12% of total cyber security job postings respectively. Similarly, Figure 2.5 (map A) shows that a high proportion of cyber security job postings in New Zealand are concentrated in the cities of Auckland and Wellington. Following the same pattern seen in Australia, economic and political centres in New Zealand account for most of the cyber security job adverts, as these two cities represent 83% of the job postings for this profession (41% and 42% respectively). Christchurch, in the South Island completes the top-3 geographical locations with 7% of the job postings in New Zealand.

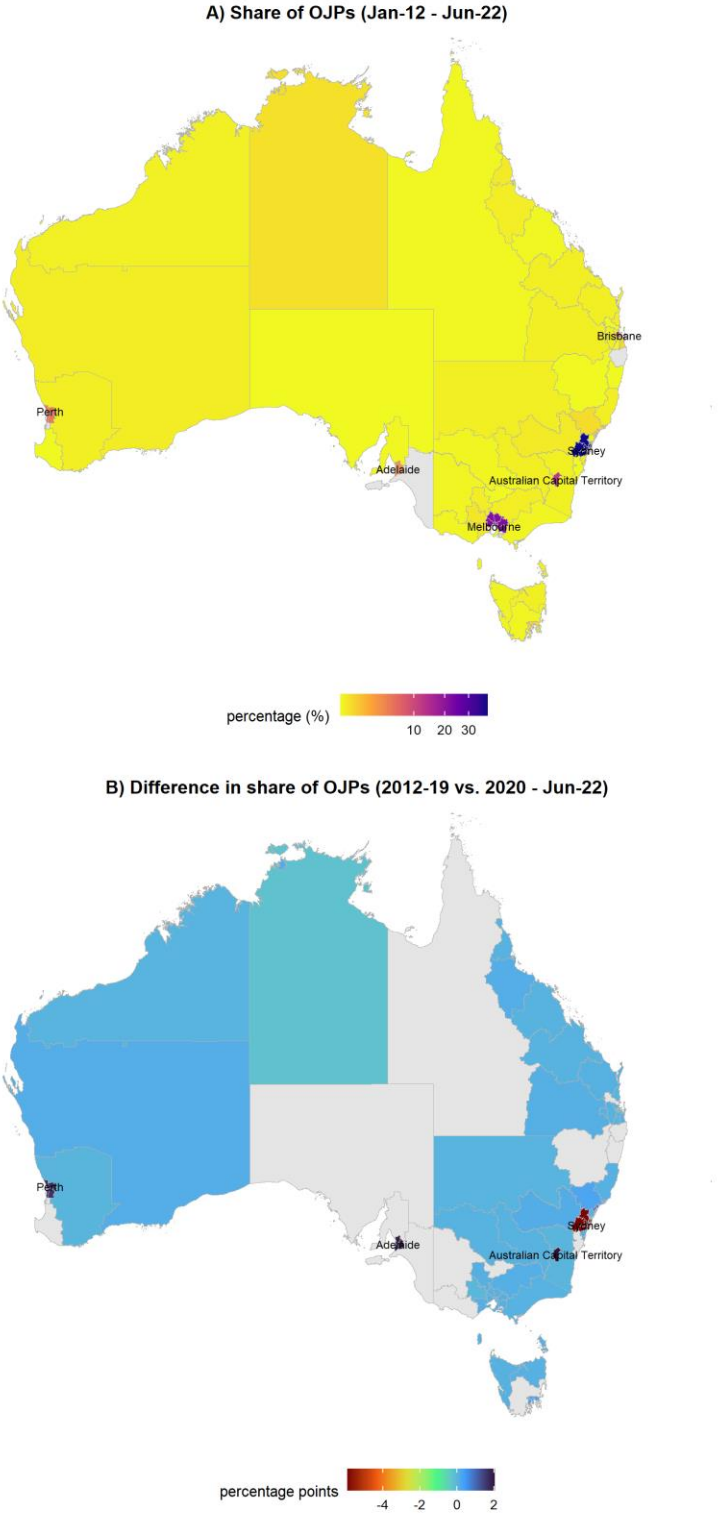
Other countries show a distribution that is even more concentrated than in Australia and New Zealand. Figure 2.4 (map A) presents the cyber security job postings shares in the Canadian territory divided by cities. The cluster Toronto-Mississauga-Markham makes roughly 40% of the job postings for cyber security workforce. Ottawa (9%), the political centre, Montreal (9%), Calgary (7%) and Vancouver (6%) follow in the raking with significantly smaller shares and concentration of job postings than Toronto.

In the United Kingdom (Figure 2.6, map A), London accounts for 38% of the cyber security job postings, followed by Manchester (5%) and Birmingham (3%). The importance of the latter relies on its position as second largest city in the United Kingdom (by population) and for its strong demand for workers in IT-related positions. Edinburgh and Glasgow together represent 3% of total OJPs for cyber security, while Belfast and Cardiff respectively account for 0.7% and 0.5% of the cyber security OJPs posted in the United Kingdom during January 2012 – June 2022.

The United States is the only exception to such highly concentrated distribution of the demand for cyber security workforce. Figure 2.7 (map A) shows the United States map divided by counties. The areas of Fairfax and the District of Columbia (DC) are at the top of the ranking by number of OJPs for cyber security professionals with 4.6% and 3.4% of the job postings, respectively. Both areas play an important role as home to the headquarters of federal government institutions. In the case of Fairfax, the strong relative demand for cyber security professionals is likely related to this city being home to key intelligence and national security institutions, such as the Central Intelligence Agency (CIA). Other economic centres across the country closely follow the federal government areas, such as New York (3.3%), Cook County (Chicago) (2.7%), Fulton County (Atlanta) (2.6%), Dallas (2.5%), Los Angeles (2.5%) and Santa Clara (2.1%).

The less geographically concentrated distribution of cyber security job postings in the United States can be traced back to several factors intertwining productive structure, technological leadership and adoption of digital technologies. In particular, the US federal administrative structure may imply the establishment of state level cyber security institutions which can be reflected in a more spread geographical distribution of the demand. Additionally, a relatively a more digitally-mature economic structure and a stronger cyber security capacity (see IMD World Competitiveness Center (2022[11]) and International Telecommunications Unit (2020[12])) have likely contributed to the demand for cyber security professionals being more spread out across a wider set of productive sectors and, hence, across geographies earlier than in other countries.

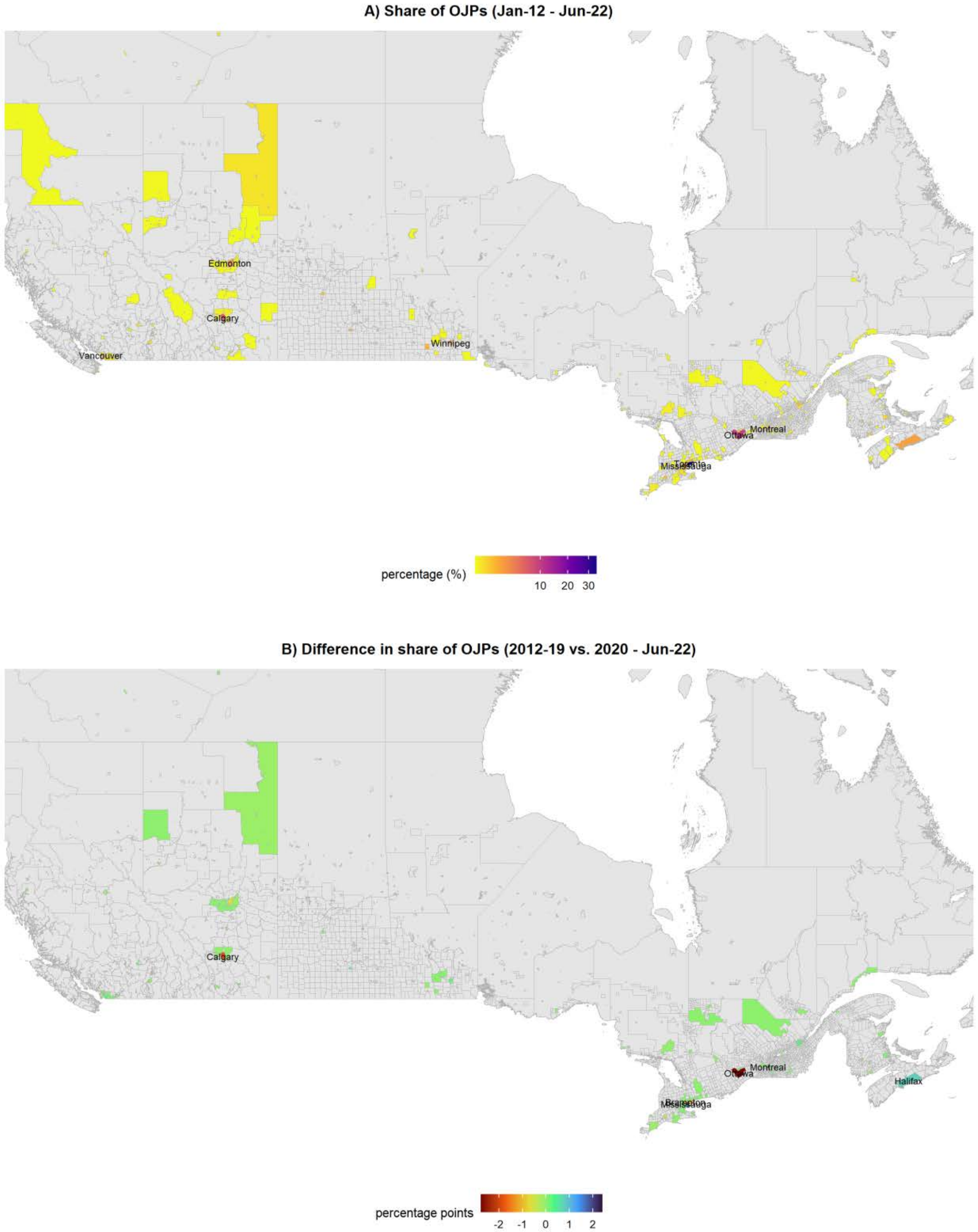
Figure 2.3. Australia: Geographical distribution of cyber security job postings (2012-22)


A) Share of OJPs (Jan-12 - Jun-22)
Brisbane
Perth
Sydney
Adelaide
Australian Capital Territory
Melbourne
percentage (%)
10
20
30
B) Difference in share of OJPs (2012-19 vs. 2020 - Jun-22)
Perth
Sydney
Adelaide
Australian Capital Territory
percentage points
-4
-2
0
2

Note: Grey areas indicate non-available information. Names are shown for areas with higher share of job postings (map A) or with higher change (positive or negative) between the two periods (map B).

Source: OECD calculations based on Lightcast data. Digital boundary file downloaded from Australia Bureau of Statistics (Jul2021-Jun2026[13]), https://www.abs.gov.au/statistics/standards/australian-statistical-geography-standard-asgs-edition-3/jul2021-jun2026/access-and-downloads/digital-boundary-files licensed under a Creative Commons Attribution 4.0 International licence.

Figure 2.4. Canada: Geographical distribution of cyber security job postings (2012-22)



A) Share of OJPs (Jan-12 - Jun-22)

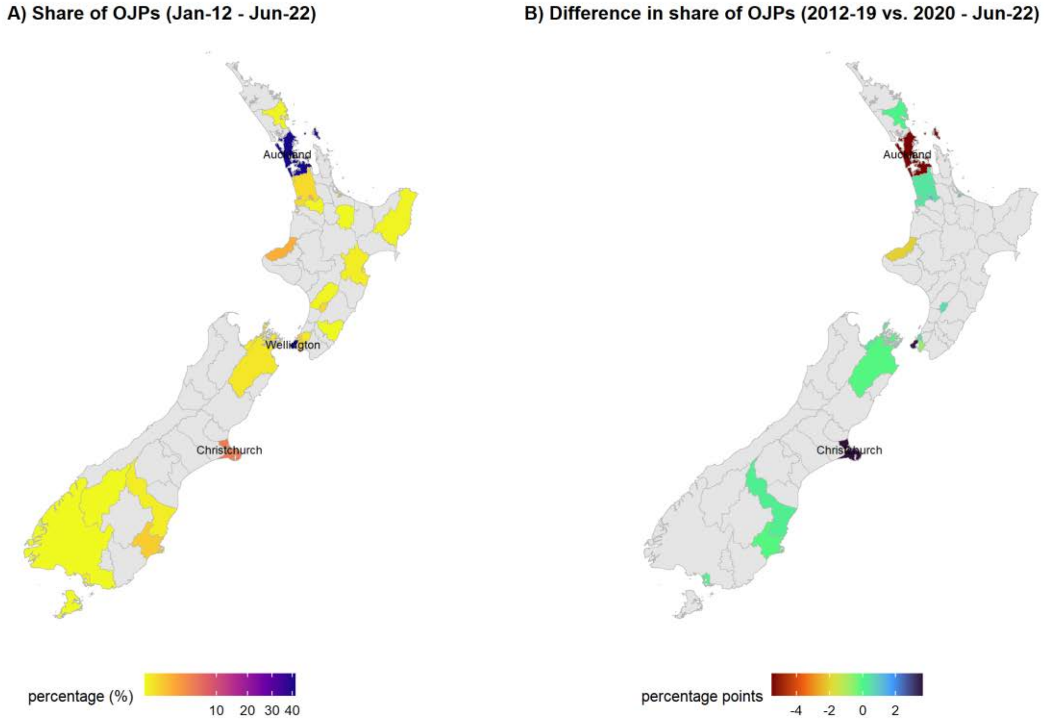
B) Difference in share of OJPs (2012-19 vs. 2020 - Jun-22)

Note: Grey areas indicate non-available information. Names are shown for areas with higher share of job postings (map A) or with higher change (positive or negative) between the two periods (map B). Given the location of job postings, a zoom into the southern area of Canada is provided to improve readability.

Source: OECD calculations based on Lightcast data. Digital boundary file adapted from Statistics Canada (2022[14]), https://www12.statcan.gc.ca/census-recensement/2021/geo/sip-pis/boundary-limites/index2021-eng.cfm?year=21. This does not constitute an endorsement by Statistics Canada of this product.

Notably, even though across most countries a large share of OJPs for cyber security professionals still remain in administrative capitals and main cities, in the last two years (January 2020 - June 2022) the geographical concentration of cyber security job postings in those economic poles has decreased significantly compared to the 2012-19 period. Figure 2.3 (map B) shows, for instance, that the share of cyber security job postings in Sydney shrunk by roughly 6 percentage points from 42% in 2012-19 to 36% in 2020-22. Conversely, the ACT, Adelaide and Perth grew approximately 2 percentage points each between the same two periods. In a more detailed view, Figure 2.8 (Panel A) shows that Sydney's yearly share decreased continuously during 2017 and 2020, while Melbourne's share increased consistently during the same years, except during the pandemic in 2020. The opposite direction of the two trends for Sydney and other cities in Australia suggests that in the last years, smaller centres have been growing their demand for cyber security professionals, as firms and organisations in those territories are increasingly adopting digital technologies and facing the risks of cyber attacks.

Figure 2.5. New Zealand: Geographical distribution of cyber security job postings (2012-22)



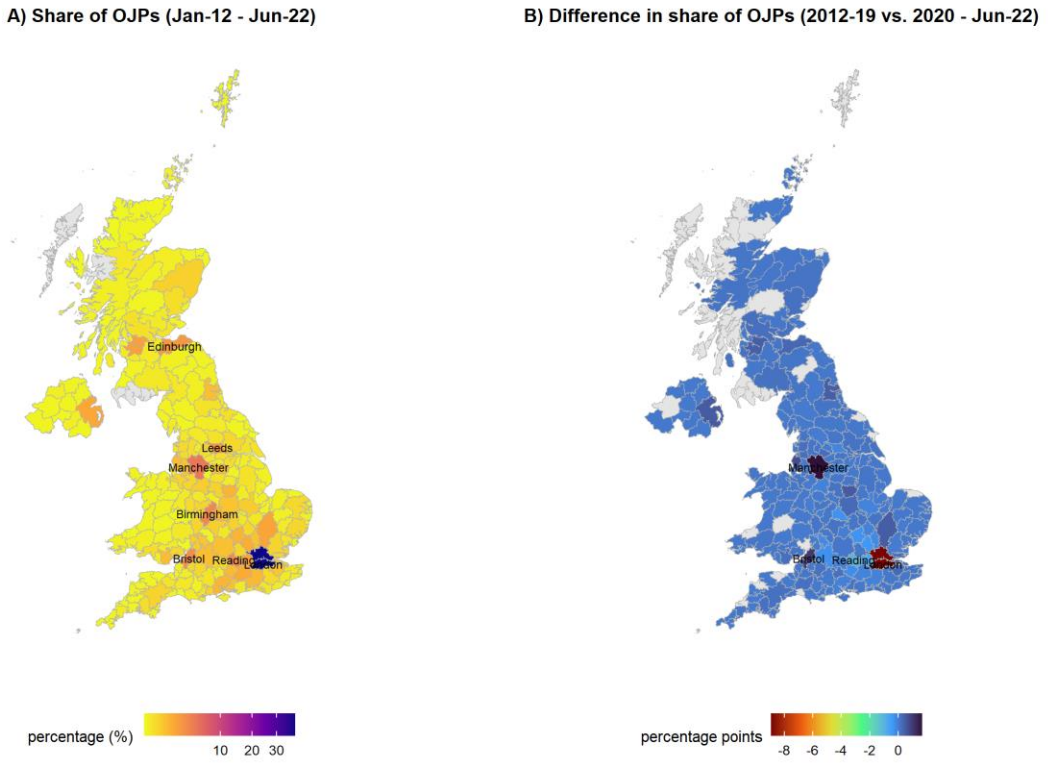
Note: Grey areas indicate non-available information. Names are shown for areas with higher share of job postings (map A) or with higher change (positive or negative) between the two periods (map B). Given the location of job postings, the map is focused on the mainland (North and South islands) in order to improve readability.
Source: OECD calculations based on Lightcast data. Digital boundary file downloaded from Stats New Zealand (2023[15]), https://datafinder.stats.govt.nz/layer/92215-territorial-authority-2018-clipped-generalised/ licensed under a Creative Commons Attribution 4.0 International licence.

In the United Kingdom, the share of cyber security job postings in London declined by 9 percentage points from 42% to 33% between the two periods (Figure 2.6, map B). Conversely, the share of job postings published in Manchester increased by 2 percentage points to 6%, the highest increase in the United Kingdom, followed by Bristol with an increase of 1 percentage point to 4%. The increase in the demand in the Bristol area is likely to be related with its proximity to the government Communication Headquarters (GCHQ), the parent organisation of the National Cyber Security Centre (NCSC). Similarly to the dynamics in Sydney, Figure 2.8 (Panel D) for the United Kingdom shows that the yearly share of cyber security job posting in London has decreased consistently from 2017 onwards, except in 2022. The negative trend in London is paired with the steady increase in Manchester's share of cyber security job postings between 2017 and 2022, signalling the significant growth in the demand in the latter, possibly linked to the recent local strategies, such as the Manchester Digital Security Hub (DiSH) (Greater Manchester Combined Authority, 2021[16]).

In Canada results are more mixed. The share of cyber-related job postings in the area of Toronto has remained stable between the two periods (a decrease of 1 percentage point in Toronto is offset by a similar increase in Mississauga). Meanwhile, Montreal experienced the highest increase in the country, going from a share of OJPs of 8% to 11% relative to the total. Nevertheless, Ottawa and Calgary reduce their cyber security job postings shares by 3 percentage points and 2 percentage points, respectively. Figure 2.8 (Panel B) shows a decreasing trend in Ottawa's share since 2014 that contrasts with significant increases in Toronto's share in 2015 and 2018.

In the case of the United States, changes in the distribution of the demand for cyber security professionals are relatively smaller (Figure 2.7, map B). The economic and financial centres of New York and Cook County (Chicago) experience a decrease in their shares of approximately 1 percentage point to 3% and 2% respectively. DC and Fairfax shares remain stable. However, Figure 2.8 (Panel E) exhibits that both areas suffered a significant decrease in their relative demand during 2021, a result that may respond to measures taken during the COVID-19 pandemic.

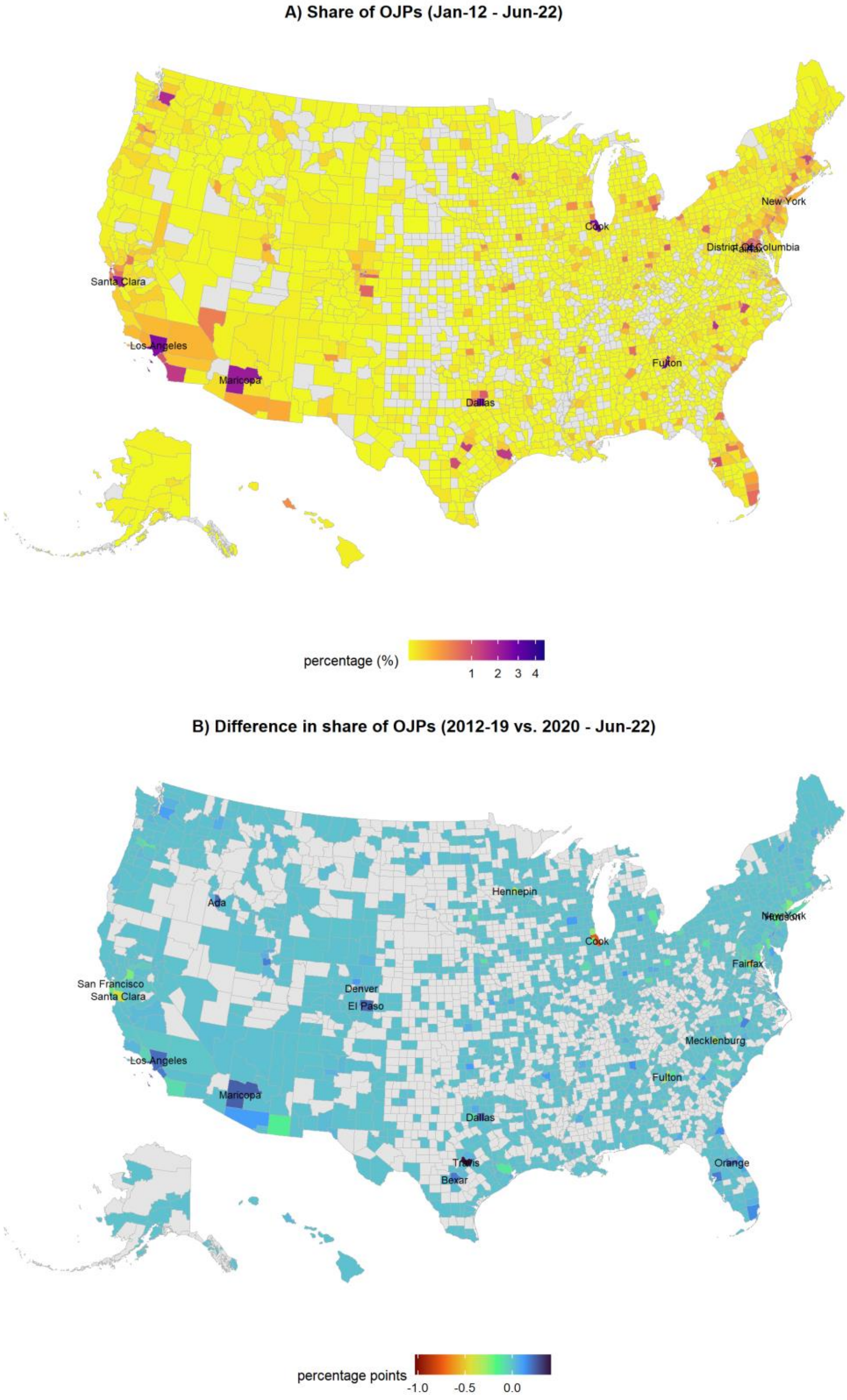
Figure 2.6. United Kingdom: Geographical distribution of cyber security job postings (2012-22)



Note: Grey areas indicate non-available information. Names are shown for areas with higher share of job postings (map A) or with higher change (positive or negative) between the two periods (map B).

Source: OECD calculations based on Lightcast data. Digital boundary file downloaded from the Office for National Statistics (2019[17]), https://geoportal.statistics.gov.uk/datasets/ons: travel-to-work-areas-dec-2011-bfe-in-united-kingdom/explore?location=55.215431%2C-3.313445%2C6.09 licensed under the Open Government Licence v.3.0.

Figure 2.7. United States: Geographical distribution of cyber security job postings (2012-22)



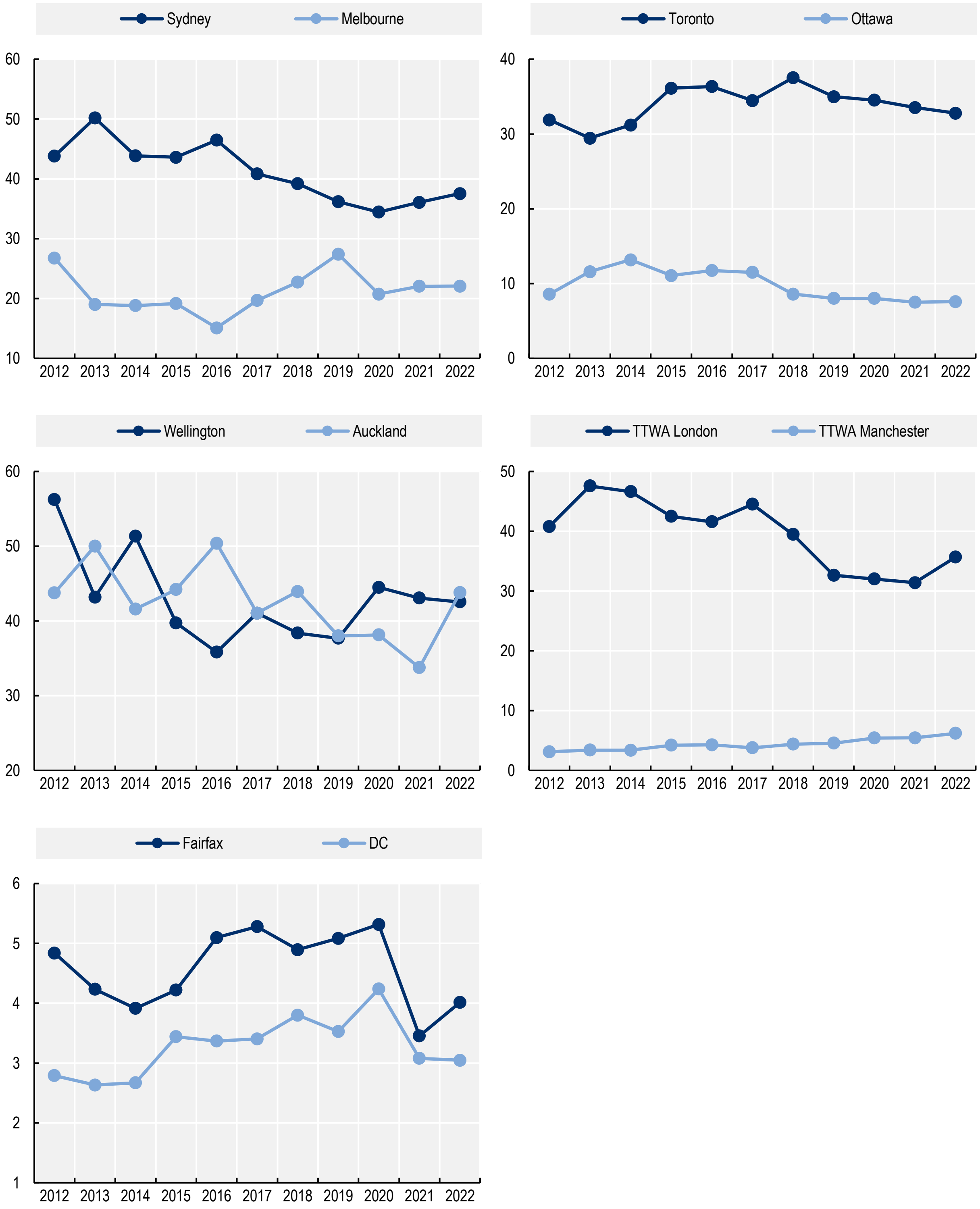
A) Share of OJPs (Jan-12 - Jun-22)

B) Difference in share of OJPs (2012-19 vs. 2020 - Jun-22)

Note: Grey areas indicate non-available information. Names are shown for areas with higher share of job postings (map A) or with higher change (positive or negative) between the two periods (Map B). Sizes of Alaska and Hawaii states are adjusted for readability reasons.
Source: OECD calculations based on Lightcast data. Digital boundary file used under the R library "urbanmpr" from the Urban Institute (2019[18]), https://github.com/UrbanInstitute/urbnmapr. Code released under the GNU General Public License v3.0.

Figure 2.8. Yearly evolution of cyber security job posting shares: Main areas per country

Areas’ share over the total amount of cyber security OJPs per country and year (as a percentage)



Note: TTWA refers to Travel to work Areas in the United Kingdom (see Box 2.2).
Source: OECD calculations based on Lightcast data.

The decreasing geographical concentration of cyber security related OJPs in main urban areas of most of the countries analysed suggests that as a country moves towards increasing adoption of digital technologies throughout their subnational geographies, cyber security markets become more mature, leading to an increase in the demand across the territory and a demand for cyber security professionals that is geographically less concentrated.

Box 2.2. Geographical information in Lightcast datasets

Data on job postings include different variables for indicating the geographical location of a job offer, ranging from broad indicators, such as the country name or main regions/provinces, to more detailed ones, such as the longitude and latitude co-ordinates. In order to show the demand for cyber security professionals in a more detailed view, Figure 2.3 to Figure 2.7 exploits information about the location of job postings in sub-national boundaries. Following, it is explained the geographical level used for each country and the source of the boundaries file used:

Australia

Data is presented for the Statistical Areas Level 4 (SA4). According to the Australian Bureau of Statistics (2022[19]), "*SA4s are the largest sub-state regions in the Main Structure of the* [Australian Statistical Geography Standard] *ASGS and are designed for the output of a variety of regional data, including data from the 2021 Census of Population and Housing*". Lightcast data includes the SA4 code for each job posting without specifying employment centres inside larger cities. Thus, several SA4 areas around cities, such as Sydney or Melbourne, are showed as they were only one. The digital boundaries file was retrieved from the Australia Bureau of Statistics (Jul2021-Jun2026[13])

Canada

Data on OJPs for Canada specifies two levels of geographical disaggregation: Provinces/territories and census subdivisions (municipalities). In order to show more granular results, maps for Canada are presented at the municipalities level, according to the classification provided by Lightcast. The digital boundaries file was retrieved from Statistics Canada (2022[14]).

New Zealand

In this case, the analysis was conducted at the territorial authorities' level, since Lightcast data only includes information for this level of geographical disaggregation. This is the second level of local government in New Zealand. The digital boundaries file was retrieved from Stats New Zealand (2023[15]) and focuses on the mainland (North and South islands).

United Kingdom

Data is shown at the Travel to Work Areas (TTWA) level. TTWA are the official British definition of local labour market areas. They are defined by the UK Office for National Statistics using workers' residence and workplace areas. Its latest update was in 2011 and comprehends 228 areas. The boundaries file was retrieved from the Office of National Statistics (2019[17]).

United States

Data is at the county level for the United States. In this case, the boundaries file is directly retrieved from an R package called "urbnmpr" from the Urban Institute (Strochak, Ueyama and Williams, 2022[20]). See also the Urbnmpr web page in GitHub for more detail (Urban Institute, 2019[18]). This package has the advantage of using maps from the US Census Bureau and includes Alaska and Hawaii in a reduced scale to facilitate the map display.

What is the relationship between the demand for cyber security professionals and that of other digital, engineering and math-related occupations?

The expansion of the demand for cyber security professionals in the last years responds to increasing concerns related to the strategic development of companies and the vulnerability of their systems in a landscape of rapid digital transformation. These concerns have emerged due to the expansion of artificial intelligence and remote working across a variety of sectors. In the Global Cybersecurity Outlook 2022, the World Economic Forum (2022[6]) surveyed 120 global leaders in the cyber security sector, finding that the factors with the greatest influence in organisations' approach to cyber security are the digital transformation, cyber attacks to third-party enterprises (i.e. service providers, suppliers, contractors, etc.) and regulatory requirements. Moreover, in the same survey, experts state that two of the more influential trends in the future for cyber security would be the implementation of automation and machine learning, and the expansion of remote/hybrid work environments (World Economic Forum, 2022[6]).

The digital transition (OECD, 2022[5]) and the expansion in the demand for digital-related occupations across labour markets is, hence, very likely to be a key driver for the increase in the demand for cyber security professionals as firms adopt new digital technologies that are potentially threatened by vulnerability, attacks and malwares.

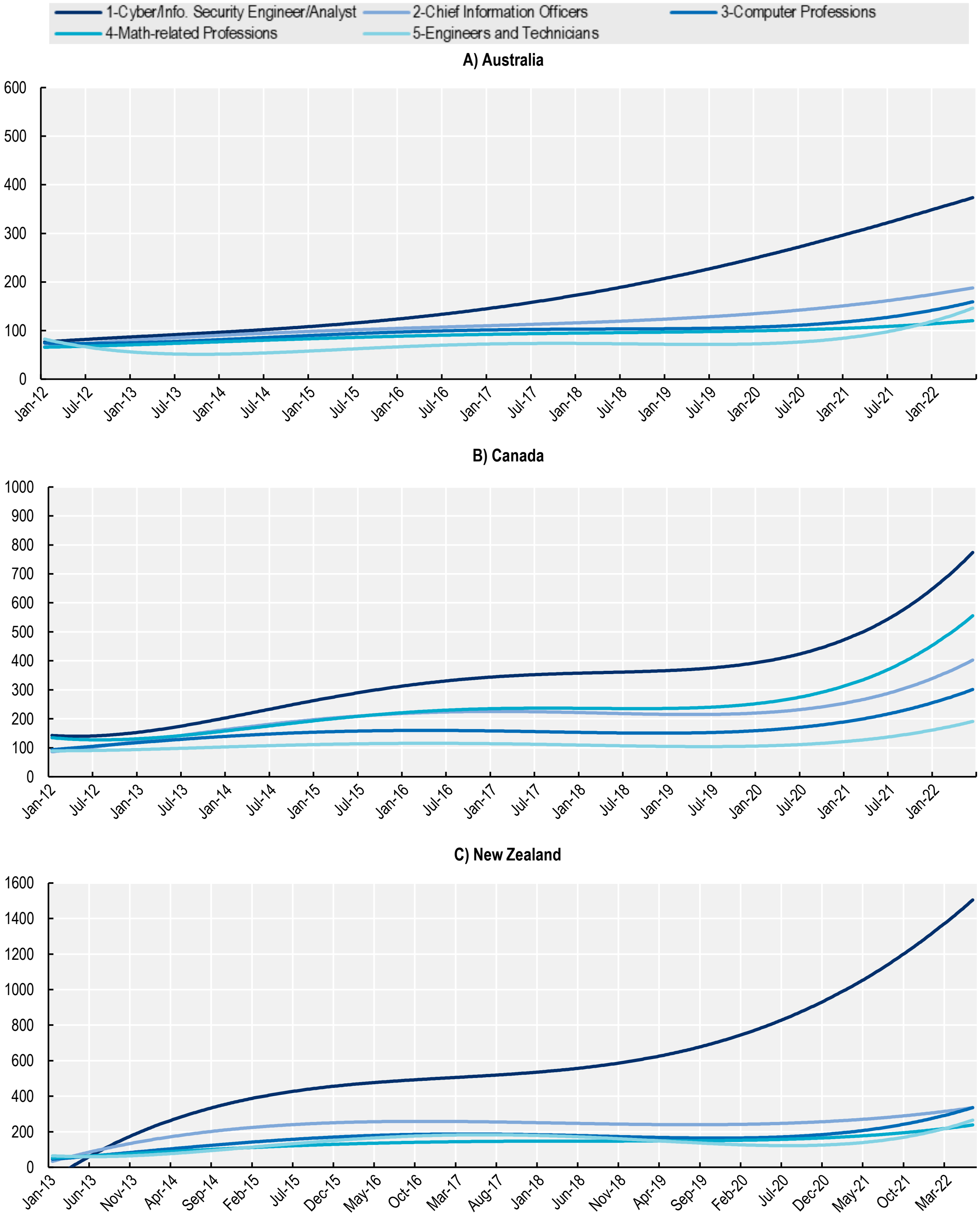
This section analyses more than 40 occupations that are gathered in four occupational groups (Chief Information Officers, Computer-based professions, Math-related professions and Engineers and technicians) to compare the dynamics in their demand with that for cyber security professionals (for more detail on the occupations selected and groups see Box 2.1 and Annex 2.A). For each country, Figure 2.9 shows the bird-eye view of the trends calculated on the standardised monthly growth of OJPs for each group, comparing them with the evolution of job postings for cyber security professionals.

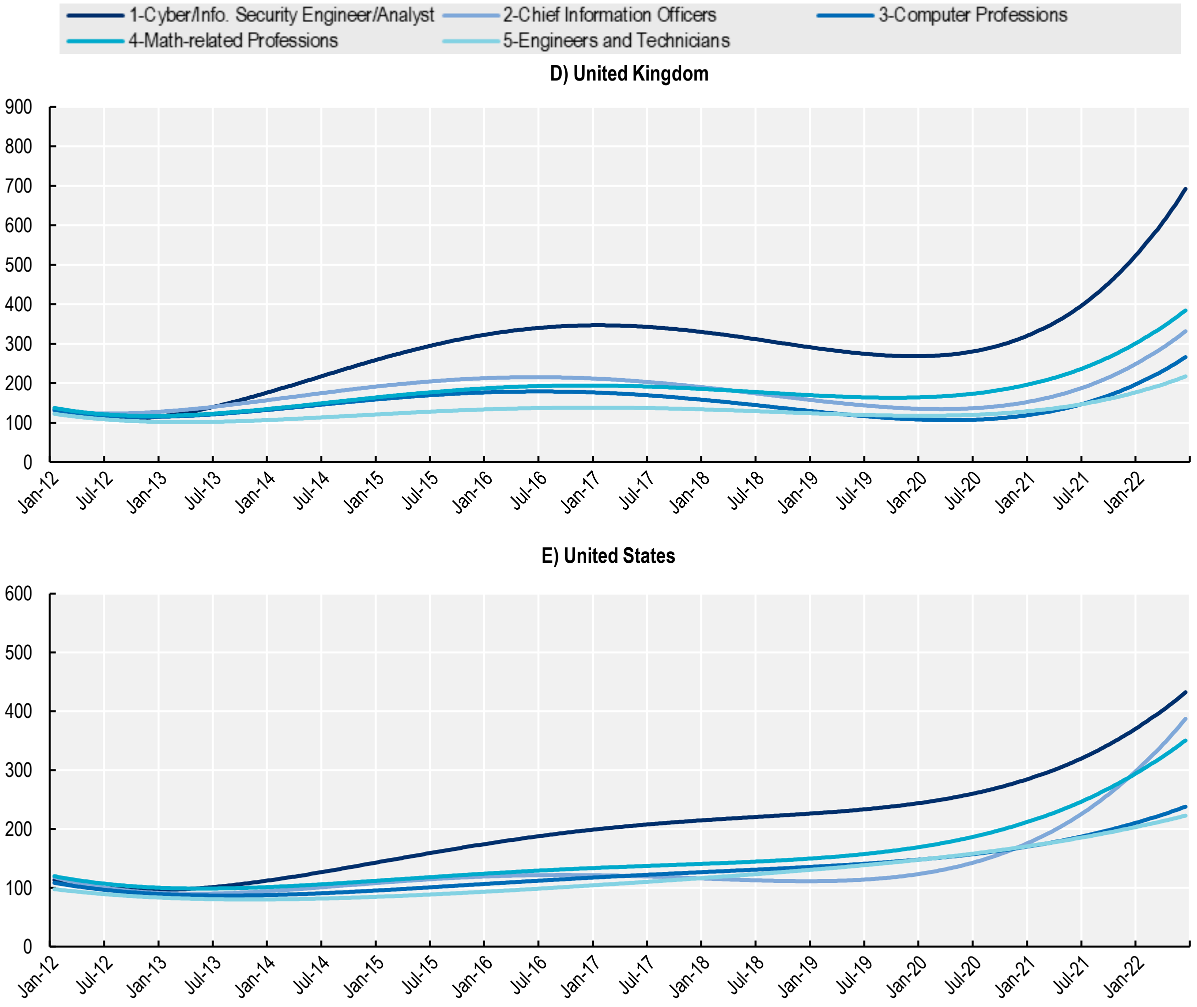
When focusing on the evolution of OJPs trends, results in Figure 2.9 show that the demands for cyber security and that for digital professionals move closely together in Canada, the United Kingdom and the United States. The average correlation index between the growth in cyber security occupations and digital occupations is strong: +0.63 for the United Kingdom, +0.68 for Canada and +0.8 for the United States. While demand for digital, engineering and math professionals has grown very strongly in all countries (OECD, 2022[5]), results in Figure 2.9 reveal that, in the five countries analysed in this report, the demand for cyber security professionals has been growing at a significantly faster pace than that for other digital-related[5] occupations.

The size of the gap between cyber security and other digital, engineering and math- professionals, however, varies significantly among countries. In Australia and New Zealand, for instance, demand for cyber security professionals significantly exceeded that of the rest of occupations considered throughout the period between January 2012 and June 2022. In Australia, the volume of job postings for cyber security professionals over the total of digital/engineering and math occupations has tripled between 2012 and 2021, going from 1.3% to approximately 3%. Among the possible explanations behind this significantly faster growth in the demand for cyber security professionals in Australia and New Zealand is the relative smaller volume of OJPs for this profession in 2012 compared to those from other countries (see Figure 2.1).[6] As the demand for cyber security in Australia and New Zealand catches up to the levels of other major OECD economies, it experience faster growth rates when transitioning to become more mature markets for cyber security professionals.

Figure 2.9. Growth in online job postings: Cyber security and other digital, engineering and math-related professions

Polynomial trends calculated on a standardised index (Jan-12 = 100) for the monthly count of job postings





D) United Kingdom

E) United States

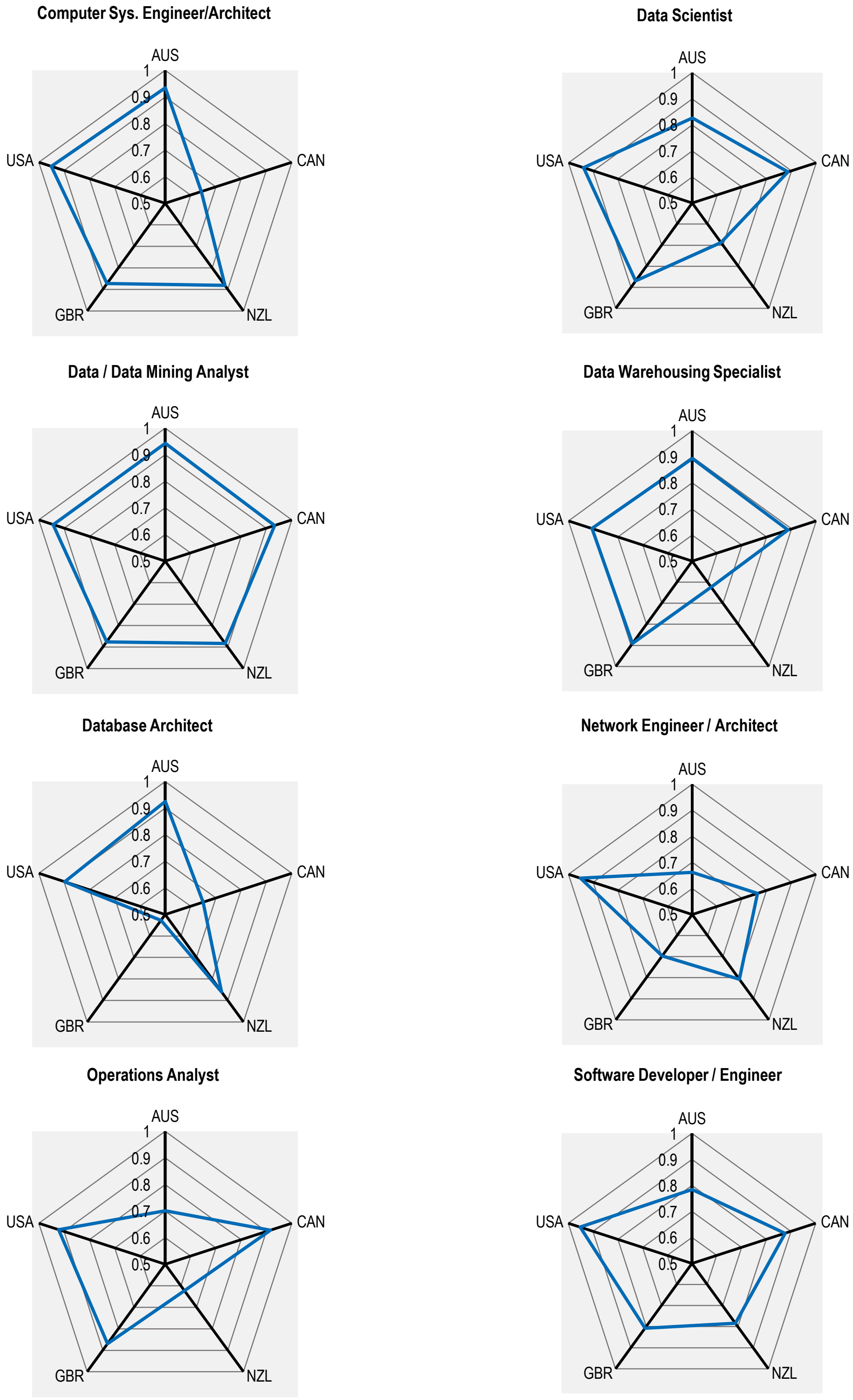
Note: The standardised index shows the evolution in the demand for a given profession in comparison the month of reference. Data for New Zealand starts in January 2013.
Source: OECD calculations based on Lightcast data.

As mentioned above, the digital transition is pushing firms to adopt new digital technologies and workers to use digital tools and devices in virtually all productive sectors. The increase in the demand for a broad range of digital professionals, stemming from the adoption of a variety of new digital technologies, is behind the contextual growth in the demand for cyber security experts as well, as these latter represent the barrier protecting the work of other digital professionals from vulnerabilities of all sorts. The information contained in online job postings allows to investigate what occupations are more tightly linked to the demand for cyber security professionals across the countries analysed.

Figure 2.10 presents, for each country, the correlation indices between the growth in the demand for cyber security professionals and the growth in demand for selected professions in the digital, engineering and math related occupations group. Results suggest that the demand for several digital occupations is tightly linked with the demand of cyber security workers (see Figure 2.11 which reports the full ranking of correlations for each country[7]). Nonetheless, the degree of association between demand for cyber security professionals and demand for other digital professionals can vary across countries. The growth in the demand cyber security professionals, for instance, is strongly linked with that for data/data mining analysts, computer systems engineers/architects and data warehousing specialists (average correlation across countries is 0.92, 0.85 and 0.81 respectively, in the period in January 2012 to June 2022).

Figure 2.10. Correlation between cyber security and selected professions

Correlation indices per country calculated on a monthly standardised index (Jan-12 = 100).



Computer Sys. Engineer/Architect

Data Scientist

Data / Data Mining Analyst

Data Warehousing Specialist

Database Architect

Network Engineer / Architect

Operations Analyst

Software Developer / Engineer

Note: The professions in this chart have been selected as they typically show the highest correlation indices with the cyber security profession across the countries considered. Wider blue pentagons indicate a tight link between the growth in the demand for cyber security and the growth in the occupation at hand over time and across countries. Data for NZL starts on January 2013.

Source: OECD calculations based on Lightcast data.

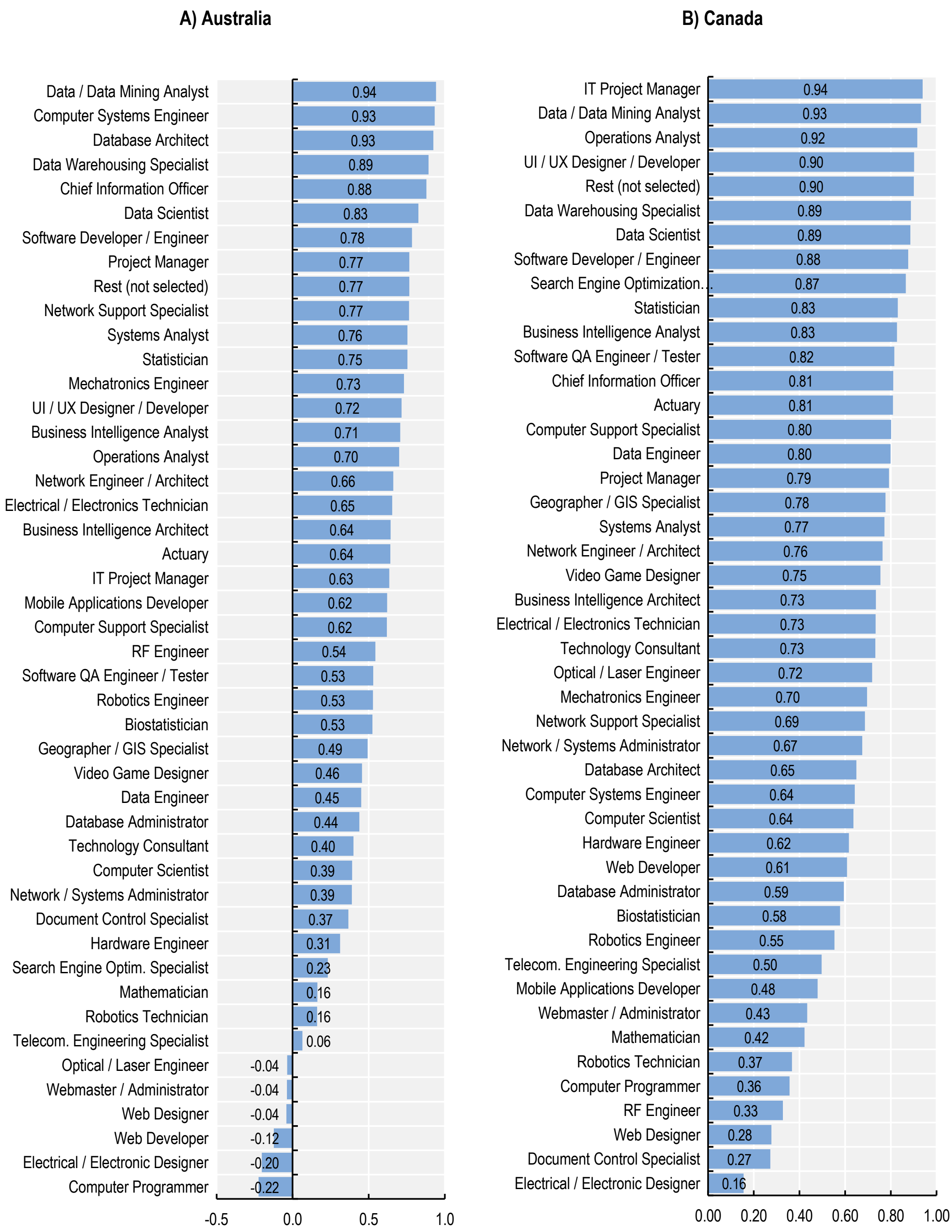
The correlation between the demand for cyber security professionals and data analysts, data mining analysts or computer systems engineers/architects does not come as a surprise. Data analysts,[8] for instance, are in charge of collecting and analysing data from a variety of sources, rely on computer systems, such as database management or user interface software. As firms increasingly digitise their businesses, relying on a wider number of data analysts, they also face increasing vulnerabilities and potential cyber attacks. Digitisation of services and processes within firms, inevitably lead to increasing pressures to protect sensitive information and cyber security protocols and systems play a key role in protecting confidential information stored in digital systems from existing or potential threats.

Similarly, computer system engineers/architects design and develop integrated computer systems to solve application problems, system administration issues or network concerns (O*NET, 2022[21]). Professionals in this occupation are likely to be frequently interacting with cyber security professionals, such as security architects or penetration testers since these professionals are in charge of assessing networks' security robustness and implement security policies and technology to protect files and infrastructures.

Results for the United States indicate a strong correlation of cyber security and most of the digital, engineering and math related professions. However, two professions, software developers/engineers and networks engineers/architects, stand out as those with the highest correlation with cyber security in this country. The functions performed by these roles are closely intertwined with that from computer system engineers/architects.

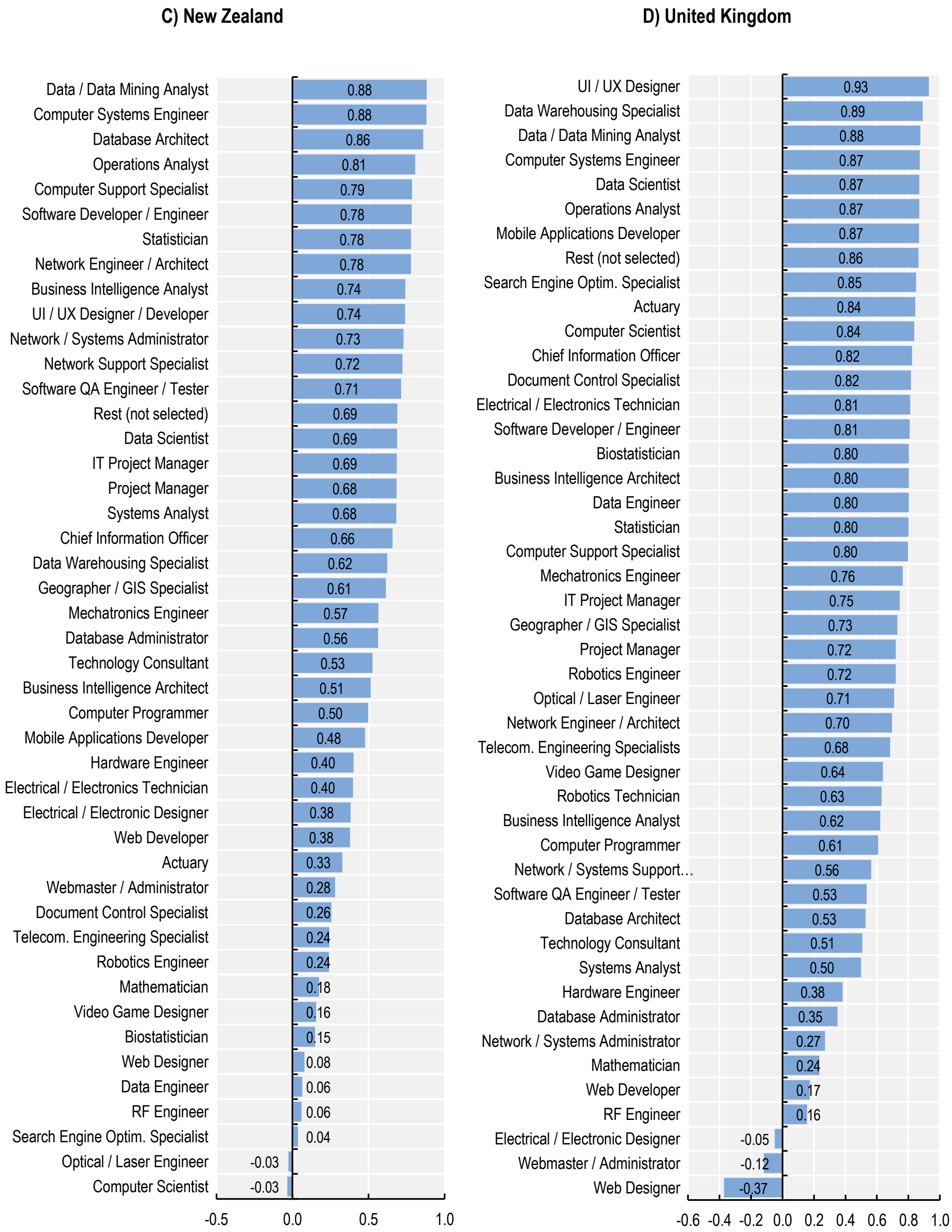
At the other side of the spectrum, Figure 2.11 shows that web designers, webmaster/administrators and electrical/electronic designers are the professionals with the lowest correlation coefficients in the five countries, with an average correlation of -0.05, 0.11 and 0.21, respectively. Those occupations are not closely related to the data and systems management and only marginally interacting with cyber security professionals.

Figure 2.11. Correlation: Cyber security and other digital, engineering and math-related professions



A) Australia

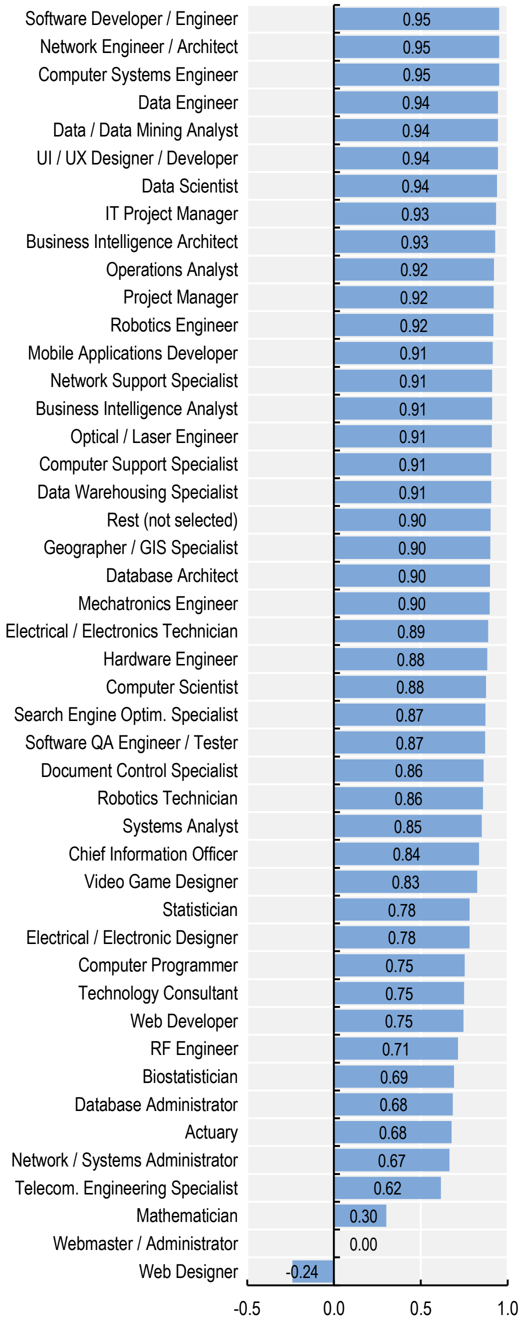
B) Canada



C) New Zealand

D) United Kingdom

E) United States



Note: Correlation indices calculated on the monthly standardised index Jan-12=100. Data for NZL starts on January 2013. Larger bars indicate stronger correlations, signalling a tight link between the growth in the demand for cyber security and that for the occupation at hand over time.
Source: OECD calculations based on Lightcast data.

Zoom in: What are the job roles in high demand within the cyber security landscape?

The previous section provided a detailed analysis of the evolution of the demand for the occupational category "Cyber / Information Security Engineer / Analyst" (Lightcast code 15 1122.00). Within this category, however, different roles can be identified for workers carrying out a variety of tasks. Cyber security professionals (broadly defined) can be involved in different activities ranging from analysing cyber threats or auditing cyber security infrastructures in firms, to managing the teams in charge of protecting IT systems.[9]

The wealth of information contained in job postings can offer a very detailed overview of the different roles demanded by enterprises in the cyber security space and tracking the evolution of their demand (see Box 2.1 and Annex 2.A). Figure 2.12 presents the trends and shares in the demand of four groups of cyber security roles: analysts, architects and engineers, auditors and advisors, managers.

Detailed analysis of OJPs carried out at the "job-role" disaggregation level shows that architects and engineers are among the roles with the fastest growth in the last decade, driving the growth for cyber security positions in Canada and the United States (see Figure 2.12, Panel A).

Cyber security architects ensure that business security needs are adequately addressed on enterprises' architecture, which implies the design and modelling of security solutions (NICCS, 2022[22]). Engineers, instead, while working closely with architects, focus more on the processes necessary for the implementation of security solutions and their integration with other IT products (Joint Task Force Transformation Initiative, 2018[23]). Figure 2.12 (Panel B) confirms that cyber security architects and engineers stand at the core of the cyber security demand with, on average, 37% of OJPs looking for this role across the countries analysed in this report. Canada is the only exception to this result, where the demand for Cyber security Architects and Engineers is still relatively more modest compared to that for other cyber security roles.

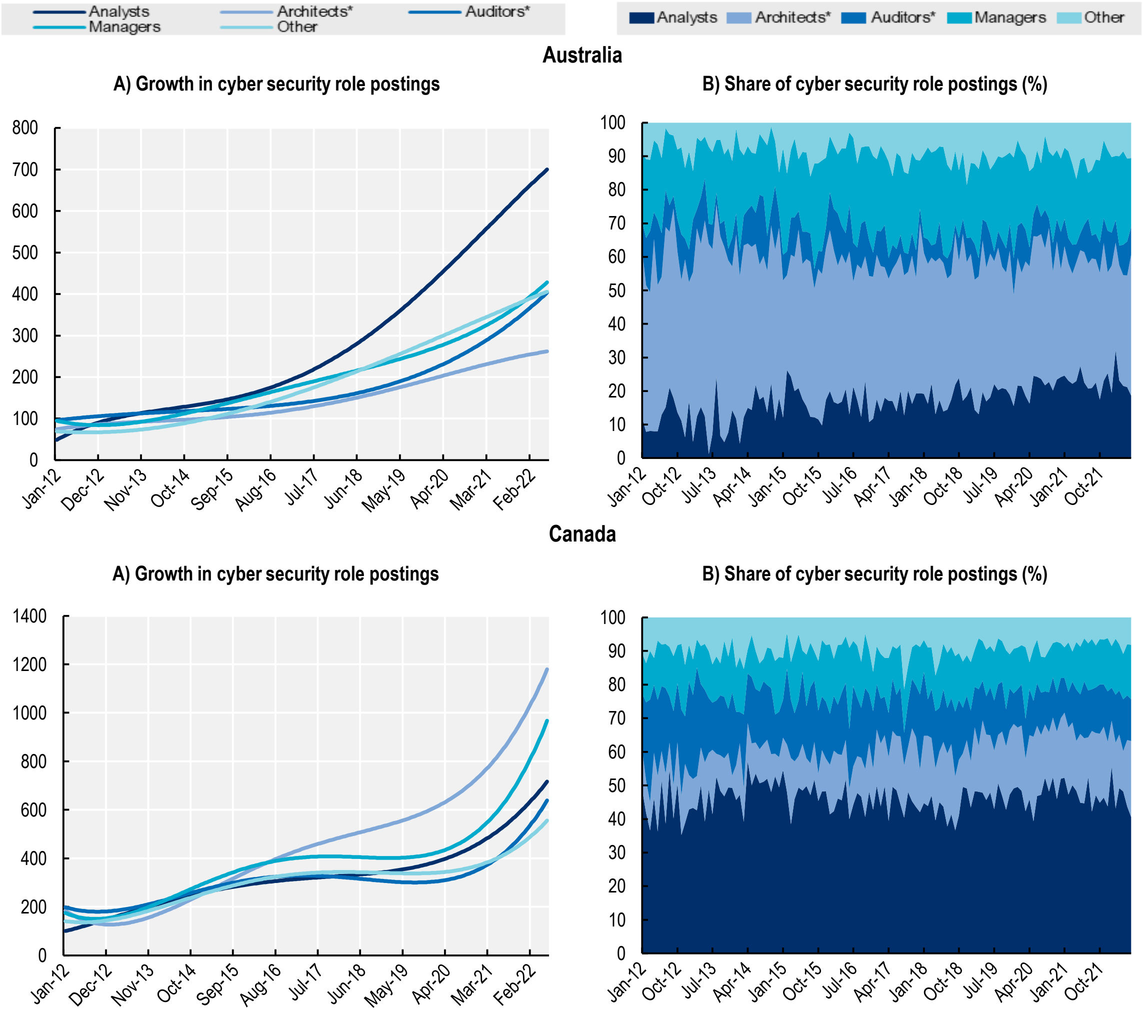
Cyber security analysts are the second most in-demand cyber security role in many countries, accounting for, on average, 26% of the total job postings for cyber security in the five countries selected. Cyber security analysts are commonly in charge of getting insights from multiple data/information sources, supporting the planning, operations and maintenance of systems security (NICCS, 2022[22]). This group of professionals is particularly important in Canada and the United States where it represents, on average, 40% of the job postings advertised in the last decade in the cyber security space. It is interesting to note that the demand for this group of cyber security workers is growing faster than that of most of the other groups in Australia and New Zealand.

Cyber security managers are the third most important role within the cyber security labour market, with 17% of the total posts in the cyber security landscape of the countries analysed. Cyber security managers include those positions involved in decision-making of the cyber security team structure as cyber security managers are tasked to optimise resource allocation, ensure compliance with internal and public regulations and mitigate risks in the networks (Tulane University, 2022[24]). Although managers, being atypical roles, have usually fewer job postings relative to analysts or technicians, it is interesting to notice that this group is the second most important in Australia and New Zealand, even above Analysts. Besides, data shows that this is one of the top-growing roles in Australia, Canada and the United States. This increasing trend is in line with a recent report on the state of the cyber security profession (ISACA, 2022[25])[10] that shows that senior managers and executive or chief information security officers (CISO) are the vacancies with the largest increase between 2018 and 2022.

Finally, cyber security auditors and advisors include professionals devoted to providing external or internal advice about the efficiency and compliance of security solutions. In most of the countries analysed in this report, this group shows a lower share of job postings and the slowest growth relative to other cyber security professionals.

Figure 2.12. Cyber security roles: Trends and shares

Polynomial trends calculated on a standardised index (Jan-12 = 100) for the monthly count of job postings



Australia

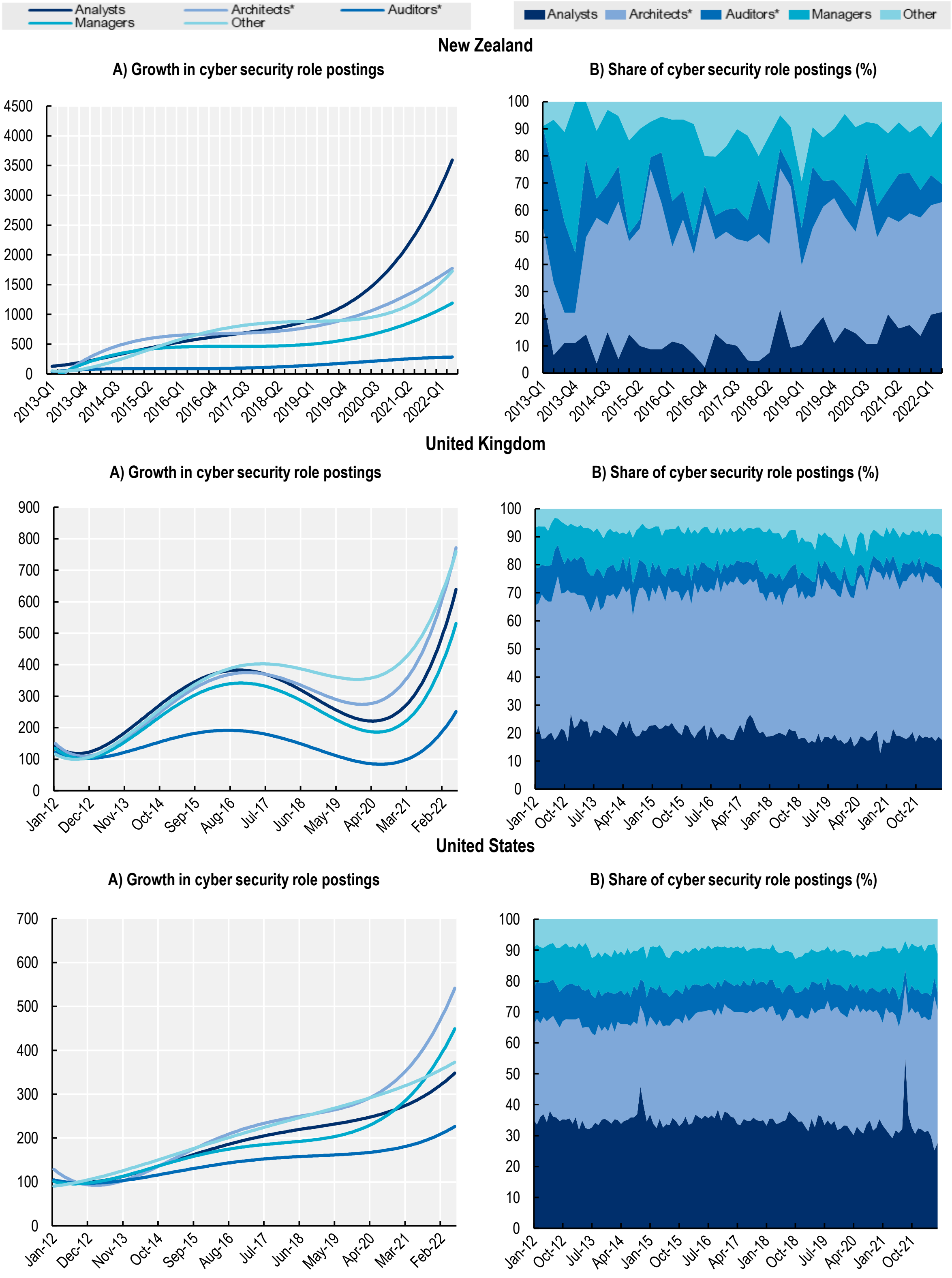
A) Growth in cyber security role postings

B) Share of cyber security role postings (%)

Canada

A) Growth in cyber security role postings

B) Share of cyber security role postings (%)


New Zealand

A) Growth in cyber security role postings

B) Share of cyber security role postings (%)

United Kingdom

A) Growth in cyber security role postings

B) Share of cyber security role postings (%)

United States

A) Growth in cyber security role postings

B) Share of cyber security role postings (%)

Note: For Panel A, the standardised index shows the evolution in the demand for a given profession in comparison the month of reference. Data for NZL uses quarterly instead of monthly information due to few or no observations available for all roles considered. *Architects and engineers, Auditors and advisors.

Source: OECD calculations based on Lightcast data.

The professional profile in cyber security online job postings: What are the characteristics of cyber security demands?

The cyber security sector is facing a significant workforce shortage globally. The (ISC)^2 Cyber security Workforce Study (2021[2]) quantifies this gap in nearly 2.7 million professionals around the world. Another recent report indicates that almost two-thirds of the organisations surveyed have unfilled cyber security vacancies, and for most of them filling those jobs takes on average more than three months (ISACA, 2022[25]). Similarly, a survey interviewing IT decision-makers in more than 30 countries on their perceived cyber security skills gap shows that 60% of the respondents have struggled to fill some positions in the area, mainly in roles related to cloud security and security operations (Fortinet, 2022[26]).

This section explores some of characteristics that define the cyber security professional profile enterprises are looking for in the labour market. The analysis of these requirements in OJPs can shed lights on the mismatches between supply and demand that drive the cyber security workforce gap. Specifically, it reviews the qualifications and the minimum experience required by firms in each country to fill cyber security positions. Using a machine learning approach, it recognises the professional and technical skills that are more relevant for the profession, emphasising on the most recent emerging technologies required by enterprises. Finally, this section provide some insights about how earnings offered in the OJPs for cyber security professionals compare with the earnings for other occupations with similar skills demand.

Qualification and experience requirements in cyber security online job postings

Qualifications and work experience are among some of the key aspects that enterprises use to select qualified candidates in the cyber security job market. It is worth noting that this information is not available for significant share of the OJPs considered in this report (see Annex 2.B), nevertheless, the information available can contribute to characterise the cyber security workers' profile by retrieving the typical educational degrees and the years of experience demanded by firms across labour markets over thousands of different job postings.

Figure 2.13 shows two panels by country analysing education and experience required in cyber security OJPs:

- Panel A exhibits the proportion of job postings requiring, as a minimum, a qualification below bachelor's level (that require less than 16 years of total education[11]), bachelor's, master's or PhD degrees.[12]
- Panel B shows the proportion of job postings by ranges of minimum years of experience required.

On average, results indicate that enterprises reporting education and experience requirements typically look for cyber security workers with at least a bachelor's degree (83% of the job postings) and with more than three years of experience (65% of the job postings). In Australia and the United States, for instance, the proportion of job postings requiring at least a bachelor's degree is nearly 85%, while only 11% require a qualification at a level below a bachelor's degree.

The education requirements in cyber security follow similar patterns that in other information technology (IT) roles. For the United States, for instance, Indeed (2022[27]) and the Bureau of Labor Statistics (2022[28]) show that, in areas such as computer science, computer engineering or IT management a bachelor's degree is the minimum requirement for an entry-level position in most IT jobs.[13]

In the case of England, the supply of education and training programmes in cyber security at lower levels of education is still limited, and policies to expand enrolment in this type of programmes have taken off recently. The vast majority of programs focused on cyber security require prior knowledge of ICT or experience in the sector and are often offered at the most advanced levels of education (Level 5-7, equivalent to ISCED 5 – 8) (see Chapter 3). There have been efforts to expand the supply of non-advanced technical short courses in cyber security (e.g. skills bootcamps) in order to meet specific employer requirements. However, many of these initiatives started recently (2020) and are possibly still unknown (Department for Education, 2021[29]). In the last five years, enrolment in ICT programmes, including cyber security, has grown essentially among the youngest students, especially for Level 3 qualifications (ISCED 3), which is expected to affect trends regarding labour force availability in this field.

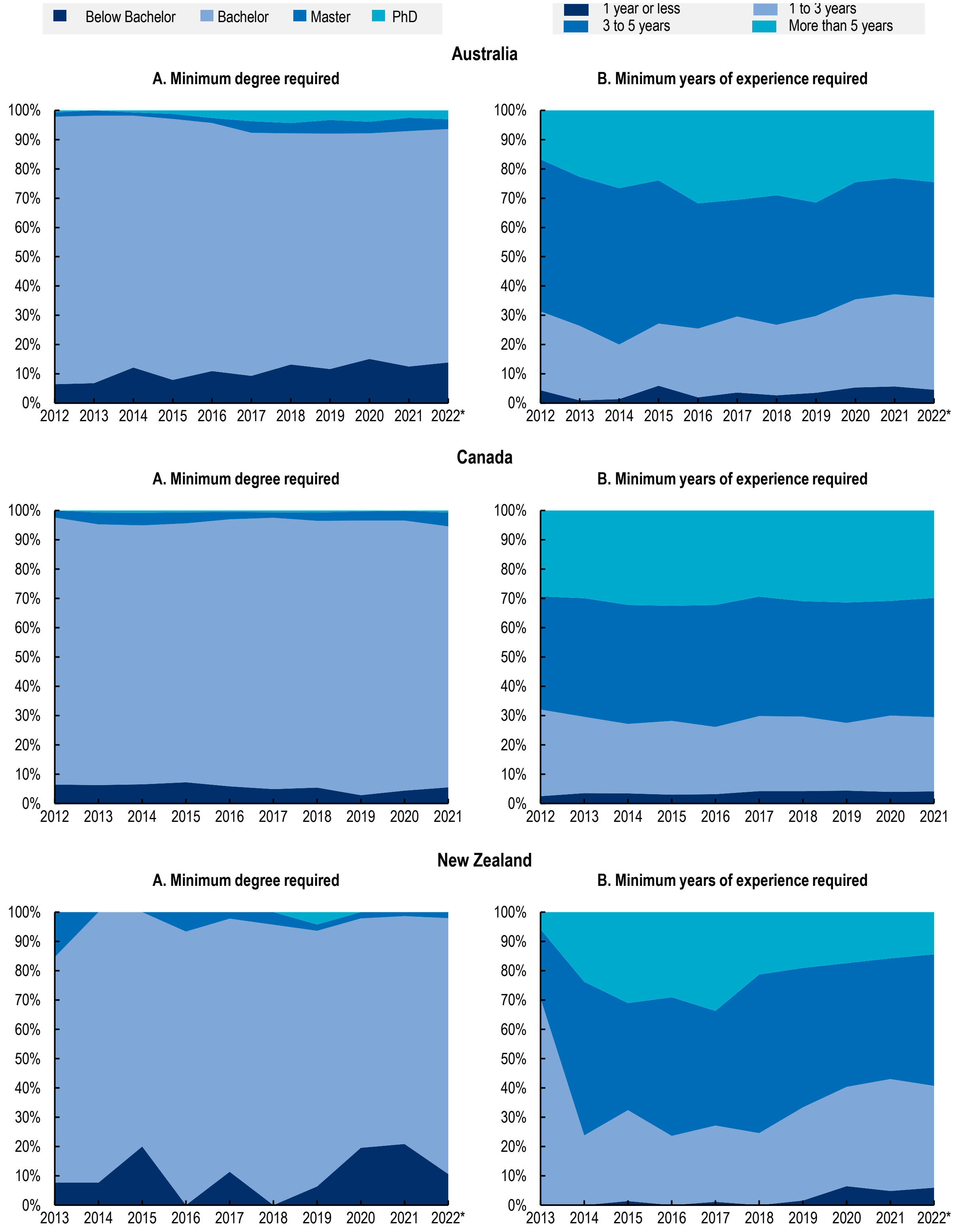
Experience, along with education, is another aspect that employers use to select cyber security professionals. Analyses of online job postings in Figure 2.13 indicate that, on average, 65% of the job postings where information on experience is available, seek professionals with more than three years of experience. In contrast, entry-level positions (with one year or less experience) are not widely demanded across labour markets representing, on average, only 5% of the cyber security job postings. This share goes up to 35% when considering job postings requiring a maximum of three years of experience.

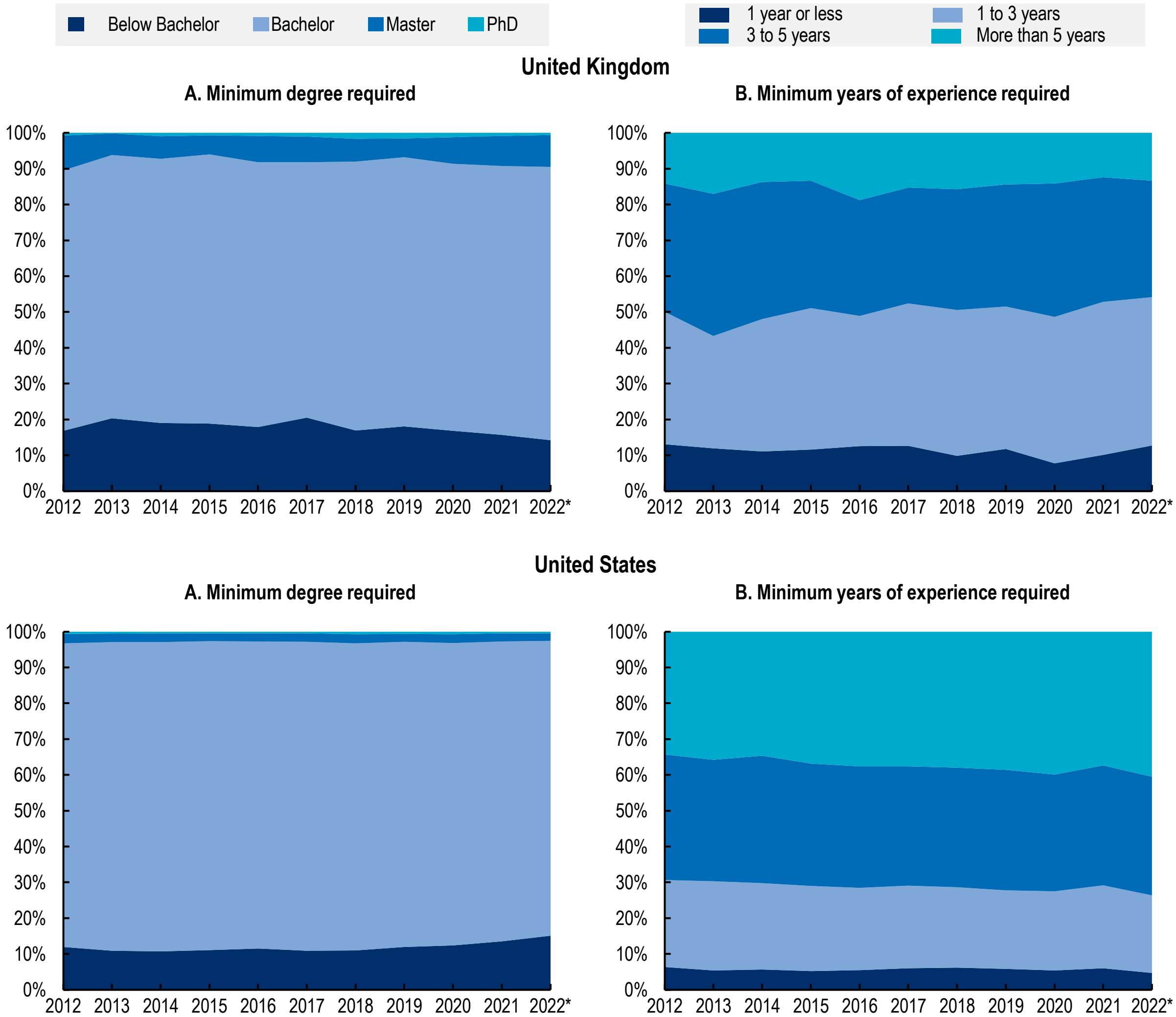
This focus on highly educated and experienced workers is in line with the description of cyber security workers in qualitative analyses based on surveys on cyber security and IT professionals. The (ISC)^2, for instance, describes a cyber security professional as a well-educated worker (86% of the respondents have a bachelor's degree or more) with an average of 7 years of experience in a cyber security role[14] ((ISC)2, 2021[2]). These results suggest that in the cyber security market there may be a small space for young professionals, with little experience or relatively lower education titles. These results are in line with the analyses by ISACA which indicate that only 44% of their survey respondents manage personnel with less than three years of work experience and highlights the potential challenges that the lack of entry-level positions can exert on an ageing workforce (ISACA, 2022[25]).

Lightcast's recent research (2022[30]) found that employers not only seek high levels of education and experience, but also that job openings for entry-level cyber security positions requiring a bachelor's degree exceed the number of bachelor's degrees conferred in cyber security programs in 2021. Additionally, the number of job openings requiring certifications such as CISSP or CISA is higher than the total number of individuals holding those certifications in the entire country. This mismatch creates barriers for new workers entering the field, contributing to the widening shortage of skilled cyber security professionals.

Notably, the demand in the United Kingdom seems to follow a slightly different pattern than in other countries when it comes to the experience required to access a cyber security job. In the United Kingdom, nearly 10% of the yearly job postings in cyber security with available information request one year or less experience, while half of them require three years or less, a share that is significantly larger than in other countries where experience requirements seem to be more exigent.

Figure 2.13. Minimum degree of education and years of experience required in cyber security-related online job postings





Note: For AUS, NZL and GBR, approximately 20% of the data specify education or experience. For CAN and USA, non-missing data is 55% and 70%, respectively. Data for NZL starts on January 2013. * Data until June 2022, except for CAN because of consistency issues.
Source: OECD calculations based on Lightcast data.

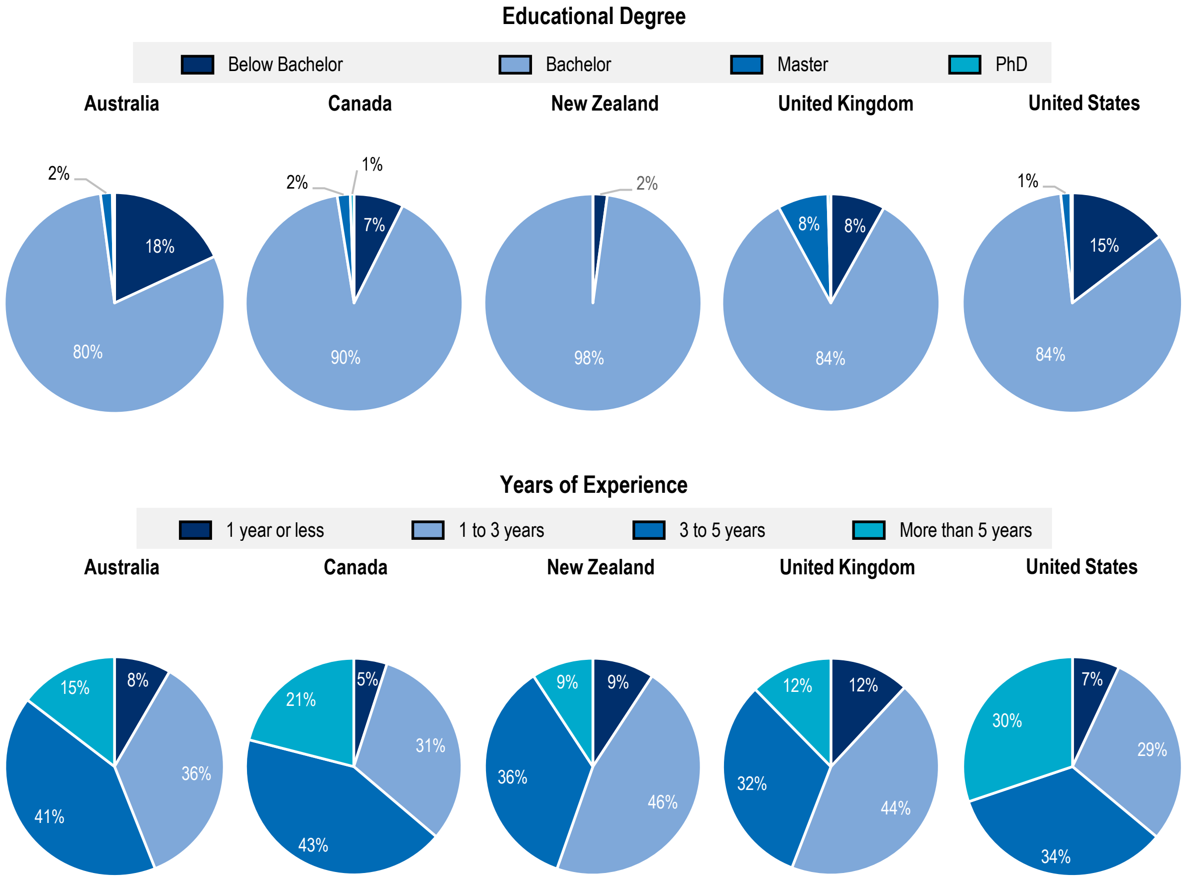
The fewer opportunities for young workers with little experience to enter the cyber security labour market represent an additional challenge to countries wanting to close the global cyber security workforce gap. Boosting the use of apprenticeships or graduate programmes in cyber security can be a tool to reinforce the linkages between youth and the cyber security professions, ensuring that firms and school absorb untapped talent to work transition is smoother for youth seeking a career in cyber security. Chapter 3 zooms in on this topic.

The education and experience required in cyber security may also vary depending on the specific role workers are involved in. Information contained in OJPs allows looking into these requirements and providing insights about key differences and commonalities in a variety of cyber security roles across the countries analysed. However, given the higher occupational granularity and the low data availability (see Annex 2.B), the following analysis captures the average education and experience level required for the period between Jan-2012 – Jun-2022 as a whole to rely on sufficient data points.

Cyber security analysts

Figure 2.14 shows that a typical applicant for a position as cyber security analyst needs a bachelor's degree and, with exception of the United Kingdom, a master's degree or a PhD is hardly required. In contrast, enterprises in countries such as Australia and the United States seek a significant share of workers with qualifications below bachelor's degree (i.e. vocational or skills-based qualifications) but, at the same time, they demand more than three years as a minimum experience (in more than 50% of the OJPs). This result may suggest some flexibility in recruiters from these countries to find analysts with alternative educational degrees but, in turn, those are required to have significant experience in the sector.

Figure 2.14. Analysts: Share of cyber security OJPs per experience and education required



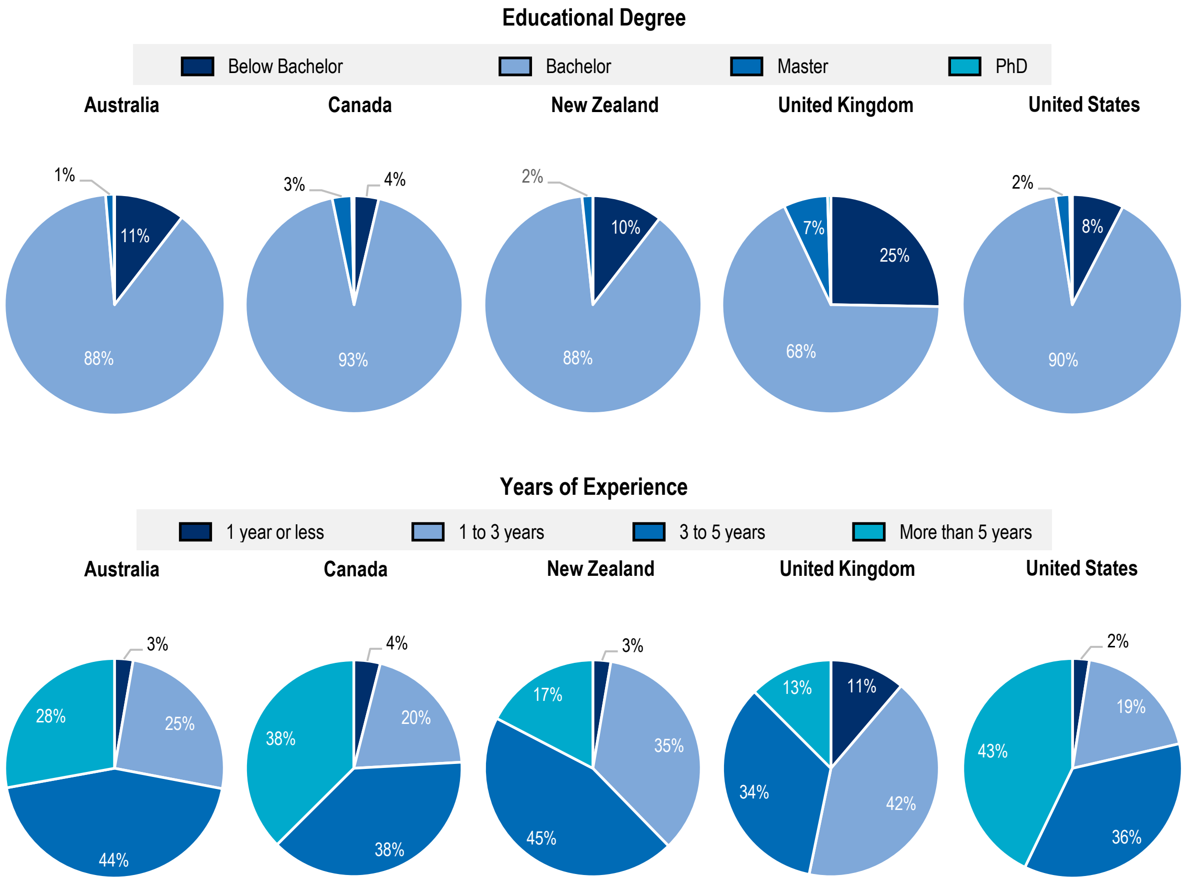
Note: Below bachelor comprehends those degrees awarded with less than 16 years of education.
Source: OECD calculations based on Lightcast data.

Cyber security architects and engineers

Job postings published online for cyber security architects/engineers usually demand candidates to have a bachelor's degree, while higher education titles such as a master's degree or a PhD are not typically required (Figure 2.15). The United Kingdom stands out as an exception to this pattern. Enterprises in the United Kingdom that post vacancies online for cyber security architects and engineers usually demand a higher proportion of workers with qualifications below bachelor's degree for this cyber security role. One of the reasons behind these peculiar results for the United Kingdom may lie in that, in the United Kingdom, there is a relatively broad availability of skill-based certificates in cyber security that require less years than a bachelor's degree and provide the practical and theoretical knowledge in the area (see for example the HNC/HND in cyber security offered by the Scottish Qualifications Authority (2020[31])). Employers in the United Kingdom may be targeting professionals with that kind of education and experience, more than in other countries.

Regarding the years of experience, job postings for cyber security architects/engineers typically look for candidates with more experience than those for cyber security analysts. In all countries selected but the United Kingdom, more than 60% of the job postings require workers with more than three years of experience. Even, in Canada and the United States, nearly 40% of the job postings require five years or more. The demand for professionals with just one year or less of experience is, hence, almost absent. Again, the United Kingdom represents the only exception, with half of the job postings requiring workers with less than 3 years of experience.

Figure 2.15. Architects/engineers: Share of cyber security OJPs per experience and education required



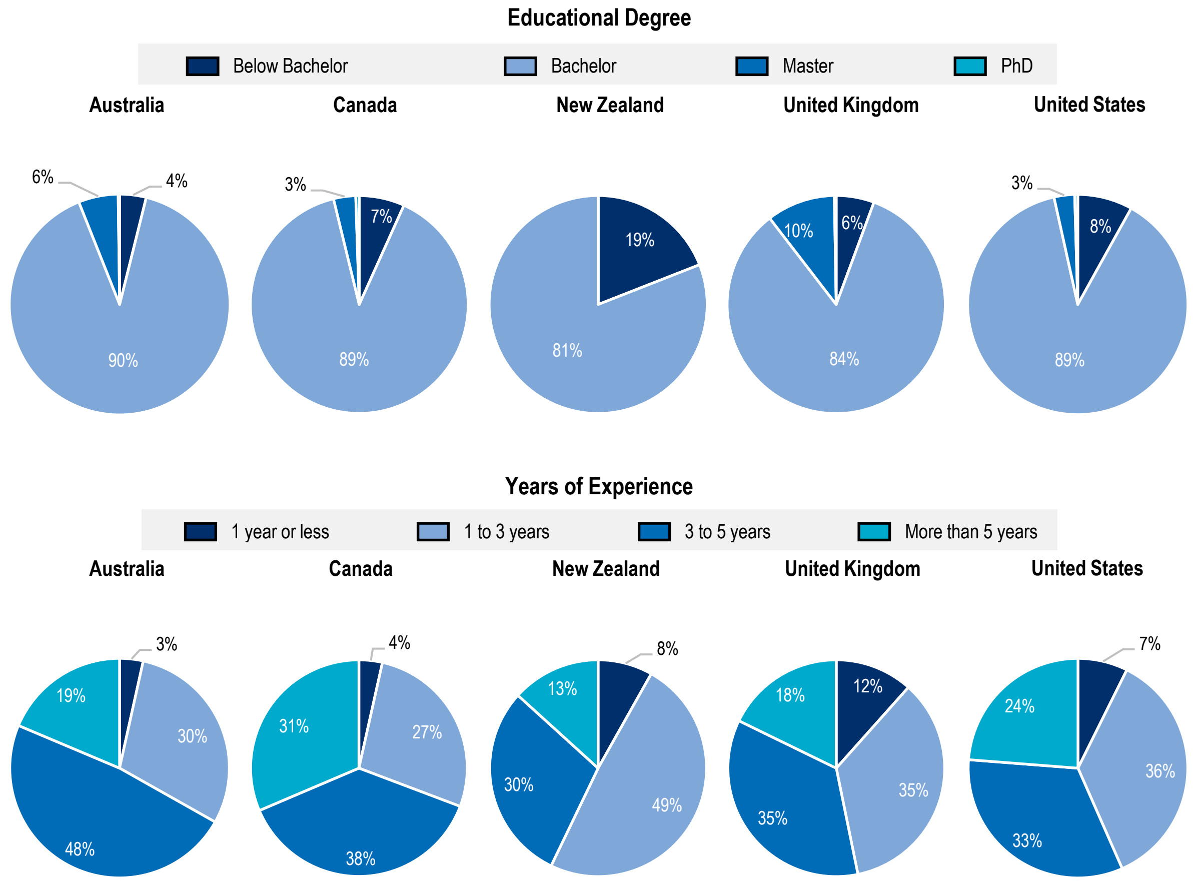
Note: Below bachelor comprehends those degrees awarded with less than 16 years of education.
Source: OECD calculations based on Lightcast data.

Cyber security auditors and advisors

Figure 2.16 shows that the demand for cyber security auditors and advisors commands a relatively larger share of workers with at least a master's degree when compared with analysts and architects/engineers. Since the tasks of these positions require providing audits or advisory of the enterprises' security systems, it is reasonable to find a demand for a more specialised workforce. New Zealand stands out as the only case in which a high demand for workers with qualifications below bachelor's degree remains high. In this case, the demand is mainly for professionals with diplomas, a Level 5 or 6 qualification (among 10 levels) in the New Zealand's education system that certifies theoretical and technical knowledge in specialised fields (New Zealand Qualifications Authority, 2016[32]).

The required years of experience for a cyber security auditor/advisor do not differ significantly from those demanded to cyber security analysts. Most new OJPs for cyber security auditors and advisors look for workers with one to five years of experience while less than 10% look for workers with little or no experience. Notably, in Canada nearly one-third of the job postings require a person with more than five years of experience, while in the United States almost one out of four postings require such extensive level of experience.

Figure 2.16. Auditors/advisors: Share of cyber security OJPs per experience and education required



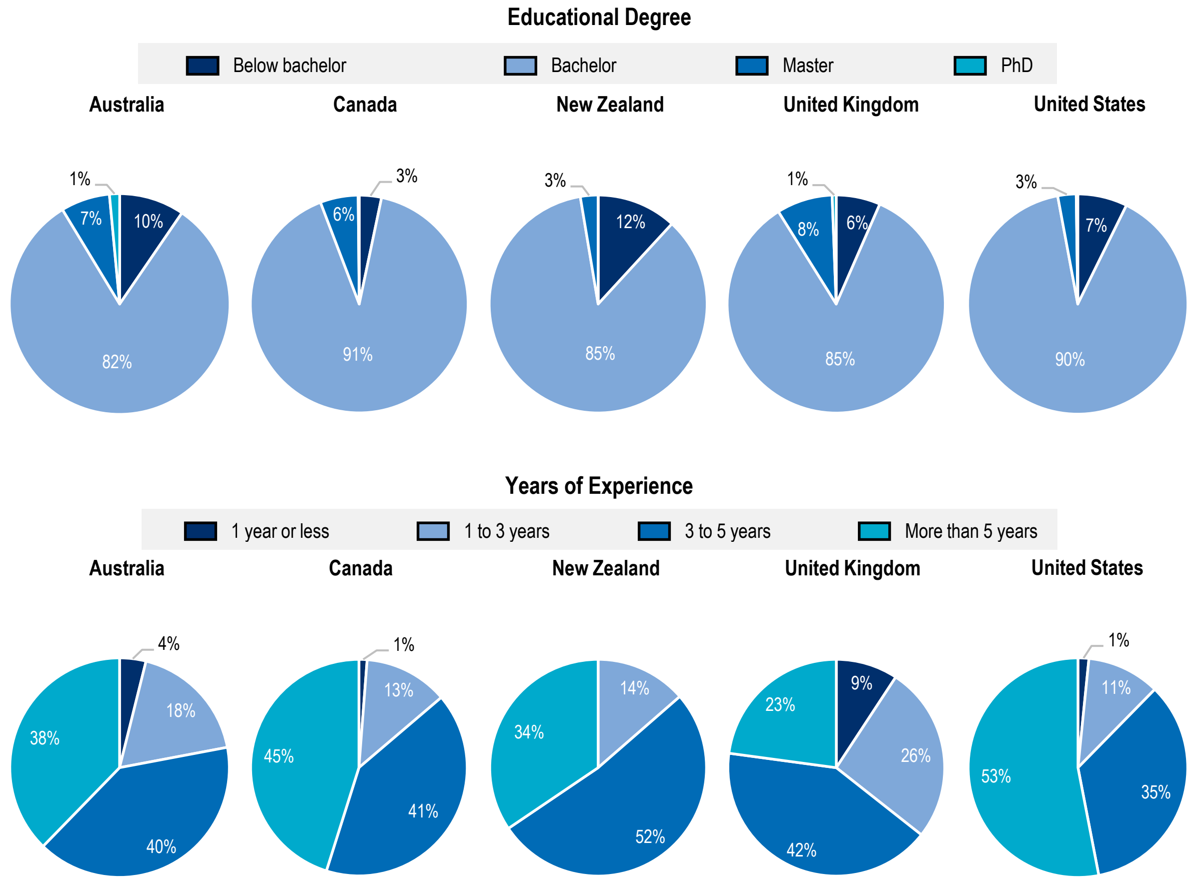
Note: Below bachelor comprehends those degrees awarded with less than 16 years of education.
Source: OECD calculations based on Lightcast data.

Cyber security managers

Finally, in line with the tasks usually associated to this role, the demand for cyber security managers (i.e. leads, managers, directors, etc.) require both more education and experience (Figure 2.17). The proportion of job postings requiring at least a master's degree is similar to the case of cyber security auditors/advisors, but in this case, a small share of job postings in Australia and the United Kingdom requires, as a minimum, also a PhD degree. However, In Australia and New Zealand, the demand for cyber security managers with qualifications below bachelor's degree is larger than in other countries, which suggest a higher emphasis on the experience than on the educational qualifications for some positions. For instance, in Australia, the Certificate IV and the Diploma (Level 4 and 5, respectively, in the Australian Qualifications Framework), are vocational qualifications below a bachelor that are demanded as the minimum required degree in job postings looking for security managers or administrators.

The profile for cyber security managers also requires more experienced applicants. In most of the countries selected, more than 75% of job postings target applicants with more than three years of experience. Even though the United Kingdom follow the same overall trends, the proportion of job postings demanding highly experienced workers is lower (65%). Moreover, a small proportion of job postings in the United Kingdom (9%) require less than one year of experience. This requirement of low experience is present in job adverts for positions as team leads, administrators or managers.

Figure 2.17. Managers: Share of cyber security OJPs per experience and education required



Note: Below bachelor comprehends those degrees awarded with less than 16 years of education.
Source: OECD calculations based on Lightcast data.

The skills bundle of cyber security professionals

The rapid expansion and adoption of new digital technologies is constantly reshaping the skills that enterprises are demanding when hiring new professionals for cyber security roles. Overall, in the cyber security market, professionals blend technical skills (e.g. programming languages, cloud computing or IT infrastructures) with security-strategy skills (e.g. Governance, Risk and Compliance or threat intelligence/modelling) to create security systems that protect businesses against cyber threats while complying with internal and external regulations.

According to the (ISC)^2, the most relevant skills for cyber security professionals include cloud computing security, governance and risk assessment, AI/machine learning and threat intelligence analysis ((ISC)2, 2021[2]). Professional skills, as in other occupations, have reportedly gained importance in the cyber security sector. A report on the state of the cyber security profession indicates that 54% of the managers surveyed report gaps in 'soft' skills among cyber-professionals (ISACA, 2022[25]), signalling the importance that the mix of both technical and professional skills plays in creating a dynamic cyber security workforce.

The analysis in Figure 2.18 leverages machine learning approaches (see Box 2.3) to identify the most relevant technical and professional skills in the employer's demands for cyber security positions collected through OJPs. When focusing on technical skills, the first group of relevant skills encompasses knowledge areas at the profession's core, such as Information Security and Network Security. These are particularly relevant for cyber security professionals in Canada and the United Kingdom.

Information Security and Network Security, along with "Cyber Security" are terms that can sometimes overlap in day-to-day jargon but that are conceptually different (University of San Diego, 2022[33]). Information Security refers to all those different systems and policies designed to protect the confidentiality and privacy of any kind of information (digital or physical). Cyber security, as a subset of Information Security, aims to protect systems, networks and devices connected to the Internet against cyber threats. Meanwhile, Network Security is a subset of cyber security that comprises different measures to protect network infrastructures and data on them.

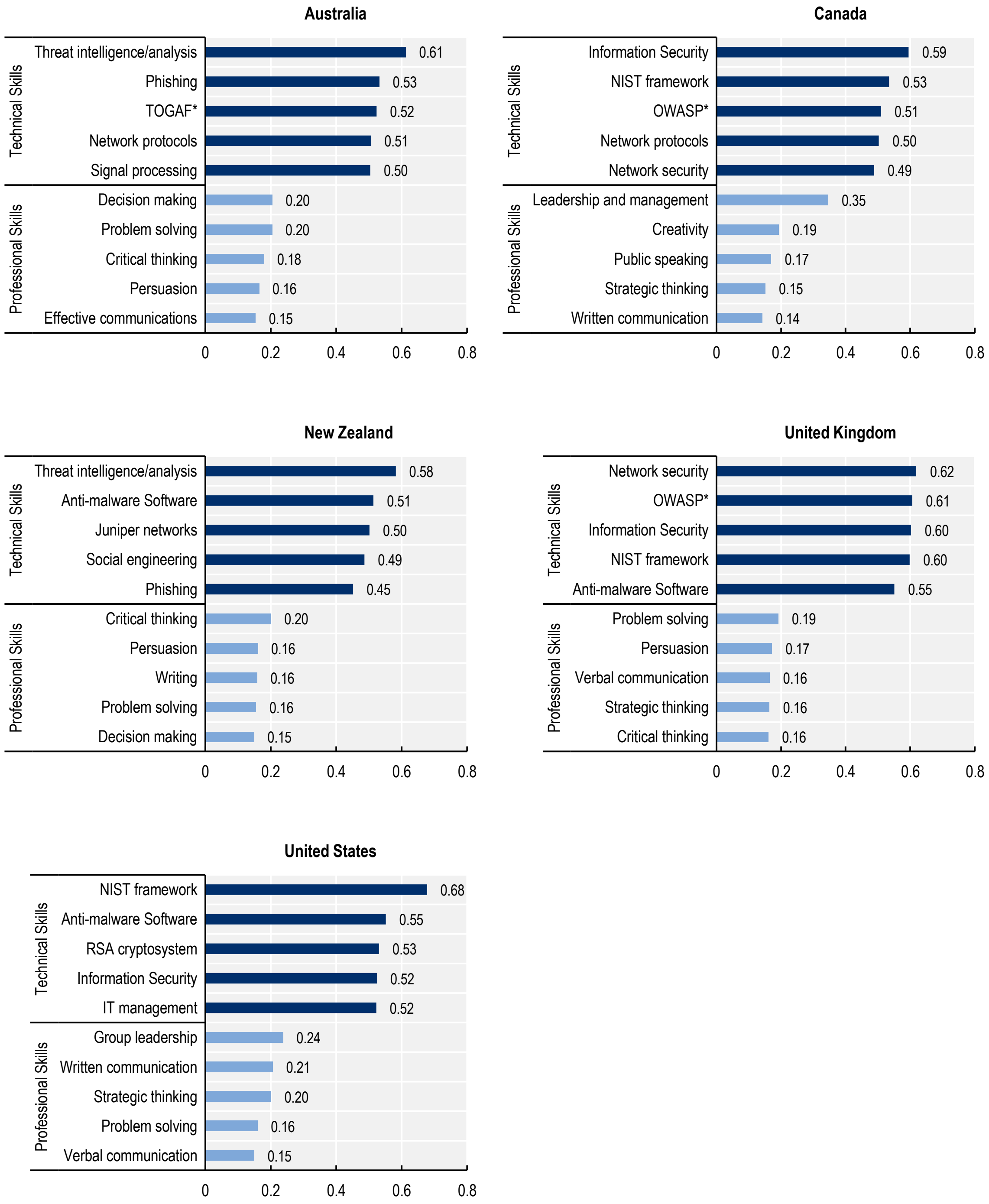
Results in Figure 2.18 also indicate the knowledge of specific frameworks that are highly relevant to the cyber security profession. Amongst those, the Open Group Architecture Framework (TOGAF), the Open Web Application Security Project (OWASP) and the National Institute of Standards and Technology (NIST) Framework.

Specifically, TOGAF is a framework used by enterprises as a standard for designing and implementing Enterprise Architecture[15] (The Open Group, 2022[34]). TOGAF is used in the implementation of security architectures aiming to align security needs and business goals. OWASP is a foundation based on open-community contributors that works to improve web security by offering guidance, standards and open-source tools and technologies to create applications that can be trusted (OWASP, 2022[35]). Finally, the NIST Cybersecurity Framework has been created by the United States Government and industry to provide standards, guidelines and best practices to manage cyber security risks and foster cyber security management communications among stakeholders (NIST, 2022[36]). Other technical skills appearing in the rankings includes technical knowledge on network protocols, anti-malware software and encryption systems (i.e. RSA cryptosystem), but also threat assessment-oriented skills, such as threat intelligence and knowledge of social engineering practices and phishing.

Cyber security is a profession requiring much technical knowledge with its main domain covering the areas of computing systems and IT networks. Along with technical skills, cyber security professionals also need a variety of professional skills to communicate procedures, strategies and to convey technical messages and concepts in ways that other stakeholders within the firm can understand. However, results in Figure 2.18 shows that similarity indices are in most cases below 0.3, suggesting that professional skills are not as relevant as the technical competencies across demands of employers in cyber security roles.

Figure 2.18. Skill bundle demands of cyber security professionals

Skills with the highest relevance for the cyber security profession in 2021 (closer to 1 = more relevant)



Note: The relevance scores are derived from a semantic analysis of the online job postings for each country in 2021. The closer the score to 1, the more relevant the skill for the cyber security occupation in the country at hand. For more details on the methodology see Box 2.3 and Annex 2.A. * In the Figure OWASP refers to Open Web Application Security Project and TOGAF to The Open Group Architecture Framework.
Source: OECD calculations based on Lightcast data.

When considering only the group of professional skills, OJPs mainly demand problem solving, critical thinking and communication skills. In the five countries considered, verbal communication (or public speaking) and/or written communication (or writing) are amongst the most relevant professional skills for the occupation along with effective communication. Problem-solving and strategic/critical thinking skills are also relevant to the profession in most of the countries. As cyber-threats are evolving constantly, professionals in the area constantly need to develop new techniques and approaches to overcome emerging challenges. Problem-solving and critical thinking are at the core of the implementation of technical solutions to cyber-threats. Interestingly, in the United States and Canada, leadership skills are also relevant for the profession. This result is in line with the increase in the demand for cyber security managerial roles after 2020 in both countries (see Figure 2.12), as well as for a relatively higher interest for more experienced professionals. Figure 2.13 shows that, in either countries, 30% or more of the job postings that specify the minimum years of experience request five or more years of experience.

Box 2.3. Using machine learning to assess the relevance of skills in cyber security occupations

Recent advances in machine learning techniques led to the development of so-called language models which have the objective of understanding the complex relationships between words (their semantics) by deriving and interpreting the context those words appear in. Language models (in particular Natural Language Processing- NLP- models) interpret text information by feeding it to machine learning algorithms that derive the logical rules to interpret the semantic context in which words appear. NLP and language models, used in the remainder of this paper, are therefore better suited for the analysis of text information than traditional statistics and, as such, they are used for the analysis of online job postings in the remainder of this report.

In particular, the approach taken in this report leverages 'Word2Vec', an NLP algorithm developed by researchers in Google. This algorithm functions by creating a mapping between the meaning (i.e. the semantics) of words contained in text and mathematical vectors, so-called 'word vectors'. This representation allows the calculation of mathematical and semantic similarity measures between different skills and occupations (see Annex 2.A for more details on the cosine similarity calculations). Following a recent report from the OECD (2022[5]), skills that are more semantically similar to a certain occupation are interpreted in this report as being more 'relevant' to the occupation. Applying this approach is, therefore, possible to assess whether the skill "Excel" is more relevant to the occupation "Economist" or to "Painter", based on the semantic closeness of these words' meanings extrapolated from millions of job postings. This is used, in turn, to generate indicators of the relevance of technical and professional skills for cyber security professionals based on the language/semantic analysis of the text contained in the OJPs in each country considered.

Recent OECD work (2022[5]) validated the assumption by which semantic similarity scores derived from word embeddings can be used as a measure of skills relevance for each occupation. In particular, the report compares the results of the similarity scores with expert constructed scores available in the O*NET database. It shows that correlation between similarity scores and the O*NET values is positive, strong (0.62) and statistically significant across all possible combinations of occupations and skills.

New and emerging technology demands in the cyber security world

The dynamic nature of the digital world, to which the cyber security profession belongs to, implies that technological demands evolve constantly. New technologies emerge, requiring expertise to operate them. The information in OJPs allows to track the emergence of these new technologies in a timely manner and to identify recent trends. Results in Figure 2.19 present the top-10 emerging cyber security technologies. New and emerging cyber-related technologies are identified by computing the ratio between the skill mentions in the period 2019-22 and those in the period 2012-18 across OJPs for cyber security professionals.[16]

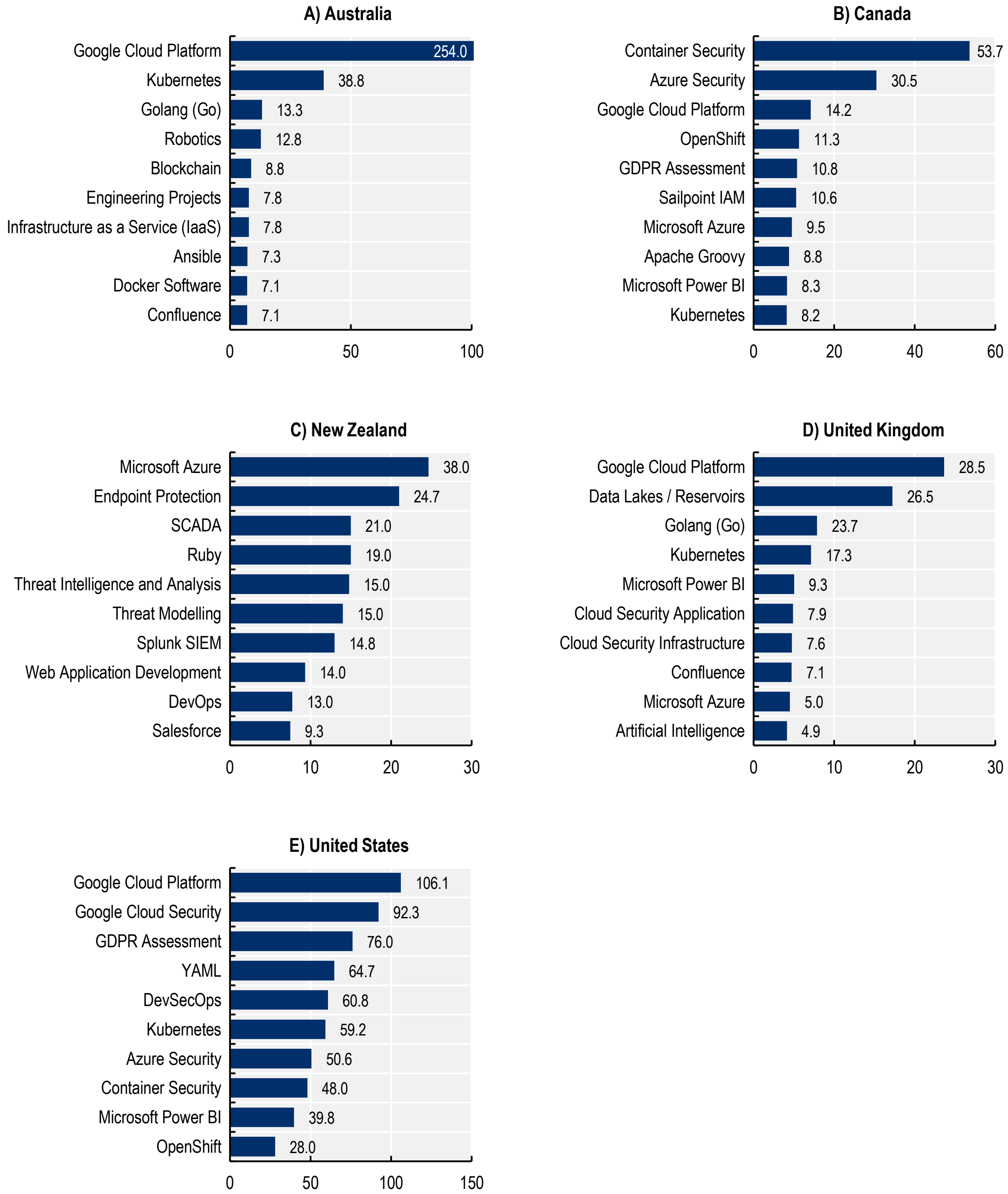
In line with the findings of the (ISC)^2, all countries show new and emerging cyber-related skills in the area of programming languages and cloud computing services. Programming languages such as GO, Ruby and YAML have significantly increased their popularity (number of mentions in OJPs) among the cyber security job postings. Microsoft Azure and Google Cloud Platform are other technologies that have gained relevance in the last years in the cyber-landscape. The ability to operate these platforms is the fastest growing skill in virtually all countries with the exception of Canada, where it is among the top-3 skills.

Virtualisation solutions, such as Kubernetes or Docker, show an important increase in their demand across different countries. Specifically, container infrastructure and security skills (i.e. Docker, Kubernetes or container security) stand out as some of the newly emerging technologies demanded to cyber security professionals in the countries analysed. These ‘technical solutions’ have increased their popularity in the last years due to their advantages for application development and deployment in terms of reducing system resources and simplifying portability. Nevertheless, since these containers include all the components necessary to run an application (i.e. code, libraries, system tools, etc.) cyber threats can compromise seriously business operations.

In the United States and Canada, the General Data Protection Regulation (GDPR) framework, implemented by the European Union in May 2018, is a framework for which demand has spread out significantly in the cyber-profession. This is not only true in EU countries, but also in those covered in this chapter, as many of the firms operating outside the EU are still subject to comply with the GDPR (GDPR EU, 2022[37]).

Figure 2.19. Growth in cyber security skills demand

Ratio between the skill mentions in the period 2019-22 compared to the period 2012-18 in cyber security job postings (code: 15-1122.00)



Note: This figure considers those skills or technologies with mentions in OJPs that are above the average observed in the 2019-22 period. Thus, skills/technologies showing a fast growth but a low number of mentions in the most recent period are excluded.
Source: OECD calculations based on Lightcast data.

The earnings of cyber security professionals

As pointed out before in this chapter, the global cyber security job market faces an increasing demand for professionals and reported skill shortages. This trend is likely to remain during the next years as the adoption of cyber security technologies is expected to grow strongly. In 2020, the World Economic Forum surveyed enterprises with more than 100 employees about the future of work and, specifically, about the probability of different economic sectors to adopt new technologies by 2025. Among these technologies, encryption and cyber security emerged as one of those with higher probability of adoption with 13 out of 14 economic sectors recording probabilities higher than 70% (World Economic Forum, 2020[38]).

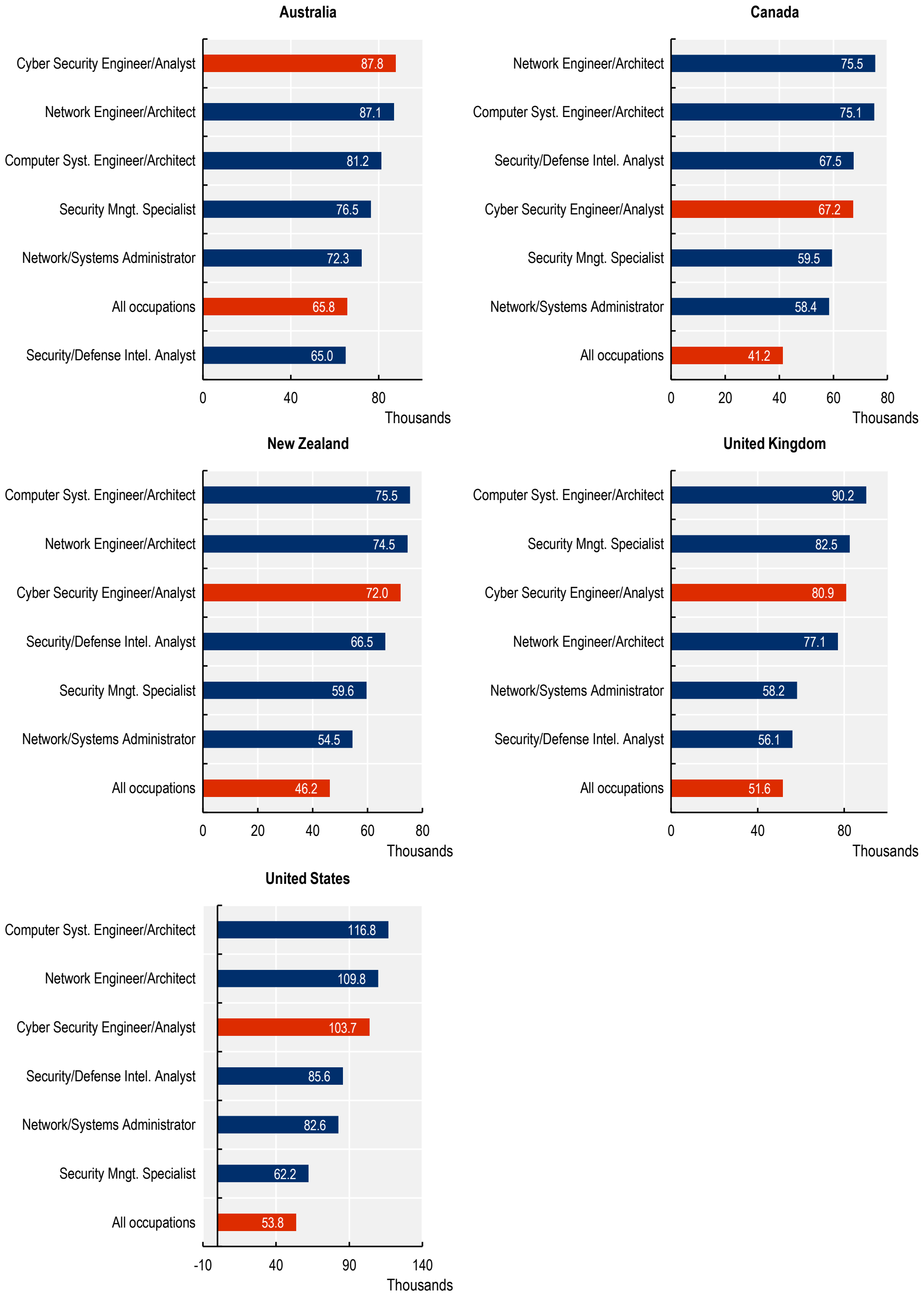
As the demand increases, wages in the sector are expected to remain high, reflecting the shortage of professionals to fill current and, possibly, future vacancies. Notably, in the United Kingdom, nominal wages advertised in cyber security OJPs between in 2021 and 2022 have increased on average 5% while average salaries posted in OJP for the rest of occupations have remained stable, signalling potential shortages in cyber security workforce.

Using the information on salaries offered in the job postings, Figure 2.20 compare the average wage advertised in 2021 for cyber security professionals with that for other digital professions that are in the skills-neighbourhood of cyber security professionals (See Annex 2.A) and that require similar skills. Results shown in this section should be taken carefully since the availability of OJPs specifying wages is limited (see Annex 2.B). To favour comparability, these values are shown in United States dollars (USD) adjusted for purchasing power parity (PPP).

In line with the strong demand for digital professionals (OECD, 2022[5]), Figure 2.20 shows that salaries offered in all the digital professions selected are generally above the average offered salary in each country.[17] Interestingly, cyber security professionals rank usually in the third place, after network engineers/architects and computer system engineers/architects. The difference in wages among these three professions is however small, in most of the countries less than USD 10 000. In contrast, the wage premium is higher when the cyber security profession is compared with professions such as security/defence intelligence analyst and network/systems administrator. In these cases, wages offered to cyber security professionals are typically higher by more than USD 15 000.

Figure 2.20. Annual wage per country and profession (current USD PPP)

Average annual wage offered in OJPs in 2021 for selected professions with similar skills demand



Note: Professions selected are those more similar to the cyber security profession in term of the relevance of skills demanded in OJPs, according to the Semantic Skill Bundle Matrix (see Annex 2.A). Values in local current units were transformed to USD using purchasing power parity (PPP) rates.

Source: OECD calculations based on Lightcast data. OECD Purchasing power parities indicator: OECD (2022[39]), Purchasing power parities (PPP), https://doi.org/10.1787/1290ee5a-en.

References

(ISC)2 (2021), *Cybersecurity Workforce Study 2021. A Resilient Cybersecurity Profession Charts the Path Forward*, https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. [2]

Australian Bureau of Statistics (2022), *Australian Statistical Geography Standard (ASGS) Edition 3*, https://www.abs.gov.au/statistics/standards/australian-statistical-geography-standard-asgs-edition-3/jul2021-jun2026/main-structure-and-greater-capital-city-statistical-areas/statistical-area-level-4#:~:text=Statistical%20Area%20Level%204%20(SA4s,Census%2. [19]

Australian Bureau of Statistics (Jul2021-Jun2026), *Digital boundary files*, https://www.abs.gov.au/statistics/standards/australian-statistical-geography-standard-asgs-edition-3/jul2021-jun2026/access-and-downloads/digital-boundary-files. [13]

Australian Cyber Security Growth Network (2020), *Australia's cyber Security Sector Competitiveness Plan*. [10]

Bureau of Labor Statistics (2022), *Computer and Information Technology Occupations*, https://www.bls.gov/ooh/computer-and-information-technology/home.htm (accessed on January 2023). [28]

Cammeraat, E. and M. Squicciarini (2021), “Burning Glass Technologies' data use in policy-relevant analysis: An occupation-level assessment”*, OECD Science, Technology and Industry Working Papers*, No. 2021/05, OECD Publishing, Paris, https://doi.org/10.1787/cd75c3e7-en. [4]

Carnevale, A., T. Jayasundera and D. Repnikov (2014), *Understanding Online Job Ads Data*, https://cew.georgetown.edu/wp-content/uploads/2014/11/OCLM.Tech_.Web_.pdf. [41]

Department for Education (2021), *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1027163/Bootcamps_wave_1_final_evaluation_report.pdf*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1027163/Bootcamps_wave_1_final_evaluation_report.pdf. [29]

EY (2022), *EY Financial Services Brexit Tracker: Movement within UK financial services sector stabilises five years on from Article 50 trigger [Press Release]*, https://www.ey.com/en_uk/news/2022/03/ey-financial-services-brexit-tracker-movement-within-uk-financial-services-sector-stabilises-five-years-on-from-article-50-trigger. [9]

Fortinet (2022), *2022 Cybersecurity Skills Gap*. [26]

Gartner (2022), *Enterprise Architecture (EA)*, https://www.gartner.com/en/information-technology/glossary/enterprise-architecture-ea#:~:text=Enterprise%20architecture%20(EA)%20is%20a,desired%20business%20vision%20and%20outcomes. [42]

GDPR EU (2022), *Does the GDPR apply to companies outside of the EU?*, https://gdpr.eu/companies-outside-of-europe/. [37]

Greater Manchester Combined Authority (2021), *Manchester Digital Security Hub (DiSH)*, https://www.greatermanchester-ca.gov.uk/what-we-do/digital/global-digital-influencer/greater-manchester-cyber-ecosystem/manchester-digital-security-innovation-hub/. [16]

IMD World Competitiveness Center (2022), *IMD World Digital Competitiveness Ranking 2022*, https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/. [11]

Indeed (2023), *Career Explorer - IT Security Specialist*, https://www.indeed.com/career/it-security-specialist/career-advice?from=top_sb. [44]

Indeed (2022), *IT Requirements and Qualifications (With Careers in IT)*, https://www.indeed.com/career-advice/career-development/it-jobs-qualification#:~:text=You'll%20typically%20need%20a,job%20in%20the%20tech%20industry. (accessed on January 2023). [27]

International Telecommunications Unit (2020), *Global Cybersecurity Index 2020*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. [12]

Ipsos MORI, Perspective Economics, CSIT (2021), *UK Cyber Security Sectoral Analysis*. [7]

ISACA (2022), *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations*, https://www.isaca.org/go/state-of-cybersecurity-2022. [25]

Joint Task Force Transformation Initiative (2018), *Risk management framework for information systems and organizations:*, National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/nist.sp.800-37r2. [23]

Lightcast (2022), *Hack the Gap: Fixing Cybersecurity's Broken Talent Pipeline*. [30]

New Zealand Qualifications Authority (2016), *The New Zealand Qualifications Framework*, https://www.nzqa.govt.nz/assets/Studying-in-NZ/New-Zealand-Qualification-Framework/requirements-nzqf.pdf. [32]

NICCS (2022), *NICE Cybersecurity Workforce Framework Work Roles*. [22]

NIST (2022), *Cybersecurity Framework*, https://www.nist.gov/cyberframework/getting-started. [36]

O*NET (2022), *Computer Systems Engineers/Architects*, https://www.onetonline.org/link/summary/15-1299.08. [21]

OECD (2022), *Purchasing power parities (PPP)* (indicator), https://doi.org/10.1787/1290ee5a-en (accessed on 23 October 2022). [39]

OECD (2022), *Skills for the Digital Transition: Assessing Recent Trends Using Big Data*, OECD Publishing, Paris, https://doi.org/10.1787/38c36777-en. [5]

OECD (2021), *OECD Skills Outlook 2021: Learning for Life*, OECD Publishing, Paris, https://doi.org/10.1787/0ae365b4-en. [3]

Office for National Statistics (2019), *Travel to Work Areas (December 2011) BFE in the United Kingdom*, https://geoportal.statistics.gov.uk/datasets/ons::travel-to-work-areas-dec-2011-bfe-in-united-kingdom/explore?location=55.215431%2C-3.313445%2C6.09. [17]

OWASP (2022), *About the OWASP Foundation*, https://owasp.org/about/. [35]

Scottish Qualifications Authority (2020), *HNC/HND Cyber Security*, https://www.sqa.org.uk/sqa/84394.html. [31]

SOC (2018), *Standard Occupation classification Manual*, https://www.bls.gov/soc/2018/soc_2018_manual.pdf. [40]

Statistics Canada (2022), *2021 Census - Boundary files*, https://www12.statcan.gc.ca/census-recensement/2021/geo/sip-pis/boundary-limites/index2021-eng.cfm?year=21 (accessed on February 2023). [14]

Stats New Zealand (2023), *Stats NZ Geographic Data Service*, https://datafinder.stats.govt.nz/layer/92215-territorial-authority-2018-clipped-generalised/ (accessed on February 2023). [15]

Stevens, T. and K. O'Brien (2019), "Brexit and Cyber Security", *The RUSI Journal*, Vol. 164/3, pp. 22-30, https://doi.org/10.1080/03071847.2019.1643256. [8]

Strochak, S., K. Ueyama and A. Williams (2022), *_urbnmapr: State and county shapefiles in sf and tibble format_. R package version 0.0.0.9002*, https://github.com/UrbanInstitute/urbnmapr. [20]

The Open Group (2022), *The TOGAF® Standard, 10th Edition*, https://www.opengroup.org/togaf. [34]

Tulane University (2022), *What does a cybersecurity manager do?*, https://sopa.tulane.edu/blog/cybersecurity-manager. [24]

U.S. Bureau of Labor Statistics (2022), *Occupational Outlook Handbook*, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-5. [43]

University of San Diego (2022), *Cybersecurity vs. Information Security vs. Network Security*, https://onlinedegrees.sandiego.edu/cyber-security-information-security-network-security/#:~:text=Under%20this%20view%2C%20cybersecurity%20is,IT%20infrastructure%20from%20online%20threats. [33]

Urban Institute (2019), *Urbnmapr library for R*, https://github.com/UrbanInstitute/urbnmapr (accessed on February 2023). [18]

World Economic Forum (2022), *Global Cybersecurity Outlook 2022*, https://www.weforum.org/reports/global-cybersecurity-outlook-2022/. [6]

World Economic Forum (2022), *Global Risks Report 2022*, https://www.weforum.org/reports/global-risks-report-2022/. [1]

World Economic Forum (2020), *The Future of Jobs Report 2020*, https://www.weforum.org/reports/the-future-of-jobs-report-2020/. [38]

Annex 2.A. Methodological Annex

Groups of roles within the cyber security profession

Within the profession "Cyber / Information Security Engineer / Analyst", there is a significant variety of titles used by enterprises when advertising job postings. These titles provide an additional rich source of information to characterise countries' cyber security markets through identifying roles demanded by the industry. However, job titles do not necessarily follow a particular pattern to classify them in groups of similar professions. This poses a challenge for taking advantage of this information.

In order to structure this data and get insights from it, an approach based on keywords is implemented. First, the dataset of cyber security job postings for the United States in 2021 is used as the reference point to extract keywords. The United States is the country with the highest quantity of job postings in the datasets, which is useful to extract as much words as possible. Second, job titles are transformed to a big list of single words. From this list, stop words,[18] numbers, punctuation and blank spaces were excluded to favour the recognition of keywords. Finally, the top 100 more frequent words are selected to manually identifying those roles more demanded in the cyber security market. From this step, four groups of roles are considered: Analysts, Architects and Engineers, Auditors and Advisors, and Managers. With the keywords associated to each group, job titles are classified on one of these groups. If not classified, the offer is included in the category "others". Annex Table 2.A.1 summarises the keywords used and gives some examples about the job titles included on each group.

Annex Table 2.A.1. Groups of cyber security roles

Cyber security Groups	Keywords	Sample of Job Titles
Analysts	Analyst, Operations, Officer, Specialist, Expert	Information Security Analyst, Security Analyst, Cyber Security Analyst, IT Security Analyst, Information Security Officer
Architects and Engineers	Engineer, Architect, Engineering, Infrastructure, DevOps, Penetration, Tester, Vulnerability, Testing	Security Engineer, Senior Security Engineer, Information Security Engineer, Network Security Engineer, Security Architect, Cloud Security Architect
Auditors and Advisors	Auditor, Audit, Consultant, Advisor	IT auditor, Senior IT auditor, Cyber Security Consultant, Security Consultant, Information Security Advisor
Managers	Manager, Principal, Director, Administrator, President, Vice, Leader, Lead, Team, Project	Information Security Manager, IT Audit Manager, Director of Information Security, IT Security Manager, Lead IT auditor, Information Security Lead, Cloud AWS/Azure Security Manager

Source: OECD based on Lightcast data.

Groups of Digital, Engineering and Math-related professions

Annex Table 2.A.2 shows the professions included in the Digital, Engineering and math-related group used to compare the performance of the cyber security market and its relationship with other professions. Groups are based on the Lightcast taxonomy codes and the US 2018 Standard Occupation Classification (SOC, 2018[40]).

Annex Table 2.A.2. Groups of Digital, Engineering and Math-related professions

Groups	Lightcast Code	Profession Name
Chief Information Officer	11-3021.00	Chief Information Officer / Director of Information Technology
Computer Occupations	15-1111.00	Computer Scientist
	15-1111.91	Data Scientist
	15-1121.00	Systems Analyst
	15-1131.00	Software Developer / Engineer
	15-1131.91	Computer Programmer
	15-1131.92	Mobile Applications Developer
	15-1133.00	Computer Systems Engineer / Architect
	15-1134.91	Web Designer
	15-1134.92	Web Developer
	15-1134.93	UI / UX Designer / Developer
	15-1141.00	Database Administrator
	15-1141.91	Data Engineer
	15-1142.00	Network / Systems Administrator
	15-1143.01	Telecommunications Engineering Specialist
	15-1151.00	Computer Support Specialist
	15-1152.00	Network / Systems Support Specialist
	15-1199.00	Technology Consultant
	15-1199.01	Software QA Engineer / Tester
	15-1199.02	Network Engineer / Architect
	15-1199.03	Webmaster / Administrator
	15-1199.04	Geographer / GIS Specialist
	15-1199.06	Database Architect
	15-1199.07	Data Warehousing Specialist
	15-1199.09	Project Manager
	15-1199.10	Search Engine Optimization Specialist
	15-1199.11	Video Game Designer
	15-1199.12	Document Control / Management Specialist
	15-1199.91	Data / Data Mining Analyst
	15-1199.93	Business Intelligence Analyst
	15-1199.94	Business Intelligence Architect / Developer
	15-1199.95	IT Project Manager
Math-related Occupations	15-2011.00	Actuary
	15-2021.00	Mathematician
	15-2031.00	Operations Analyst
	15-2041.00	Statistician
	15-2041.01	Biostatistician
Engineers and Technicians	17-2061.00	Hardware Engineer
	17-2072.92	RF Engineer
	17-2199.05	Mechatronics Engineer
	17-2199.07	Optical / Laser Engineer
	17-2199.08	Robotics Engineer
	17-3012.00	Electrical / Electronic Designer
	17-3023.00	Electrical and Electronics Technician
	17-3024.01	Robotics Technician

Source: OECD based on Lightcast data and taxonomy.

A semantic analysis approach to assess skills relevance

Recent developments in Natural Language Processing (NLP) are used to leverage the semantic meaning of the information contained in the online job postings. Specifically, the so-called word embedding approach is applied to generate a semantic representation of each word in an *n*-dimensional vector, where each dimension indicates a specific context item. This representation allows the calculation of mathematical similarity measures to represent the similarity between different skills and professions/occupations.[19]

To obtain the most similar professions to cyber security, a Semantic Skill Bundle Matrix (SSBM) was created by calculating the cosine similarity index between all possible combinations of skills and professions. The cosine similarity index is based on the cosine of the angle between vector representations of words. When a pair of words are closely related, the angle of their vectors is closed to 0 and the cosine is close to 1. Conversely, when the cosine is negative the words can be related but are opposite in meaning. Specifically, the calculation of the index is:

$$CosSim(A, B) = \frac{(A \cdot B)}{||A||\,||B||}$$

Using the SSBM, the top five more relevant skills to the cyber security profession (Lightcast name is Cyber / Information Security Engineer / Analyst) were extracted:

- Cyber security,
- Information security,
- Anti-malware software,
- NIST cyber security framework, and
- Open web application security project (OWASP).

Using these skills, an average index is calculated for all professions in the SSBM to rank them. Annex Table 2.A.3 shows the top five more related professions alongside with the cyber security profession (in first position by construction).

Annex Table 2.A.3. Most similar professions to cyber security based on skills demand

Lightcast Code	Profession Name	Average similarity
15-1122.00	Cyber / Information Security Engineer / Analyst	0.61
13-1199.02	Security Management Specialist	0.43
33-3021.06	Security / Defense Intelligence Analyst	0.40
15-1133.00	Computer Systems Engineer / Architect	0.38
15-1199.02	Network Engineer / Architect	0.38
15-1142.00	Network / Systems Administrator	0.36

Note: The Average similarity is based on the cosine similarity calculated using a word embedding approach.
Source: OECD based on Lightcast data.

Annex 2.B. Limitations on the use of data from online job postings

Along with the benefits that online job postings offer to the analysis of the demand in labour markets, some limitations and caveats concerning the use of this data should be noted. Not all vacancies are available online and, therefore, online job postings are not necessarily representative of the demand in every sector of the labour markets *(see OECD* (2021[3]) *and* Cammeraat and Squicciarini (2021[4])*)*. Carnevale, Jayasundera and Repnikov (2014[41]), for instance, highlight that OJPs are made to target those applicants that are more likely to conduct searches online, which implies that job postings for less-educated workers can be underrepresented in this sort of data. Although this limitation is likely to be small within the cyber security job market, it is still relevant for those figures that include metrics for all the occupations as a point of reference.

Some aspects are also not always reported in every OJP. It should be noted, for instance, that results presented in this report regarding the minimum degree of education and years of experience required in the job postings, as well as the wage offered by recruiters, should be interpreted carefully due to relatively smaller sample sizes. Depending on the country, the share of OJPs with containing information on qualifications or experience required can be a small proportion of the sample (see Annex Table 2.B.1). It is also important to note that, wages posted in the OJPs are not necessarily in line with the full compensations received by employees in the professions as negotiations during the hiring process and complementary benefits, such as bonuses, are not included in the job postings.

Despite these limitations, the insights presented in this report are derived from thousands of OJPs with available information and these can contribute to characterise the cyber security worker's profile that a large share of recruiters are seeking in the labour market. Results presented in several sections in this chapter are complemented with insights from survey-based reports on the matter or data from labour statistics offices that can offer a broader view of the profile of cyber security workers across the countries considered in the report.

Annex Table 2.B.1. Share of non-missing values in variables for education, experience and wages

Average yearly percentage of non-missing values for the variable selected

	Australia		Canada		New Zealand		United Kingdom		United States	
	Cyber sec.	All occup.	Cyber sec.	All occup.	Cyber sec.	All occup.	Cyber sec.	All occup.	Cyber sec.	All occup.
Education	20%	26%	52%	32%	14%	15%	15%	17%	67%	51%
Experience	27%	18%	63%	37%	30%	15%	15%	13%	68%	46%
Wages	19%	26%	11%	27%	9%	11%	58%	62%	13%	23%

Note: Cyber sec.: Cyber security OJPs; All occup.: OJPs for all occupations. Education and experience refers to minimum years of education and experience required in OJPs, respectively. Wages refers to annual wages posted in OJPs.
Source: OECD calculations based on Lightcast data.

Notes

[1] Cyber attacks are typically defined as the attempt by hackers to damage or destroy a computer network or system. These attacks generally aim to disable, disrupt or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

[2] https://lightcast.io/

[3] In this report, cyber security professionals are identified by jobs falling into Lightcast's occupational group named "Cyber / Information Security Engineer / Analyst".

[4] It is important to notice that the results presented in the figures do not account for the possibility that the job may be performed remotely. The information used to build the maps uses the geographical location advertised in the job posting but in an increasing number of cases, in particular after the pandemic, jobs have become more flexible and some do allow for teleworking arrangements (which may or may not also require some degree of physical presence). These aspects are not considered in the analysis at this stage, implying that geographical dispersion may be even larger than the one represented in the figure.

[5] Digital-related occupation is used here for brevity. Those occupations include the digital, engineering and math-related occupations as in Annex 2.B.

[6] The Global Cyber Security Index 2020 ranked the United States and United Kingdom as top cyber security markets worldwide. Australia and New Zealand are in the position 12 and 48, respectively (International Telecommunications Unit, 2020[12]).

[7] The analysis also includes the group "Rest (not selected)" that gathers all these professions that were not selected previously, as an indicator of how associated the demand for cyber security with that general workforce demand is.

[8] Other occupations also involved in the data management process are among the most correlated professions with cyber security, such as Database Architects and Data Engineer.

[9] Some examples of roles in the cyber security profession are Security Analysts/Engineers/Architects, Penetration Testers, IT auditors or IT Security Managers/Directors.

[10] The study is based on surveys to cyber security professionals in managerial positions around the world. Nearly half of the respondents are located in North America.

[11] The variable indicating the minimum years of education required is a proxy variable based on the degree name required in the OJPs.

[12] Qualifications below bachelor's degree comprehends those degrees awarded with less than 16 years of education (including Associate's in the case of the United States and Canada or NVQs and PDAs in the United Kingdom). Bachelor's covers degrees that require 16 or less than 18 years. Master's, 18 or less than 21. PhD, 21 or more years.

[13] Indeed's data shows that approximately 70%-80% of the job postings seeking for network engineers, web developers, data scientist or IT security specialists in the United States require at least a bachelor's degree (Indeed, 2023[44]).

[14] Although the average experience in the (ISC)^2 report is two years higher than in the job postings, it may respond to the focus of the analysis on the minimum experience required in job postings.

[15] Enterprise Architecture is a concept concerning the alignment between business' objectives and the availability of technology and data solutions (for more detailed definitions see, for example, Gartner Glossary (2022[42])).

[16] To avoid misleading conclusions with technologies showing a fast growth but a low number of mentions, this section only consider those technologies with mentions above the average observed in the 2019-22 period.

[17] Results for the United States are in line with the median wages estimated by the US Bureau of Labor Statistics (2022[43]), which estimates for 2021 a median annual wage of USD 102.000 for the occupation Information Security Analysts, while the estimated median compensation in all occupations for the same year is USD 46.000.

[18] Words usually omitted in the analysis of texts or Natural Language Processing since they do not provide additional information or context (i.e. and, for, of, a).

[19] For a more detailed discussion on word embedding, review Annex 3.A on (OECD, 2022[5]).

3 The landscape of cyber security education and training programmes: The case of England (United Kingdom)

This chapter looks at the provision of cyber security education and training programmes in England (United Kingdom). It zooms in on the characteristics of the education and training programmes leading to entry-level jobs in the cyber security field, the current profile of learners, and their education and labour market outcomes. Particular attention is paid to strategies and initiatives to diversify enrolment, especially among young people and adults from disadvantaged backgrounds, boost employers' participation in the design and delivery of cyber security learning opportunities, and ensure the quality of cyber security training.

Introduction: The need for accessible and relevant cyber security training

Chapter 1 highlights the strong and growing demand for cyber security professionals. The volume of Online Job Postings (OJPs) in this field has increased substantially in Australia, Canada, New Zealand, United Kingdom and the United States as remote working has been expanding and a broader range of digital technologies has been adopted, especially since the COVID-19 pandemic. When this growing demand for cyber security professionals is not met with a sufficient supply of trained workers for the field, this results in shortages that can potentially lead to cyber security threads. Shortages are already observed today, with research by (ISC)² (2022[1]) showing that the workforce gap for the five countries included in this study is among the highest in the world, especially in the United Kingdom.

Education and training to develop the right cyber security skills are therefore crucial to tackle shortages and avoid cyber security risks. This chapter zooms in on the case of England (United Kingdom) to provide an overview of its education and training programmes in the cyber security field and related policies. As in the rest of the world, the United Kingdom's society has become increasingly digital. Cyber security has become a priority, including the need for a skilled cyber security workforce. The number of cyber attacks is outstripping defence capabilities in the United Kingdom, and cyber security threats are growing both in number and sophistication – it is estimated that around 43% of businesses in the United Kingdom experienced a cyber security breach or attack in the last 12 months (2018-19) (CISCO, 2019[2]). Consequently, the share of job postings seeking cyber security professionals has increased considerably in the last decade in the United Kingdom, almost doubling in the last ten years (see Chapter 1). However, more than half of cyber security-related jobs in the country have been reported to be unfilled (CISCO, 2019[2]).

Cyber security skill shortages may reflect the limitations of education and training systems to provide cyber security programmes that prepare the professionals needed in the sector, as well as the absence of policies to encourage the supply of high-quality courses in this field and to promote them among young people and adults. Moreover, the current training provision may need more flexibility to respond to rapidly changing skills needs in the sector and to be accessible to a diverse group of learners. Engaging employers in the design and delivery of programmes is crucial to ensure their content is aligned with the needs of the labour market. Ensuring prospective learners understand the cyber security field and that the pathways into cyber security careers are clear and easy to access is important to attract learners from various backgrounds. Making the cyber security profession more attractive for women can help address their significant underrepresentation in the industry and simultaneously fill the workforce need. Common barriers to participating in cyber security education and training include a lack of basic digital skills for carrying out further and higher education in the field, as well as financial and non-financial barriers to engaging with learning opportunities, especially those related to STEM fields (Malcom and Feder, 2016[3]; Houston et al., 2022[4]).

This chapter provides an overview of the supply of cyber security education and training programmes in England. The chapter describes strategies and policies implemented to expand the supply of cyber security education and training and to encourage greater participation in these programmes. Special attention is given to initiatives that seek to increase the diversity of the profession and promote access for people from disadvantaged backgrounds. It also looks at strategies that encourage employers to participate in the design and delivery of learning opportunities in cyber security and initiatives to foster quality training. This chapter leverages information collected from interviews with relevant stakeholders in the cyber security sector, including training providers and different government bodies.

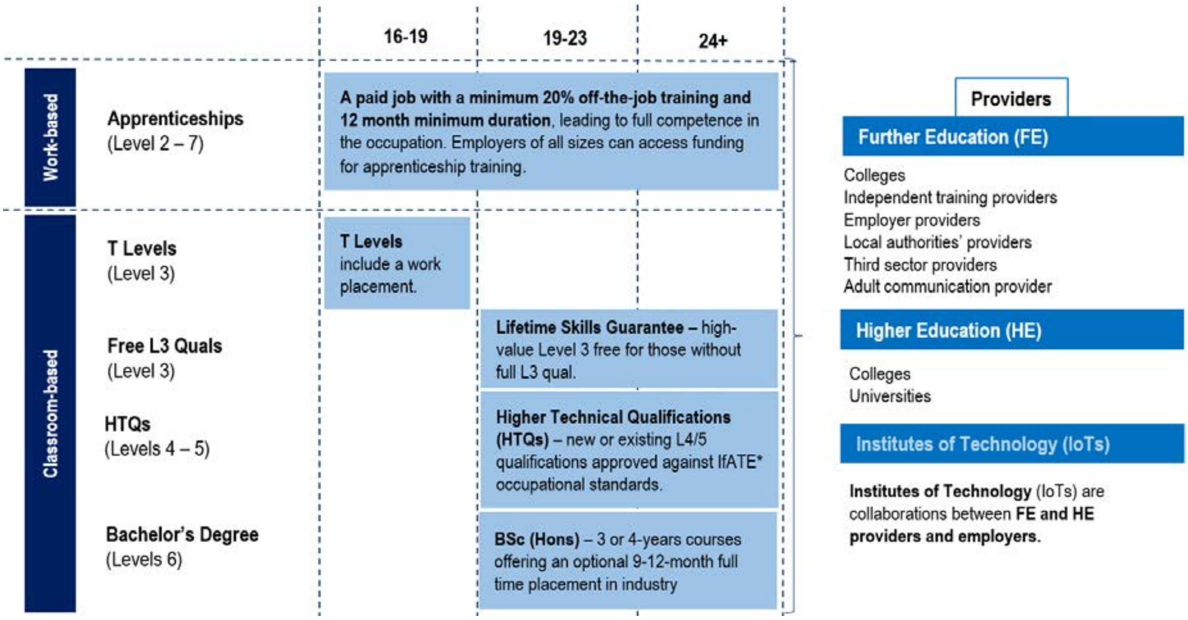
A snapshot of cyber security education and training in England

The provision of cyber security education and training programmes in England

In England, the provision of education and training programmes for developing cyber security skills for entry-level jobs (i.e. a job that typically does not require advanced levels of education and training in the field or many years of relevant work experience) takes multiple forms. Training programmes in this field can be offered through formal and non-formal education and training. Formal education, which leads to formal qualifications such as bachelor's degrees, includes courses and programmes offered by Further Education (FE) and Higher Education (HE) institutions. For this study, programmes at the Master's level and above are excluded from the analysis (see Box 3.1). Non-formal education and training includes courses outside the formal education system and not leading to a formal qualification but awarding certificates in some cases or, as in bootcamps, leading to a new job outcome.

Depending on where the training takes place, cyber security education and training programmes in England can be classified into work- and classroom-based (see Figure 3.1). Within formal education, the first group includes all the programmes with significant on-the-job training. The training content is typically employer-led, and the on-the-job training is complemented by learning activities offered by a college, university or other training providers. Programmes within this group include apprenticeships.

Figure 3.1. Formal education and training that cover cyber security skills in England



A paid job with a minimum 20% off-the-job training and 12 month minimum duration, leading to full competence in the occupation. Employers of all sizes can access funding for apprenticeship training.

T Levels include a work placement.

Lifetime Skills Guarantee – high-value Level 3 free for those without full L3 qual.

Higher Technical Qualifications (HTQs) – new or existing L4/5 qualifications approved against IfATE* occupational standards.

BSc (Hons) – 3 or 4-years courses offering an optional 9-12-month full time placement in industry

Colleges
Independent training providers
Employer providers
Local authorities' providers
Third sector providers
Adult communication provider

Colleges
Universities

Institutes of Technology (IoTs) are collaborations between **FE and HE providers and employers.**

Note: This figure does not include graduate higher education programmes such as master's and PhD. Qualifications are grouped into different levels. In England, there are nine different levels of qualifications: Entry level (Skills for life) and Levels 1 to 8. Mapped into the International Standard Classification of Education (ISCED), Level 2, Level 3, A-levels, T-levels, intermediate apprenticeships, and advanced apprenticeships correspond to ISCED 3 (i.e. upper secondary education); Level 4 and 5 qualifications correspond to ISCED 5 (i.e. short-cycle tertiary education); Bachelor's degrees correspond to ISCED 6 (i.e. bachelor's or equivalent level).
Source: Adapted from information received from the Department for Education.

The second group of programmes are predominantly delivered in school-based settings (including online provision), although they may include some short work placements. In the cyber security field, this group encompasses Level 3 Qualifications,[1] T-Levels,[2] Higher Technical Qualifications (HTQ),[3] and bachelor's programmes. More details about these programme types are provided in the remainder of this section.

The diversity in cyber security education and training in terms of qualifications, levels and providers allows learners to find the most suitable training for their learning needs. For example, learners with limited background in information and communication technology (ICT) can enrol in introductory training programmes in cyber security – offered mostly at Level 3 (equivalent to ISCED 3, i.e. upper-secondary education) but also including several programmes at Level 2 (equivalent to ISCED 3)[4] in the ICT field that provide students with the foundations for engaging in more field-specific training in cyber security. In some cases, cyber security courses may include modules on basic digital skills relevant for progressing into the more advanced parts of the training. For more experienced learners, higher technical qualifications and higher education degrees at Levels 4 to 6 (equivalent to ISCED Levels 5 and 6, i.e. short-cycle tertiary education and bachelor's programmes) provide various options for developing advanced cyber security skills.

Non-formal education programmes are also part of students' options to engage in cyber security education and training. Bootcamps, for instance, are flexible courses of up to few weeks or few months, which can be offered by public or private training providers. The Department for Education offers Skills Bootcamps which can be fully funded by the government (these bootcamps supported by the Department for Education are referred to as "Skills Bootcamps" in the remainder of the chapter). These courses provide students with knowledge and skills currently relevant to priority sectors.

Figure 3.2 shows an overview of the provision of cyber security education and training in England, including formal education and training and Skills Bootcamps (non-formal). In 2022, around 890 Skills Bootcamps in digital skills were available, of which 77 were in cyber security (Department for Education, 2022[5]). Two of the 26 apprenticeship standards in digital occupations are specifically for cyber security. Level 3 and T-level qualifications in digital all include cyber security subjects in the core. Various HTQs and Bachelor's degrees have cyber security content or a cyber security specialisation.

Box 3.1. Defining the scope of cyber security education and training for this study

Cyber security education and training covers a broad topic and touches upon multiple intertwined areas of knowledge (CyBOK, 2019[6]). It can go from cyber security awareness, which helps the general public identify and avoid cyber threats, to more technical skills, such as management of intrusion detection software or penetration testing, oriented to a more specialised labour force capable of working in cyber security occupations. These technical skills typically are imparted within structured training programmes involving dedicated trainers and experts.

This study focuses on the education and training programmes for developing cyber security technical skills. Moreover, it focuses on education and training programmes that develop the technical skills required for entry-level jobs. Entry-level jobs usually do not need many years of relevant work experience or advanced education and training in the field (e.g. no master's degree in engineering with cyber security specialisation). Therefore, the study focuses on formal programmes at the bachelor's level and below and non-formal programmes at comparable levels. While master's degrees and above are vital for the wider cyber security profession, the lower-level qualifications are particularly valuable for making the profession more accessible and potentially more diverse (and possibly provide pathways into the more advanced qualifications).

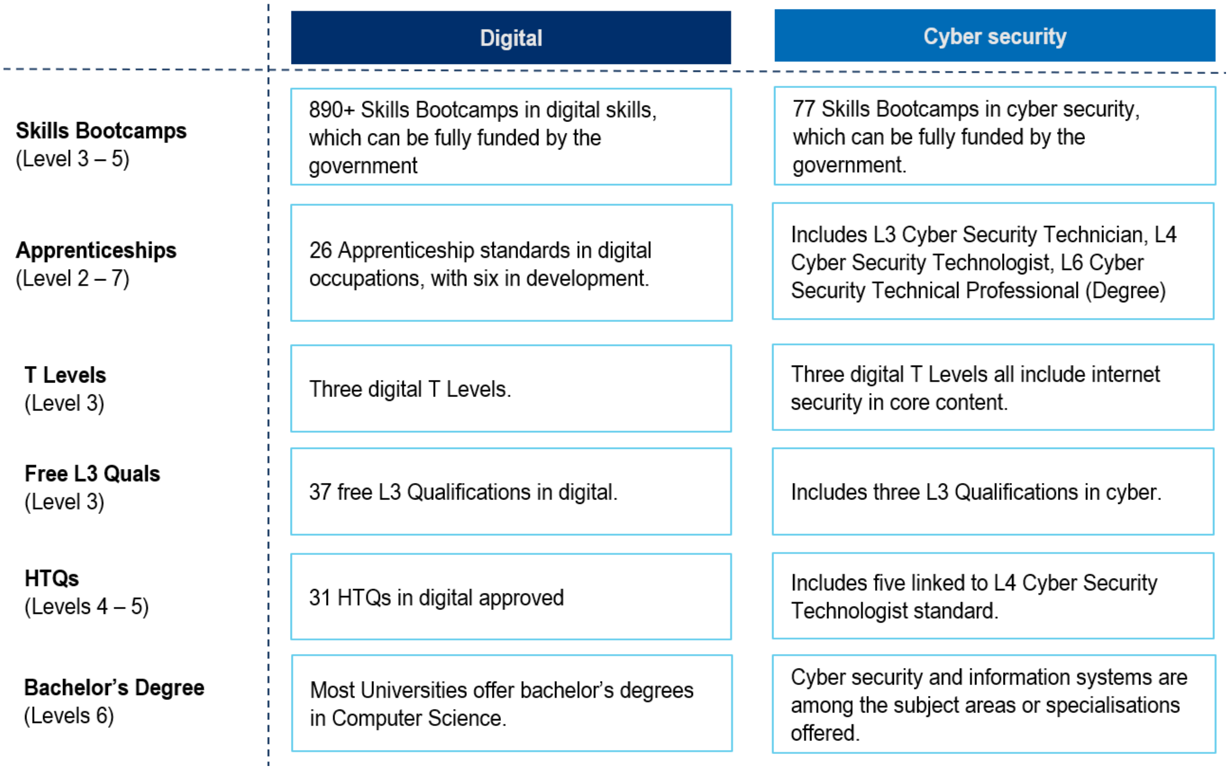
The set of relevant technical skills for cyber security professionals is extensive and diverse. According to the Department for Culture, Media and Sports (DCMS), cyber security can be defined as a set of techniques designed to protect systems, networks and data in cyberspace. It comprises processes, technologies and controls to protect such systems, networks and data from cyber attacks, damage or unauthorised access (DCMS, 2019[7]). Similarly, CyBOK (i.e. a comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector in the United Kingdom) identifies 21 top-level knowledge areas (see Table 3.1) related to cyber security and its profession (CyBOK, 2019[6]). These knowledge areas are grouped into five broader categories: 'Human, organisational and regulatory aspects of cyber security'; 'System security'; 'Software and platform security'; 'Infrastructure security'; and 'Attacks and defences'. The "human organisation and regulatory" aspects are typically not targeted by dedicated programmes but are instead embedded in other education and training programmes and are, therefore, outside the scope of this study.

Table 3.1. Cyber security areas of knowledge, according to CyBOK

Infrastructure security	System Security	Software and platform security	Attacks and Defence	Human organisation and regulatory aspects
Physical layer and telecommunications security	Operating systems and virtualisation security	Web and mobile security	Security operations and incident management	Law and regulation
Applied cryptography	Cryptography	Software security	Forensics	Privacy and online rights
Cyber-physical systems	Formal methods for security	Secure software lifecycle	Adversarial behaviours	Human factors
Network security	Distributed systems security		Malware and attack technologies	Risk management and governance
Hardware security	Authentication, authorisation and accountability			

Note: The right column is not included in the scope of this study.
Source: CyBOK (2021[8]), Introduction to CyBOK Knowledge Area Version 1.1.0., National Cyber Security Centre 2021, https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf.

Figure 3.2. An overview of the main cyber security and digital programmes in England



	Digital	Cyber security
Skills Bootcamps (Level 3 – 5)	890+ Skills Bootcamps in digital skills, which can be fully funded by the government	77 Skills Bootcamps in cyber security, which can be fully funded by the government.
Apprenticeships (Level 2 – 7)	26 Apprenticeship standards in digital occupations, with six in development.	Includes L3 Cyber Security Technician, L4 Cyber Security Technologist, L6 Cyber Security Technical Professional (Degree)
T Levels (Level 3)	Three digital T Levels.	Three digital T Levels all include internet security in core content.
Free L3 Quals (Level 3)	37 free L3 Qualifications in digital.	Includes three L3 Qualifications in cyber.
HTQs (Levels 4 – 5)	31 HTQs in digital approved	Includes five linked to L4 Cyber Security Technologist standard.
Bachelor's Degree (Levels 6)	Most Universities offer bachelor's degrees in Computer Science.	Cyber security and information systems are among the subject areas or specialisations offered.

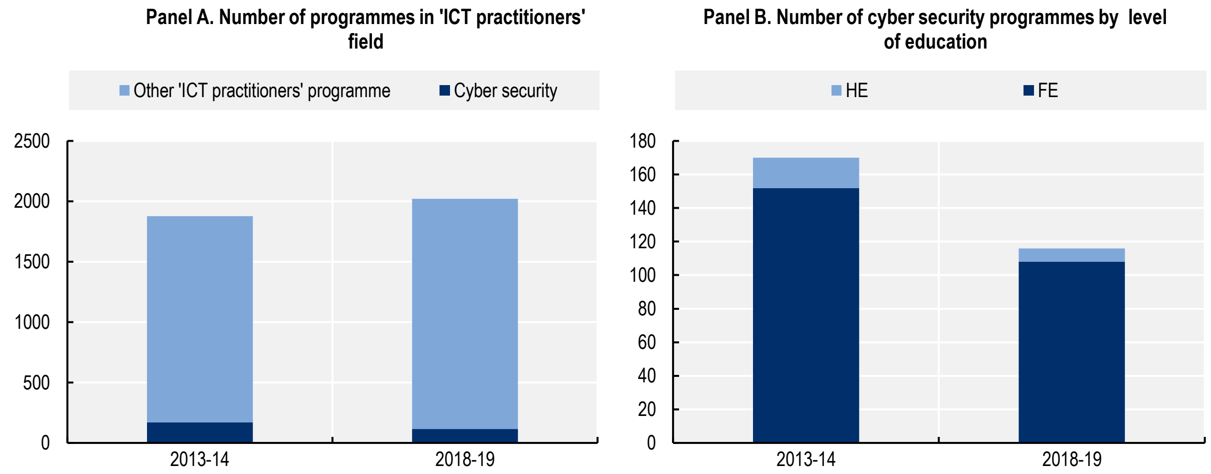
Note: See Figure 3.1 for the details about the levels. All numbers refer to the offer in September 2022. There is no record on the supply of commercially delivered bootcamps, thus this table only includes information from the Skills Bootcamps offered by the Department for Education.
Source: List of Skills Bootcamps training providers from the Department for Education, https://www.gov.uk/government/publications/skills-bootcamps-training-providers; complemented with information from the Association of Colleges and information retrieved from Colleges' websites on 17 October 2022 and the website 'Find Apprenticeships' of the UK Government, https://www.gov.uk/apply-apprenticeship.

Formal education and training: The role of further and higher education

Formal education and training programmes in the cyber security field include higher education programmes (HE) and further education (FE) programmes. FE includes any study after secondary education (post-16) that is not part of higher education (not taken as part of an undergraduate or graduate degree). FE programmes typically equip young people and adults with skills and qualifications that are immediately relevant for the labour market but also allow studying at higher education levels (including higher levels of FE and higher education). Especially in cyber security, FE's role focuses on providing building blocks for more advanced programmes. Provided that learners have relevant foundational skills, they can progress throughout a cyber security training pathway, allowing them to engage with more complex issues and topics.

FE and HE institutions are essential in providing ICT education and training programmes. According to the Department for Education, there are 510 formal education and training providers in ICT, including FE colleges and HE institutions (Department for Education, 2022[9]). There are 226 different qualifications available in ICT, of which 89 are related to 'ICT practitioners' (i.e. a set of programmes within the ICT field providing practical knowledge, skills, capabilities and competencies on information technology, including cyber security)[5] – including six that indicate having cyber security in the title. As shown in Figure 3.3, the total number of 'ICT practitioner' programmes offered across FE and HE providers amounts to around 2 000, of which only about 120 are in cyber security. The number of cyber security training programmes offered across institutions has slightly decreased compared to 2013-14, but enrolment went up (see next section). One possible explanation is the diversification of training. More and more formal and non-formal education institutions offer non-formal cyber security training, such as bootcamps, which may be correlated with the reduction of formal cyber security training (see below). Moreover, cyber security subjects may be included in broader fields such as computer science or network without being indicated in the programme's title or qualification.

Figure 3.3. Provision of formal cyber security education and training programmes



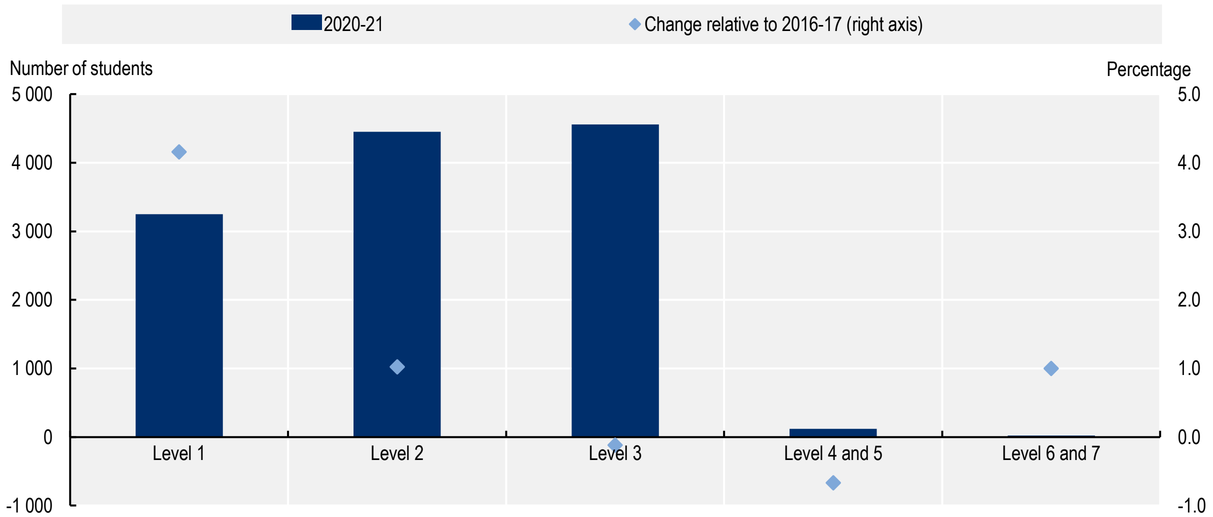
Note: The number of programmes corresponds to the number of qualifications times the number of institutions offering them. Refers to programmes leading to a formal qualification only. Panel B is a zoom-in of Panel A focused on cyber security programmes. Cyber security programmes were identified based on the description of the qualification awarded. The programmes that have cyber security content or with cyber security titles are Computer science (cyber security), computing and ICT (cyber security), Technical level IT Networking (Cyber security), Computing (cyber security), Diploma in Information Technology (cyber), Digital and IT (cyber).
Source: OECD computations 2022 using data from the Department for Education, https://www.gov.uk/government/organisations/department-for-education/about/statistics.

Level 2 and 3 FE programmes

Cyber security training at Levels 2 and 3 in FE is typically an introduction to the cyber security field.[6] Level 2 courses tend to be generalist in ICT or digital skills. but they include some elements of cyber security in the core content more focused on cyber awareness and cyber security and e-safety. However, some Level 2 courses dedicated to cyber security foundations exist. At Level 2 cyber awareness courses provide the learner with an introduction to cyber security covering areas such as computer systems and the impact of cyber security, information technology for business and the internet of everything, impact of cyber security in the business environment. Since 2020, the number of Level 2 courses in digital skills has increased, expanding students' chances to engage with cyber security foundational training at an earlier stage (Department for Education, 2022[9]). Figure 3.4 shows a relatively large and growing number of learners in ICT practitioners programmes at that level. Level 3 courses are a common starting point for students to engage with cyber security training within the FE sector. There are a range of quals covering networking and cyber security in a more in depth and focussed way, offering the opportunity to cover areas such as applying networking and cyber security projects, and looking at issues around cloud based solutions, security solutions and surveillance software. These courses are subject-based qualifications equivalent to Advanced level qualifications (A-levels), generally taken after students finish their General Certificate of Secondary Education (GCSE). These courses provide young people and adults with the capabilities needed to be successful in the labour market or go on to study at a higher FE level or the HE level, for example, to pursue a degree at a university in a cyber security-related field.

Figure 3.4. Enrolment in FE programmes in ICT practitioners' fields, by level

Number of FE students in ICT practitioners' fields (including cyber security) in 2020-21 and change relative to 2016-17



Note: Volumes are rounded to the nearest 10. The figure does not show the Applicable/Not Known category, which includes qualifications with no level or taken at several levels. The data include Apprenticeships, Community Learning, and Education and Training provision at General Further Education Colleges (including Tertiary), Sixth Form Colleges, Special Colleges (Agricultural and Horticultural Colleges and Art and Design Colleges), Specialist Colleges and External Institutions. The number of students at Level 6 and Level 7 is 20.
Source: UK Education Statistics, https://explore-education-statistics.service.gov.uk/data-tables/permalink/27cbce98-f34f-4f6f-3300-08dac71eb496.

Table 3.2 shows a sample of the FE programmes for students at Levels 2 and 3. Most Level 2 and 3 programmes offer an "introduction", "principles", or "essentials" of cyber security, indicating that learners will develop foundational knowledge in the field. There are also a considerable number of Level 2 and 3 qualification courses that include cyber security as a module (e.g. computer science) (DCMS, 2019[7]), since programmes at these levels are typically meant to be broader and less specialised.

Introductory cyber security skills are also developed within T-level programmes. T-levels are two-year, career-focused qualifications and one of a number of post-16 education options in England, alongside A-levels and apprenticeships. T-level students spend 80% of the course in their learning environment, gaining the skills that employers need. The other 20% is a meaningful industry placement, where they put these skills into action (Department for Education, 2023[10]). T-levels are available at selected colleges, schools and other providers across England. The courses are usually developed in collaboration with employers and education providers, so the content meets the needs of industry and prepares students for entry into skilled employment or further learning (including apprenticeships or programmes in further or higher education). T-levels are relatively new in the English education system. In 2023, there are over 20 T-level subjects and more being rolled-out in future years. There are three Digital T-levels available "digital business services", "digital production, design and development", and "digital support services". The digital support services T Level includes technical aspects of internet security, digital environment and cloud environments and security testing software as part of the core content. Career options upon completion might include becoming an infrastructure technician or a role in IT security support (HM Government, 2022[11]).

Table 3.2. Sample of Level 2 and 3 FE programmes in England

Programmes/course title	Description
Level 2 Principles of cyber security certificate	Qualification ideal for learners who wish to build a strong foundation of knowledge in cyber security. Among other topics, it covers an Introduction to cyber security, the terminology used in cyber security, common Threats and Maintaining.
Level 2 Certificate in Cyber Security and Digital Forensics	A practical and multi-modular course that covers many areas of new emerging technologies. Students learn by completing industry-focused digital projects while developing the technical and transferable skills required to work in this sector. Course topics include development, cyber security, networking, and cloud technologies.
Level 2 Certificate in the Principles of Cyber Security	This foundational online course is available for anyone looking to increase their understanding of computing, specifically how to keep themselves and their work secure.
Level 3 Northern Council for Further Education (NCFE) certificate in Cyber security basics	A qualification designed to provide learners with knowledge and skills in cyber security practices. Learners can develop knowledge and skills about cyber security practices to seek employment or further study.
Level 3 Certificate in Principles of cyber security	This qualification is designed to provide learners with sector awareness. It increases the knowledge and understanding of roles and issues relating to cyber security. This qualification aims to focus on the study of cyber security principles and offer breadth and depth of analysis, incorporating essential critical core of cyber security knowledge. The training covers Introduction to cyber security, relevant terminology, common threats and maintaining.
Level 3 Diploma in Networking and Cyber security	This course suits anyone looking to develop their understanding of Digital Technologies, specifically Networking and Cyber security. The course covers access control, data communications, ethical hacking, network management and network threats and vulnerabilities.

Source: Websites of the following FE colleges: Bath college (https://bathcollege.ac.uk/course/view/2720/principles-of-cyber-security-certificate-l2-22-23), Derwentside college (https://www.derwentside.ac.uk/school-leavers/courses/digital-technology/), Northampton college (https://www.northamptoncollege.ac.uk/courses/computing-it/level-2-certificate-in-the-principles-of-cyber-security), East Sussex College (https://www.escg.ac.uk/courses/computing-ict/software-practice/cyber-security-basics-cert-l3-73973/), Macclesfield college (https://macclesfield.ac.uk/courses/certificate-in-the-principles-of-cyber-security/) and West Thames college (https://www.west-thames.ac.uk/courses/computing-and-ict/253-level-3/1617-gateway-level-3-diploma-in-networking-and-cybersecurity). Information accessed on 23 October 2022.

Higher technical education (Levels 4 and 5)

Higher technical education allows learners to develop cyber security skills at more advanced levels (Levels 4 and 5, equivalent to ISCED 5). As shown above, enrolment in Level 4 and 5 ICT programmes in FE is relatively low. In 2020, the DfE approved the higher technical education reform to improve the quality and labour-responsiveness of higher technical education (Department for Education, 2020[12]). As a result, in September 2022, the first cycle of new or existing Level 4 and 5 qualifications, meeting occupational standards for the digital sector, was approved by the Institute of Apprenticeships and Technical Education and launched as Higher Technical Qualifications (HTQs).

According to the Institute for Apprenticeships and Technical Education (IfATE), there are 31 HTQs in the digital field, of which 12 are offered in cyber security or include a cyber security specialisation (IfATE, 2022[13]). Table 3.3 shows a sample of HTQs in cyber security provided in England in the academic year 2022-23. The core content of the courses is more advanced and field-specific than the programmes at Levels 2 and 3. The courses cover computer forensics, networking and software systems, applied cryptography and information security management. Alongside these new HTQs, a range of other Level 4 and 5 qualifications exist, including some with a cyber security specialisation.

Table 3.3. Sample of cyber security-related Higher Technical Qualifications (Level 4 and 5) courses provided by FE Colleges and HE institutions

Programme/course title	Description
Level 5 Foundation degree in cyber security (HTQ)	This course emphasises the essential hands-on knowledge and skills demanded by employers. Learners can develop practical skills in computer forensics and implementing secure networks. Additionally, learners can explore networks and learn about scripting, ethical hacking, attacking and defending infrastructures and operating systems such as Linux.
Level 5 Foundation degree in Digital Technology (Cyber security) (HTQ)	This course provides an overview of computing and information security principles to support business needs using current, industry-standard technologies and approaches, with a strong focus on problem-solving. This course covers fundamentals of computer hardware, networking, and software systems to the organisational and legal aspects of managing information security, with practical, hands-on experience via our custom-designed virtual cyber security lab.
Level 4 in Computing (Cyber security) (HTQ)	This is a full-time programme which comprises eight modules studied over one year. Learners can develop a range of specialist skills to meet the demands of employers. The course covers computing fundamentals, programming, networking, professional practice, database design and development, security and planning a computing project. In addition, the system includes a mandatory specialist unit on cyber security.
BTEC Level 4 in computing (Cyber security) (HTQ)	This programme is a specialist pathway focused on Cyber security. Learners can achieve an industry-recognised HND, enhancing career prospects and employability. The course content includes programming, networking, professional practice, database design and development, security, planning a computing project, cyber security, website design and development, computing research project, business process support, applied cryptography in the cloud, forensics, and information security management. Upon completing this course, learners can use to study for an additional year to gain a full BSc (Hons) degree and progress to a university.

Source: Website of the following FE colleges: University Centre Leeds (https://ucleeds.ac.uk/), York College (https://www.yorkcollege.ac.uk/study/foundation-degree-fd-digital-technology-with-cyber-security), Tameside College (https://www.tameside.ac.uk/pages/course_info.aspx?x=178508), and Bedford College (https://bedfordcollegegroup.ac.uk/courses/computing-cyber-security-hnd-full-time-fa073/). Information retrieved on 30 October 2022. BTEC stands for the Business and Technology Education Council.

Higher technical education is delivered by FE and HE providers. In addition, Institutes of Technology (IoTs) play an important role in providing higher technical education and training across a range of STEM occupations and industries. IoTs are a collaboration between FE providers, HE institutions and employers. They specialise in delivering employer-led training programmes, reacting quickly to an area’s current and evolving technical skills needs. Among 15 specialisms, IoTs offer courses in digital and IT fields, including cyber security. Although most of the training programmes provided by IoTs are at Levels 4 and 5 (including HTQs), some of them also include courses at lower levels (T-levels and Levels 2 and 3) covering most of the FE training building blocks for the cyber security profession (see Table 3.4).

Table 3.4. A sample of cyber security-related courses offered by an Institute of Technology

Programme/course title	Description
T-Level in Digital Support Services	This T-Level in Digital Support Services is for those who want to progress to work in front-line technical or hardware and software support, cloud technologies, or data or IT business analysis.
Level 3 Advanced apprenticeship Information Communication Technician (including a cyber security specialised role)	This Information Communication Technician apprenticeship offers the opportunity to prepare for a role in the industry whilst gaining real-life experience in a working environment with an employer. The cyber security specialism covers the following subjects: Information technology systems, programming, introduction to networking and security management.
FdSc Cyber Security **(HTQs)**	The programme aims to meet the complex and organic needs of the computing and IT sector by providing appropriately trained, qualified and skilled staff with the requisite knowledge, competence and understanding of cyber security threats and protective measures.
Level 4 Higher Apprenticeship cyber security Technologist (Higher apprenticeships)	In this course, learners develop an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organisations' systems and people. This programme offers two roles for specialisation within the cyber security field: Technical role and risks analysis role. Students can progress to the BSc (Hons) Digital Technology Solutions (Top-up) degree apprenticeship or BSc (Hons) Cyber security (Top-up)
BSc (Hons) Cyber security (Top-up) (**HE programme)**	This programme is designed to provide learners with the skills and knowledge to become a professional computing practitioner specialising in Cyber Security. Learners will study Ethical Hacking, The Cyber Security Landscape, and Principles of Computer Forensics and will complete various projects.

Source: Website of the North East Institute of Technology (https://neiot.ac.uk/subjects/digital). Information retrieved on 11 November 2022.

Higher education degrees (Undergraduate programmes)

At the higher education (undergraduate) level, students can opt for a technical or non-technical route into cyber security. Within the technical route, which is the focus of this study, there are two broad options at the undergraduate or bachelor's level: cyber security programmes (e.g. cyber security, cybernetics, digital forensics, etc.) or other programmes with a cyber security specialisation. The latter include, for example, programmes in computer science with cyber security specialisation (e.g. 'Computer science with cyber security'), and other STEM programmes with a cyber security focus – the most common ones being mathematics or engineering (e.g. Engineering with cyber security) (DCMS, 2019[7]). Non-technical courses can offer a module or specialisation in cyber security, such as Management, Business Studies or Psychology in cyber security- these are outside the scope of this report.

Programmes vary in the extent to which the content is field-specific, providing a variety of options for students with different preferences, needs and backgrounds. Some programmes have a modular approach, covering a wide range of ICT-related topics and competencies in the first year to build the foundations for more specific (and advanced) cyber security subjects later on. At the University of Royal Halloway, for instance, students can undertake courses on generalist ICT subjects, including 'software design', 'machine fundamentals' and 'operating systems' during the first year, allowing them to develop the fundaments required for more specialised subjects covered during the second year. Some other programmes are heavily focused on cyber security from the start and cover more specialised cyber security subjects in the following years. For instance, at the University of Warwick, students can undertake foundational courses in the cyber security field, such as security and information risk management, during the first year already, and more advanced courses, such as 'cyber security incident management' and 'data science and complexity in the cyber context', during the last two years of study.

The cyber security field in higher education is a relatively new discipline (DCMS, 2019[7]). However, it is attracting more students every year. The number of undergraduate programmes in cyber security (96) compared to computer science (694) is low, as is the number of students enrolled in this field (see Table 3.5 and Figure 3.5). However, among all ICT fields, cyber security has the highest student growth rate. During 2020-21, 5 900 students pursued a cyber security higher education degree, 30% more than the previous academic year (see Figure 3.5).

Table 3.5. Number of cyber security and computer science programmes provided by universities in England (2022-23)

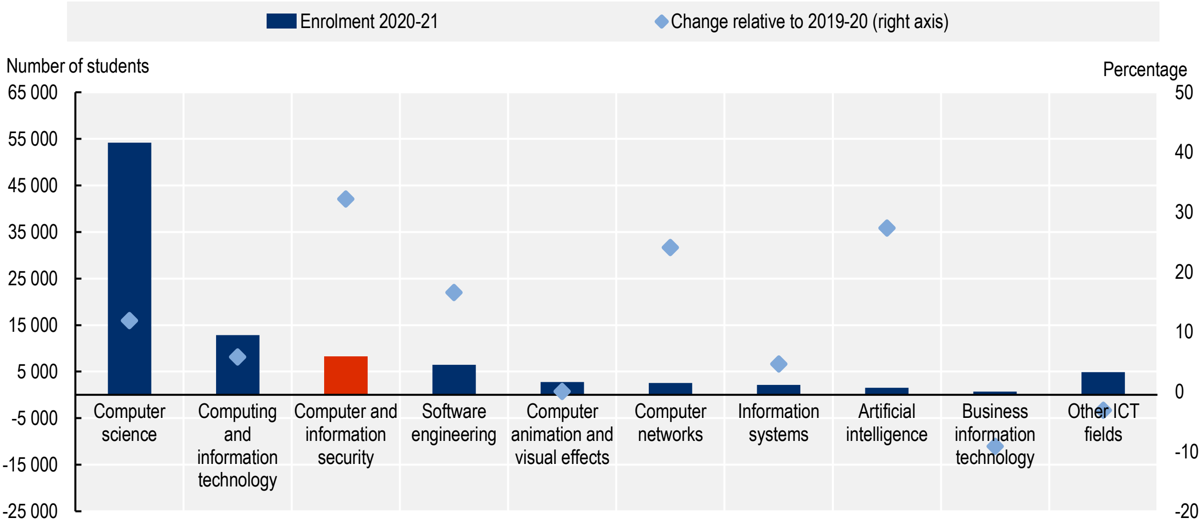
Number of programmes provided by universities by type of qualification

Qualifications	Computer science	Cyber security
Bachelor's	620	78
Other qualifications	74	18
Total	694	96

Note: Numbers include all programmes offered by universities below the master level. Cyber security figures also include cyber crime and forensics and programmes in computer science with cyber security specialisation. Numbers are based on UCAS' programme finder. Other qualifications include HND and HNC (Levels 4 and 5) offered by universities.
Source: Universities and Colleges Admission Service (UCAS), https://www.ucas.com/, (information retrieved on 11 November 2022).

Figure 3.5. Enrolment in ICT fields in higher education

Enrolment for the academic period 2020-21 and percentage change compared to 2019-20



Note: All students enrolled in higher education in programmes below the master's level with HECoS codes between 100 358 and 100 378 (ITC fields) in England are included in this figure. Other ICT fields include information technology, applied computing, business computing, business information system, creative computing, web and multimedia design, geographical information system and internet technologies, which account for less than 5% of the total enrolment. Data refer to rounded totals.
Source: Higher Education Statistic Agency (HESA), https://www.hesa.ac.uk/data-and-analysis/students/table-52.

Apprenticeships

Apprenticeship is another option to prepare for entry-level cyber security jobs. Apprenticeships combine practical training on the job with off-the-job training, allowing apprentices to gain job-specific skills while working alongside experienced staff from the sector in addition to the more theoretical aspects of cyber security. Students can participate in apprenticeships at various levels – depending on their previous experience, their knowledge in the field, and -in some cases- their prior qualifications. There are three cyber security apprenticeship qualifications approved: Cyber security technician at Level 3 (intermediate), cyber security technologist at Level 4 (advanced) and cyber security technical professional at Level 6 (degree level).

FE providers and HE institutions provide the off-the-job component of the apprenticeship. Academic entrance requirements to apprenticeships are broadly similar to those of classroom-based FE or HE programmes, with typically additional criteria added by employers as part of the recruitment process. Table 3.6 shows some examples of apprenticeship postings in the cyber security field. Based on these examples, employers seek candidates with technical aptitude and good all-around skills, such as attention to detail, communication, problem-solving and work ethic, among others.

Table 3.6. A sample of cyber security apprenticeship openings (employer postings)

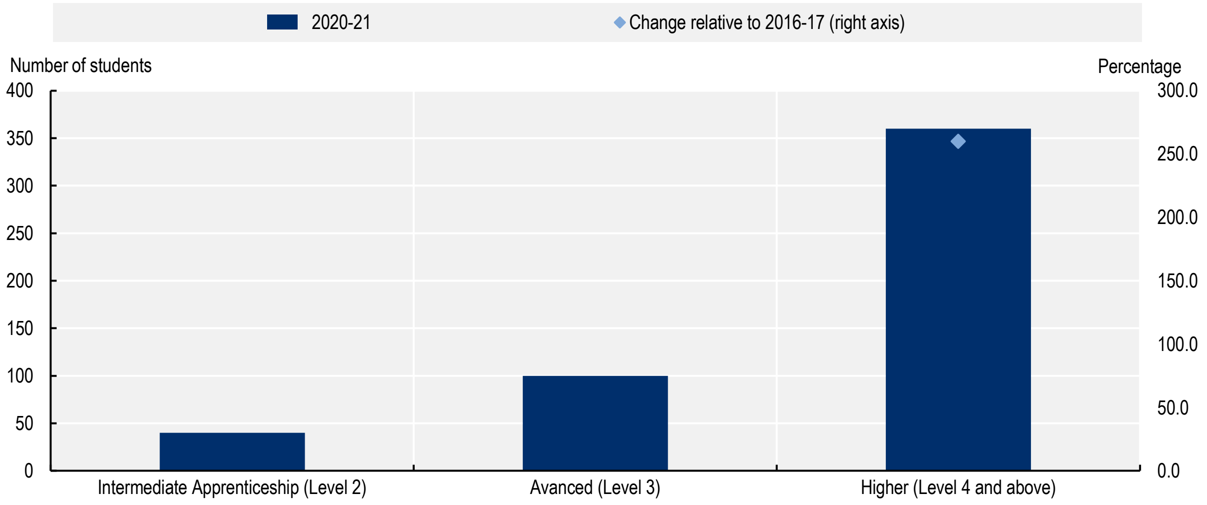
Programmes/course title	Sector	Apprenticeship posting information	Qualifications required
Level 3 Cyber security technician (Intermediate)	Finance	The Cyber and Security team are central to defending the bank, so the apprentice will have the opportunity to play a key part in keeping customers, clients and colleagues safe in a world entire of 21st-century digital threat. Defending the bank can be reactive or proactive. Whether placed in strategic intelligence, operational or tactical, the apprentice will be given all of the resources needed to kick-start a career in one of the most impactful areas of the bank.	5 GCSEs at A*-C (9-5), including Maths and English (or equivalent)
Level 4 Cyber security technologist qualification. (Advanced)	Social Service	Apprentices will be involved in all aspects of Cyber Security and be the escalation point for all Cyber Security-related issues. As the Cyber Security Analyst, the apprentice will undertake security assessments, manage any security Incidents, and be involved in all security-related tasks: Improving security for web applications, web servers, application technologies, frameworks and protocols concerning application development and deployment; and managing and advising on endpoint security and email filtering.	GCSE or equivalent Higher-Level Apprenticeship (Grade Level 2) desired
Level 6 cyber security technical professional. (Higher or Degree)	Media	Cyber security apprentices will advise on best practices, deal with threats, and manage potential cyber attacks across the company globally. Working with other teams, the apprentice will develop skills and knowledge to perform security risk assessments for a range of IT and Production systems and propose solutions jointly with other specialists.	A minimum of BBB A Levels or a DDM BTEC in a relevant subject; Maths and English GCSEs or Standard at 9-4 (A-C) or equivalent

Note: When retrieving the information from the UCAS website, there were 37 apprenticeship postings in cyber security fields. This table only presents one for each level of qualification.
Source: Universities and Colleges Admission Service (UCAS), https://www.ucas.com/ (information retrieved on 11 November 2022).

While apprenticeships in the cyber security field are available at different levels of qualification, most apprentices participate in higher programmes (Level 4 and above). Enrolment in apprenticeships increased strongly in the last five years (see Figure 3.6). In 2020-21, 4, 100 and 360 learners completed intermediate, advanced and higher apprenticeships, respectively, in this field. Additionally, the number of students in higher apprenticeships in cyber security has increased substantially compared to 2016-17 (by 2.5 times, see Figure 3.6). Nonetheless, the absolute numbers remain relatively low – especially at the intermediate-level. According to the University and College Admission Service (UCAS) portal, in November 2022, 37 cyber security apprenticeship positions were posted, of which only three were offered at an intermediate level.[7]

Figure 3.6. Apprenticeships starts in cyber security by the level of qualification

Number of apprenticeship starts in cyber security in 2016-17 and 2020-21



Note: Intermediate and Advanced apprenticeships in cyber security have only been on offer since 2018-19. The term 'starts' refer to number of new people starting an apprenticeship each year. More detailed information about the number apprenticeships starts can be found in this link: GOV.UK, Further education and skills statistics: methodology, Methodology: Explore education statistics, https://explore-education-statistics.service.gov.uk/methodology/further-education-and-skills-statistics-methodology.

Source: UK Education Statistics, https://explore-education-statistics.service.gov.uk/data-tables/permalink/765f8afa-19b3-4fb3-c74d-08dac7ae389f.

Non-formal training: The characteristics of training outside the formal education system

In addition to formal education and training, young people and adults in England can participate in cyber security training outside the formal education system. These non-formal courses do not lead to a formal qualification, although a certificate can be awarded in some cases. Bootcamps are one particular form of non-formal training in England, mostly offered by independent training providers but also by universities and further education colleges.

Bootcamps

Bootcamps are intensive skill development programmes that cover topics highly relevant to a specific sector, such as cyber security (Learn21, 2022[14]). These short courses can take a few weeks or a few months to complete and aim to provide training as a starting point for an absolute beginner or custom advanced learning for candidates through a selection process. Bootcamps are job-oriented and give the opportunity to build sector-specific skills and, in some cases, fast-track to an interview or progress in their current role. In England, cyber security bootcamps are offered by public and private training providers covering a wide range of topics at several difficulty levels. They can be fully funded by the government after meeting eligibility requirements (e.g. Department for Education Skills Bootcamps) or can be fully or partially covered by learners.

The Department for Education Skills Bootcamps (in the remainder of the chapter referred to as Skills Bootcamps) are free, flexible courses of up to 16 weeks at Levels 3-5, available in England, giving people the opportunity to build up sector-specific skills and fast-track to a job interview with a local employer once the training is completed (Department for Education, 2022[15]). The courses are open to adults aged 19+ who have the right to work in the United Kingdom, live in England and meet residency requirements. Some

Skills Bootcamps have additional eligibility criteria. They are available in several subjects and sectors, including (as of January 2023) digital, technical, construction, logistics, and green skills, with the scope to expand into a wider range of sectors. Skills Bootcamps are designed for adults who want to upskill quickly to work in specific sectors (e.g. cyber security or construction) or for those who wish to gain in-demand skills applicable to multiple areas (e.g. digital skills). Skills Bootcamps are co-designed with employers, providers, and local authorities to respond to skills shortages, and course subjects vary according to needs in each local area. In 2021-22, 16 120 people participated in Skills Bootcamps, with further expansion of learner numbers planned in the coming years covering multiple subjects.

Skills Bootcamps in the digital field are delivered both online and in-person in a range of subjects, including digital marketing, software engineering, cloud services engineering, coding, social media and digital leadership and cyber security (Department for Education, 2021[16]). Further expansion is planned for digital Skills Bootcamps.

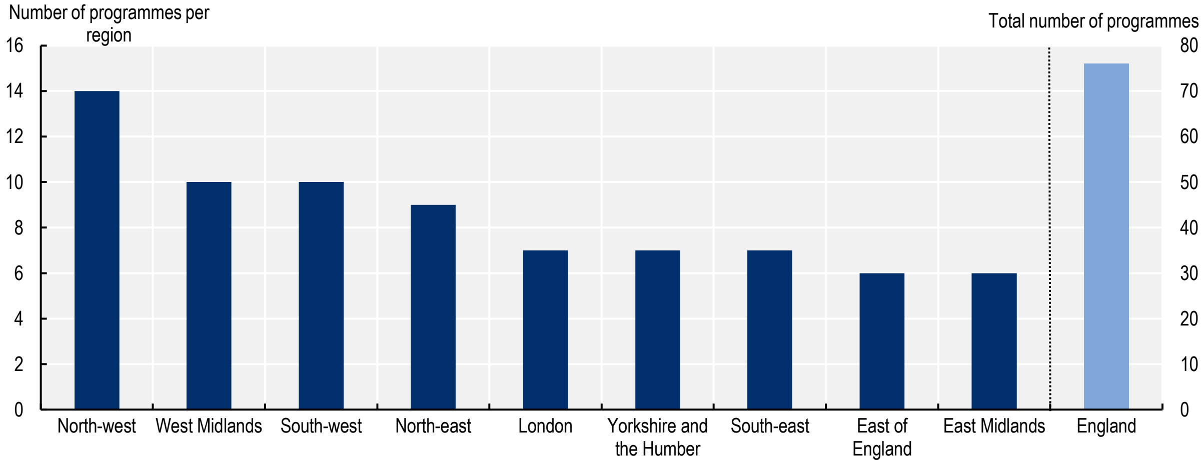
Within cyber security Skills Bootcamps, a range of subjects is covered, including 'cyber technician', 'cyber security', 'cyber technologist', 'cyber security operations and technology', 'networking and cyber security'. This type of training aims to promote an understanding of the core principles and knowledge involved in providing a secured business, responding to cyber incidents, reducing the risk of data breaches or managing cyber threats (see some examples in Table 3.7). Cyber security Skills Bootcamps are available across the country, with the largest numbers being offered in the North-west (e.g. Chester) and West Midlands (e.g. Birmingham) and South-west (e.g. Cheltenham) (See Figure 3.7).

Table 3.7. A sample of Skills Bootcamps in cyber security available in 2022

Course	Description	Provider
Skills Bootcamp in cyber security fundamentals	A flexible 8-week course in cyber security fundamentals for learners looking to upskill or change their career path to a growing area by learning about the modern cyber security landscape. Learners will develop knowledge in areas such as the cyber threat landscape, organisational cyberculture, incident response, and digital forensics.	Aston University
Skills Bootcamp in cyber security	The primary objective of this Skills Bootcamp is to promote an understanding of the core principles, knowledge, behaviours and skills involved in providing, managing and sustaining an environment that facilitates Secure Business Operations. This Skills Bootcamp will also aim to focus on an awareness of the impact of Cyber Security issues on businesses, the communities in which they operate, and other more significant global problems.	Purple beard LTD
Skills Bootcamp in cyber security (cyberoperations)	This 16-week online course covers in-depth knowledge, hands-on experience and skills in Cyber Security. It is designed to help Security Analysts working in a Security Operations Centre successfully handle their tasks, duties and responsibilities. This Skills Bootcamp allows learners to understand different cyber security threats, reduce the risk of data breaches and device compromise, effectively use up-to-date cyber security protection mechanisms, and improve their cyber security practices.	Birmingham city university

Source: Websites of the following providers: Aston University (https://www.aston.ac.uk/study/courses/skills-bootcamp-cyber-security-fundamentals), Purple beard LTD (https://purplebeard.co.uk/individuals/skills-bootcamp/cyber-security/), and Birmingham city university (https://www.bcu.ac.uk/courses/cyber-security-short-course). Information retrieved on 30 October 2022.

Figure 3.7. Number of Skills Bootcamps in cyber security available in England, by region in 2022



Note: This figure includes in-person and online Skills Bootcamps. For online programmes, the region is defined by the provider's location.
Source: Department for Education, https://www.gov.uk/government/publications/skills-bootcamps-training-providers.

Online learning and short courses

Beyond bootcamps, the non-formal education and training sector includes a wide range of low-cost or free online modules and courses that individuals can undertake in their own time. Whilst these modules may not always contain a direct certification, they provide interesting and accessible opportunities for skills development and could facilitate access to further training.

Universities and FE colleges have also expanded their portfolio of non-formal training programmes providing online or blended courses through their website (e.g. University of Manchester) or joining existing platforms (e.g. the University of London in Coursera), especially for courses on digital skills. The list of online courses on digital skills offered through online platforms is long, and a comprehensive overview of those courses falls outside the scope of this study. Nonetheless, Box 3.2 provides some insights based on information from the most popular e-learning platforms in the United Kingdom.

Further, many dedicated cyber security training organisations have been set up in the England in recent years to help grow the cyber security recruitment pool through non-formal training. For example, Immersive Labs provides an interactive training platform for cyber security skills, with hands-on gamified labs that enable new and experienced individuals to learn new capabilities (Immersivelabs, 2022[17]). Another example is CAPSLOCK, which offers a cyber academy model for re-training individuals in a new cyber security career. With an Income Share Agreement, individuals only have to repay their tuition costs once they earn over GBP 27 000 per annum. This model requires a 16-week full-time or 26-week part-time programme. In 2021, CAPSLOCK intended to reskill 200 adults into cyber security (CAPSLOCK, 2022[18]).

Box 3.2. Online courses in digital skills: Insights from e-learning platforms

Looking at the most popular e-learning online platforms in the United Kingdom (Coursera, EdX, LinkedIn Learning, Udemy, FutureLearn and Skillshare) (Hosting Data UK, 2022[19]), the number of online courses offered in digital skills or computer science reaches almost 20 000 (See Table 3.8). 40% of the total provision of online courses is in the digital field. In cyber security, the options are more limited. Udemy is the online platform that hosts most cyber security online courses (4 898 courses available at the moment of the search in September 2022), and they are available at different levels, prices, and estimated times for completion. Learners with no experience in the field can enrol in courses such as 'The beginners guide to practical cyber hacking skills' or 'Essential concepts in cyber security'. For learners with more experience, there are options such as 'Networking cyber security advanced' or 'Cyber security CCE certification'.

Table 3.8. Online short courses offered in English on a selected set of e-learning platforms

Online training provider / Platform	Total number of training courses (approx.) *	Total number of courses offered in digital skills and computer sciences	% Out of the total number of courses offered	Total number of courses offered in cyber security	% Out of the total number of courses offered in computer sciences
Coursera	4 600+	3 491	76	124	4
EdX	3 000+	349	12	58	17
LinkedIn Learning	16 000+	4 113	26	530	13
Udemy	97 000+	10 000	10	4 898	49
FutureLearn	3 100+	335	11	46	14
Skillshare	20 000+	960	5	NA	NA
Total*	143 700+	19 248	40	5 656	31

Note: The numbers for digital and computer science and cyber security were retrieved from each platform course finder. The filters available by default were used for the number of digital and computer science courses. For the number of cyber security courses, "cyber security" word combinations were used in each platform's search engine after filtering by digital and computer science fields.
Source: Information collected online directly from providers' platforms on 23 September 2022. The total number of training courses is taken from multiple websites: Coursera and Udemy information comes from https://www.thinkimpact.com/; Think Impact (2021[20]), Skillshare review, https://www.thinkimpact.com/skillshare-review/; EdX (2021[21]), Accelerating our movement: 2021 EdX impact report, https://www.edx.org/assets/2021-impact-report-en.pdf; and LinkedIn learning (2022[22]), Workplace Learning Report – The transformation of learning and development, https://learning.linkedin.com/resources/workplace-learning-report; information comes from their website and statistics reports.

Education pathways to cyber security entry-level jobs

As described above, various pathways in FE, HE and non-formal education can lead to an entry-level job in the cyber security field. These can be classified into two types of cyber security training pathways that learners can take depending on their prior experience and education. The first group, referred to as the 'entry point to cyber security training', is usually undertaken by individuals with no experience and knowledge of either cyber security or any related field (e.g. computer science). This group contains all the formal and non-formal courses on cyber security or computer sciences (including general digital skills) that contain modules on cyber security, including Level 3 FE courses, intermediate apprenticeships and most bootcamps. The programmes that require no previous education and experience usually lead to generalist IT roles with cyber security tasks or responsibilities or to cyber security apprenticeships or traineeships (see Table 3.9). This indicates that cyber security education and training programmes generally require some initial ICT/cyber security knowledge or expertise. Initial cyber security training, such as a Level 3 programme or certain cyber security bootcamps, may be insufficient for an entry-level cyber security role.

The second group can be referred to as 'training pathways to advance in cyber security career' and includes all the cyber security education and training programmes that require some previous knowledge and experience in cyber security and computer science. Courses in this group allow students to consolidate their cyber security knowledge or specialise in more specific subtopics within this field. This includes higher technical qualifications and similar training (Level 4/5), bachelor's degrees, masters or PhD programmes, and advanced and degree apprenticeships. This group can also include bootcamps that provide more specialised advanced training.

Table 3.9. Cyber security training leading to entry-level jobs in cyber security

Pathways	Description	Entry-level job examples
Intermediate apprenticeship	Level 2 and 3 generalist courses in ICT are usually required to enrol in an intermediate apprenticeship programme in cyber security. Students taking this route are offered a wide range of advanced or higher level apprenticeships, which can lead to an entry-level job in cyber security.	Junior positions, such as Computing apprenticeship, Software analyst, apprenticeship Systems engineer, apprenticeship IT, Network engineer apprenticeship, Cyber security apprenticeship
Further education Level 3	After pursuing secondary education, students can opt to enrol in FE training. Students can take Level 3 qualification courses (e.g. T-levels, etc.). Few students go straight from an FE institution to an entry-level job in cyber security. Students in this route are generally able to take up generalist IT positions or cyber security support or trainee positions.	Generalist IT roles, such as Technical support, Junior developer, Trainee IT security analyst
Bootcamps	Bootcamps (Skills Bootcamps and commercially delivered bootcamps) and other non-formal training are available at different difficulty levels. Usually, learners from cyber security bootcamps continue to further studies in the field. Students in this route are generally able to take up generalist IT positions or cyber security support or trainee positions. Since most cyber bootcamps offered in England respond to specific employer skills required to fill a position, students may take up generalist IT positions with cyber security-related tasks or responsibilities.	Generalist IT roles, such as Technical support, Junior developer, Trainee IT security analyst

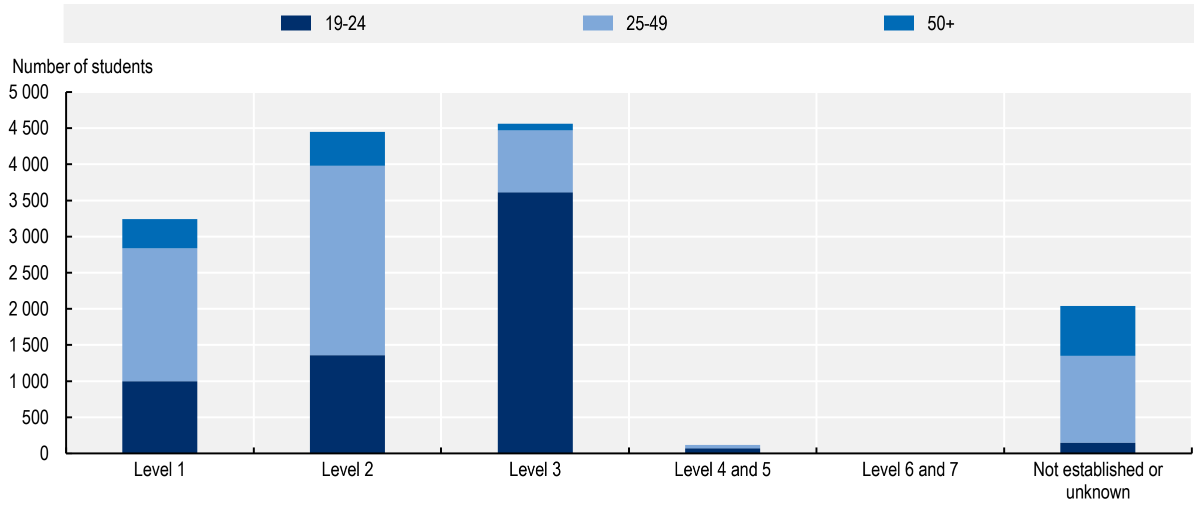
Source: Adapted from DCMS (2019[7]), The role of FE and HE in cyber security skills development, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767425/The_role_of_FE_and_HE_in_cyber_security_skills_development.pdf.

The profiles of cyber security learners

Young and adult learners in cyber security programmes

Cyber security education and training programs are available for learners of all ages and with varying ICT skills and experience levels. Looking at the "ICT practitioners" field, which includes cyber security courses, much of the FE enrolment is concentrated among 19 to 24-year-olds (42% in 2020-21). Most of the learners from that age group are enrolled in programmes at Level 3, where this age group accounted for 80% of the total enrolment in 2020-21. As described above, these Level 3 programmes are more specialised than those offered at lower levels. Furthermore, young learners are more likely to engage with advanced ICT training in FE at Levels 4/5 and 6/7 than their older counterparts – although the absolute numbers remain very low. Among those who participate in more advanced FE 'ICT practitioners' training, 62% are young students (out of 130 learners).

Figure 3.8. Enrolment in ‘ICT practitioners’ FE programmes in 2020-21, by the level of qualification and age group



Note: Volumes are rounded to the nearest 10. The data include Apprenticeships, Community Learning, and Education and Training provisions taken at General Further Education Colleges (including Tertiary), Sixth Form Colleges, Special Colleges (Agricultural and Horticultural Colleges and Art and Design Colleges), Specialist Colleges and External Institutions.
Source: UK Department for Education, https://explore-education-statistics.service.gov.uk/data-tables/permalink/5ac27a8f-1413-4b14-c759-08dac7ae389f.

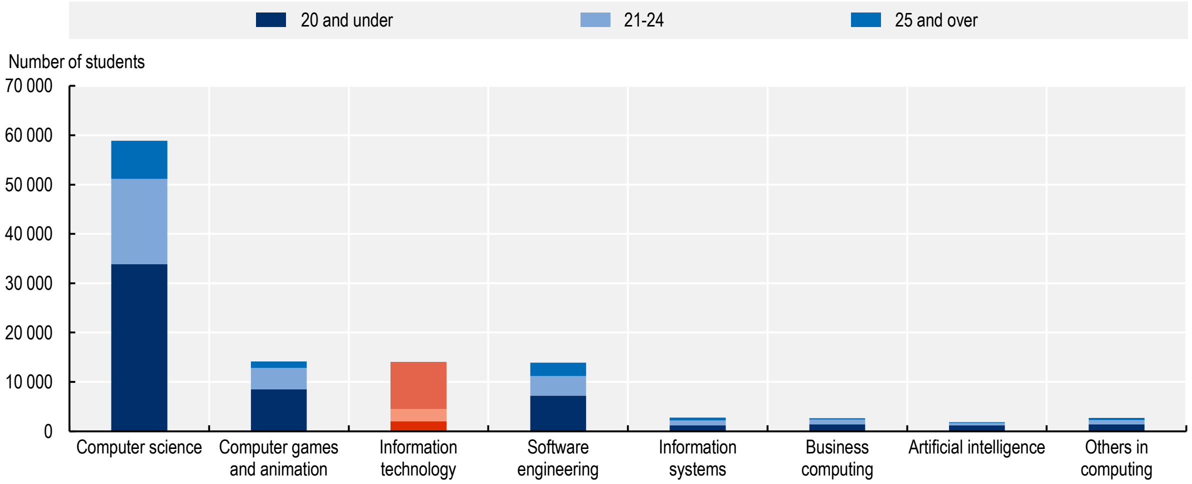
Compared to 2015-16, the number of young learners participating in FE ICT training programmes has increased by 15%, which may reflect the efforts of the UK Government to attract more young people into digital and cyber security careers (DCMS, 2018[23]). Since 2016, the DCMS, jointly with the National Cyber Security Centre (NCSC), has put in place initiatives for strengthening the national curriculum for 4-16 years old to provide young people with the initial building blocks required for more technical careers, developing broader digital skills that are increasingly vital to engaging and working in cyber security (DCMS, 2018[23]).

The vast majority of adults aged 25 or older are in FE training programmes offered at Level 1 and Level 2: in 2020-21, 8 820 adults aged 25 or older participated in ‘ICT practitioner’ courses, of which 65% in Level 1 and 2 training programmes (see Figure 3.8). Most courses offered at Levels 1 and 2 focus mainly on foundations in ICT – which can be essential for greater ownership of learning in higher-level courses. For example, Pearson Education Ltd., an independent training provider, offers an Introductory Information Technology course (Level 1), completion of which is a requirement for the Level 3 cyber security course offered by the same provider.

Enrolment in higher education undergraduate programmes in cyber security-related fields is more concentrated among older cohorts, possibly indicating the need for previous experience, knowledge or a specific level of ICT skills in the field. More than 9 500 students aged 25 or older enrolled in information technology programmes (which include cyber security), accounting for 67% of the entire enrolment in this field. This contrasts with what can be observed in other computing programmes, where the share of learners aged 25 or older in total enrolment equals 15% on average (see Figure 3.9). Programmes such as ‘computer science’ (57%) and ‘software engineering’ (52%) have a significantly higher proportion of young people (below 25) than information technology programmes (32%).

Figure 3.9. Enrolment in computing fields in higher education, by age group and field

Number of students in undergraduate computing programmes



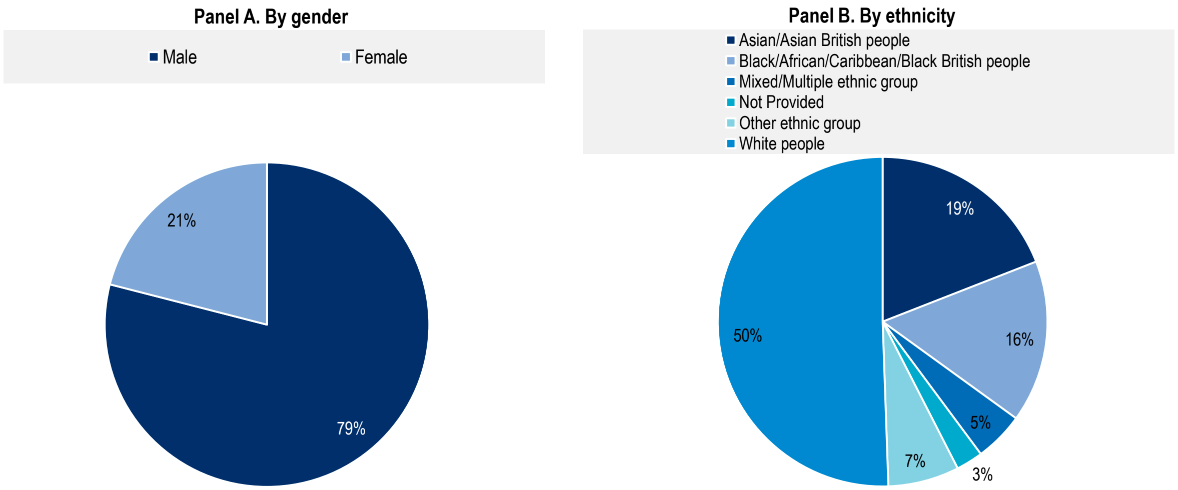
Note: All students enrolled in higher education in programmes below the master's level with Common Aggregation Hierarchy CAH equal to "11" referring to 'Computing' are included in this figure. 'Information technology' contains cyber security related fields.
Source: HESA, https://www.hesa.ac.uk/data-and-analysis/students/what-study/characteristics.

Bootcamps, in general, are designed particularly for individuals looking to upskill or reskill, including in cyber security. According to consulted stakeholders, the age profile of learners in these programmes is very diverse. Moreover, there is also large diversity in the occupational status of learners and their level of expertise. For instance, in cyber security Skills Bootcamp programmes provided by Generation, an independent training provider, most students are unemployed or with no experience in the cyber security sector but willing to acquire sector-relevant skills and participate in the recruitment process (Generation, 2022[24]). Conversely, SANS, an independent training provider, offers an "Upskill in cyber" bootcamp, a commercially delivered bootcamp in cyber security, to learners who are new to cyber security but have the knowledge and skills necessary for a practitioner in key areas of computer, information and software security (SANS, 2022[25])

The diversity of the learners in cyber security education and training programmes

Women and ethnic minorities are underrepresented in ICT education and training programmes, with cyber security programmes likely having a similar distribution as the broader ICT field. In FE, the proportion of females in the ICT field is only 21% (see Figure 3.10). ICT has the lowest share of female learners compared to other STEM fields. The share of Black and Asian learners in this field is 16% and 19%, respectively (see Panel B of Figure 3.10), which is relatively low compared to FE in general (18 and 23%, respectively, in 2021/22). Consulted stakeholders confirmed that cyber security education predominantly enrols white and male learners. This reflects the persistence of stereotypes and sociocultural factors that undermine cyber security roles among both girls (IET, 2018[26]) and young people of colour in the United Kingdom (Royal Society, 2020[27]), in addition to inequities that are perpetuated in the workplace through sizeable pay gaps between women and men in STEM jobs and across racial and ethnic groups (Fry, Kennedy and Funk, 2021[28]). It highlights the need to break stereotypes and tackle entry barriers (e.g. financial constraints).

Figure 3.10. Distribution of the enrolment in 'ICT practitioners' programmes in FE, by students' characteristics in 2021/22



Panel A. By gender

Panel B. By ethnicity

Note: The data include Apprenticeships, Community Learning, and Education and Training provision taken at General Further Education Colleges (including Tertiary), Sixth Form Colleges, Special Colleges (Agricultural and Horticultural Colleges, and Art and Design Colleges), Specialist Colleges and External Institutions.

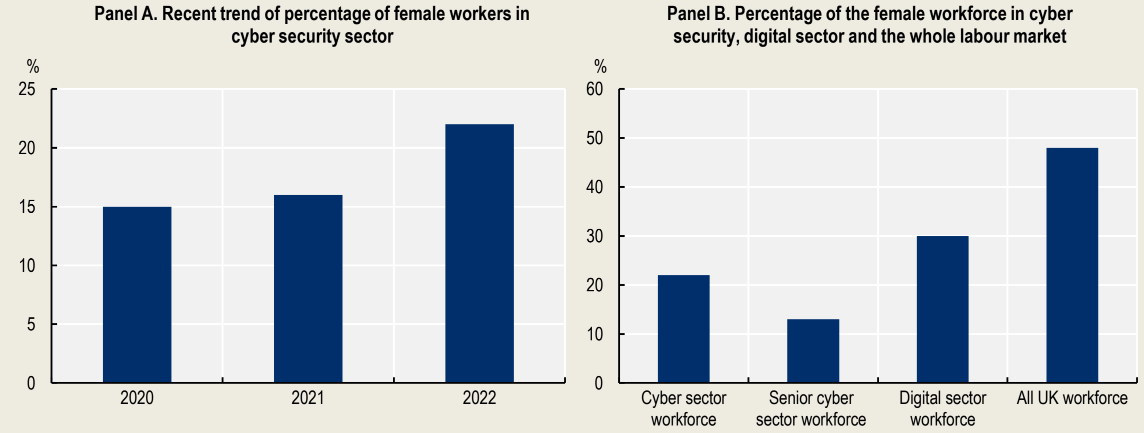
Source: UK Department for Education, https://explore-education-statistics.service.gov.uk/data-tables/permalink/998fe7ef-45cc-44ab-c7ac-08dac7ae389f.

The lack of diversity in cyber security education and training enrolment is similar to what is observed in the related occupations in the labour market, especially for gender. The cyber security workforce in England is mostly male: in 2021, 78% of cyber security professionals were men. There is evidence that overall cyber security sector diversity has improved (both in terms of gender and ethnicity); however, it remains behind overall digital sector in this regard (DCMS, 2022[29]). The cyber security profession is becoming more diverse in multiple dimensions. The proportion of women, ethnic minorities and people from a low socio-economic background in the cyber security workforce has increased in recent years (See Box 3.3), mainly due to policies and strategies implemented by the UK Government. For instance, In 2021, the government mandated the creation of the UK Cyber Security council, an institution that has been focused in identifying and promoting best practices and policies to increase outreach and diversity in the cyber security profession (UK Cyber Security Council, 2023[30]).

Box 3.3. Diversity in the cyber security profession

In terms of gender diversity, the cyber security sector has improved over the course of the last three years in England (DCMS, 2022[29]). Yet, women remain underrepresented in this sector. In 2022, the share of female workers in the cyber security sector was 22%, higher than in 2020 (15%) (See Figure 3.11, Panel A). In terms of the senior workforce (i.e. with 6+ years of experience), the lacks gender diversity in the cyber security field is even more outspoken: only 13% of the senior professionals workers in this field are female. Cyber security remains behind other digital sectors regarding gender diversity(See Figure 3.11, Panel B), as the proportion of women working in the digital industry is 30%.

Figure 3.11. Share of female workers in the cyber security field



Source: DCMS (2022[29]), Cyber security skill in the UK labour market 2022, https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2022; DCMS (2021[31]), Sector Economic estimates 2021: Employment 2019 to June 2021, https://www.gov.uk/government/statistics/dcms-sector-economic-estimates-2021-employment-2019-to-june-2021.

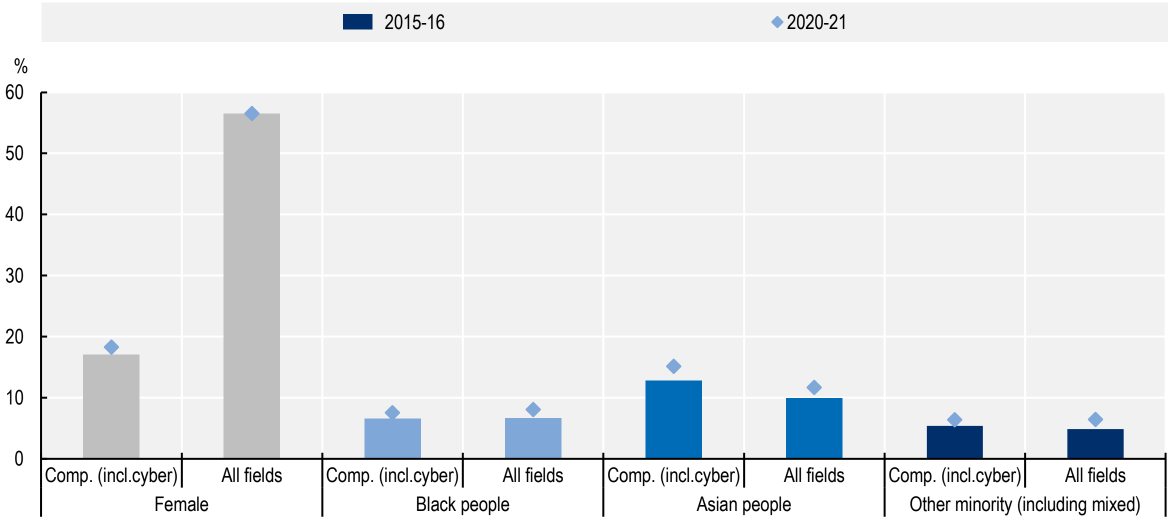
With respect to other underrepresented groups, the proportion of ethnic minorities working in the cyber security sector has increased in recent years, going from 16% in 2020 to 25% in 2022. Notably, the cyber security sector has done a better job at integrating workers from ethnic minorities than the digital sector. The share of ethnic minorities in the digital sector workforce is only 15% (DCMS, 2022[29]). In terms of socio-economic diversity, in 2021, 16% of the cyber security workforce came from a background where they were eligible for free school meals (FSM). This is slightly lower than in 2020 (17%) (NCSC, 2021[32]).

Source: DCMS (2022[29]), Cyber security skill in the UK labour market 2022, https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2022; NCSC (2021[33]), Decrypting diversity: Diversity and Inclusion in cyber security, https://www.ncsc.gov.uk/files/KPMG-and-the-NCSC-Decrypting-Diversity-2021-report.pdf.

Enrolment in ICT fields in higher education echoes what is found in FE. Figure 3.12 shows the percentage of students who identify as female or as a particular race/ethnicity in the computer science field, which includes cyber security. The share of females participating in computer science (18% in 2020-21) is low compared to other fields (57% across all fields in 2020-21). Although the participation of female learners in the field has improved slightly in the last five years (1.3 percentage points more than in 2015-16), computer science is still male dominated. Racial/ethnic minorities account for 24% of total enrolment in computer science, in line with what is observed in other fields. The share of Asian learners is higher in computing programmes than on average across all programmes in HE institutions. Compared to the 2015-16 academic year, the percentage of racial/ethnic minorities has gone up, which may reflect the affirmative action policies implemented in the last years in higher education to expand diversity in computer science (Office for Students, 2022[34]). However, the lack of racial/ethnic diversity in FE and HE remains a challenge not only in the cyber security field but in the entire education system (Oxford University, 2019[35]).

Figure 3.12. Enrolment in computing programmes in higher education institutions, by students' characteristics

Percentage of students in undergraduate programmes



Note: The residual category for gender is male and unknown; unknown accounts for less than 2%. The residual category for ethnicity is 'white people' and 'unknown'; 'Unknown' accounts for less than 3%. All students enrolled in higher education in programmes below the master's level are included in this figure.
Source: HESA, https://www.hesa.ac.uk/data-and-analysis/students/what-study/characteristics.

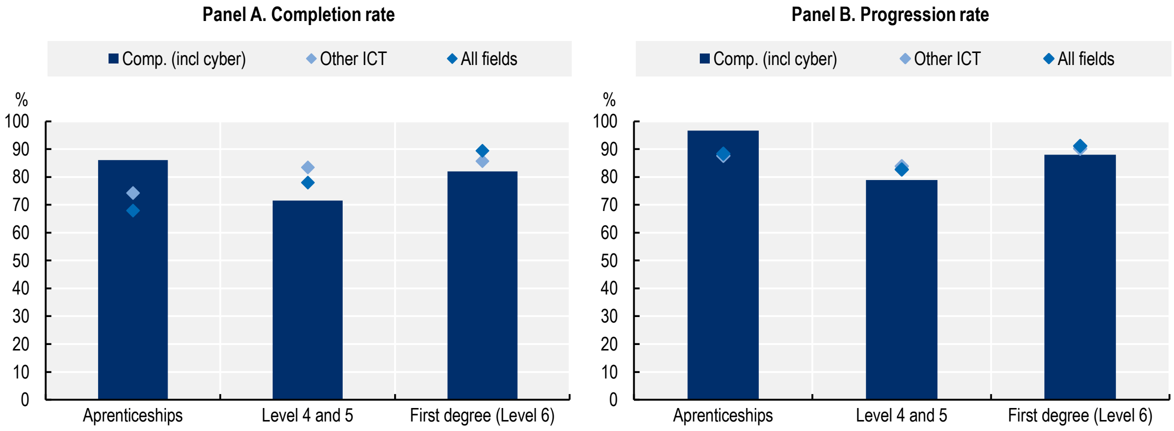
The lack of diversity in the field – particularly for gender – may reflect stereotypes embedded among young people at early ages. Such stereotypes and misconceptions about cyber security careers affect career expectations and, thus, career choice, which may perpetuate current figures in terms of gender diversity in the cyber security profession. Across OECD countries, 15-year-old old boys are more likely to expect to work in science and engineering than girls (OECD, 2019[36]). In 2018, on average across OECD countries, the 'ICT professionals' occupation was among the top three occupations aspired by 15-year-old boys, while for girls it was not among the top 10 (OECD, 2020[37]). These occupational expectation differences by gender have changed little since 2000 (OECD, 2019[36]).

Education and labour market outcomes of cyber security education and training programmes

Looking at computer science students' outcomes, including cyber security programmes, 8 out of 10 students who enrol in computer science education and training complete their studies. Yet, completion rates vary according to the type of training; see Panel A of Figure 3.13. Computer sciences apprenticeships, for instance, have higher completion rates compared to more classroom-based programmes (Level 4/5 and undergraduate programmes). This highlights the relevance of work-based learning in the ICT sector, providing labour market-relevant knowledge and skills of technical and job-specific nature. Additionally, Level 4/5 and undergraduate computer science programmes have a lower completion rate than other ICT programmes. Results from a student survey suggest that the high dropout rate in this field compared to other ICT fields is mainly because students "feel they are not getting enough for their money", lack of enjoyment studying the field, and the field being consider too hard (Tech target, 2019[38])

Figure 3.13. Completion and progression rate in computer science, by type and qualification level

Completion and progression rate during the academic period 2020-21 in England



Note: These figures include information from FE and HE institutions registered in OFS, which account for more than 750 providers in England. Computing contains cyber security programmes. The apprenticeship category consists of Level 4 and Level 6 apprenticeship programmes. The student outcomes data dashboard shows continuation, completion and progression outcomes. The completion measures count as positive outcomes for those students who have either: (a) Gained a higher education qualification from the provider at which they were previously identified as an entrant on or before the relevant census date; (b) –been recorded as actively studying for a higher education qualification at the same provider on the census date. The progression measures count as positive outcomes for those students who report in their response to the Graduate Outcomes survey 15 months after gaining their qualification: (a) paid worker, employer, self-employment, running business, voluntary/unpaid work if it is managerial or professional employment; (b) engaged in training, study or research, travel, caring for someone, or retired. Level 4 and 5 completion rate do not represent all Level 4 and 5 provision and tend to be disproportionately skewed towards higher education providers offering Level 4 and 5 programmes.
Source: Office for Students (OFS), Students outcome data dashboard, https://www.officeforstudents.org.uk/data-and-analysis/student-outcomes-data-dashboard/data-dashboard/.

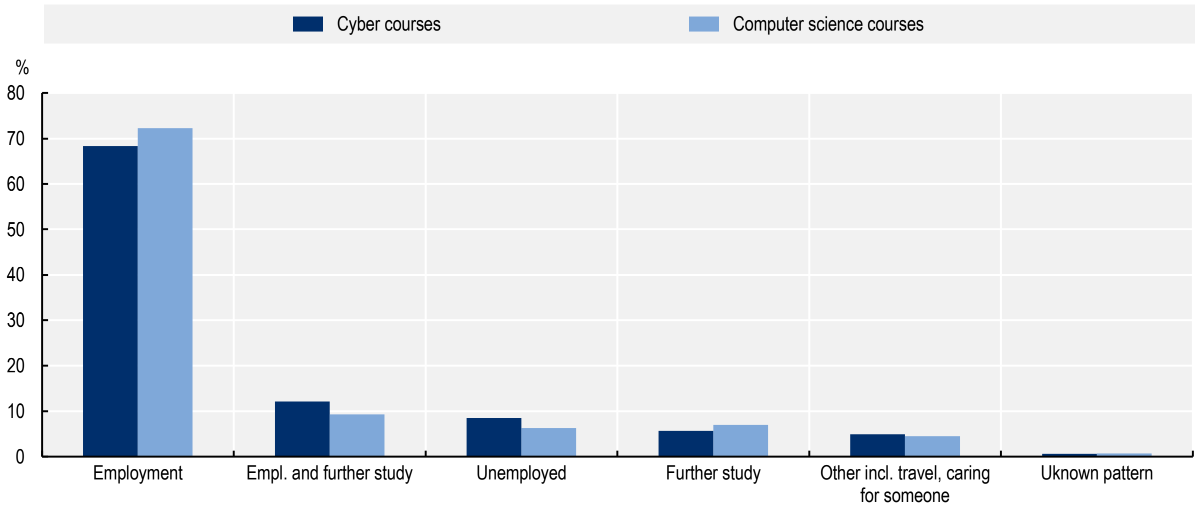
In computer science in general, which includes cyber security education and training programmes, almost nine out of ten students, after completing their degree, enter the labour market or pursue further education. This ratio is the highest for students who complete apprenticeships (97%). Students who complete a first degree (undergraduate programme) have more chances to progress to a positive outcome than those who complete a Level 4 or 5 programme. This may reflect that employers value higher-level degrees more and/or are looking for workers with at least some prior experience in the sector (or related) – which is often a requirement in the Level 6 programmes.

Figure 3.14 shows the outcomes for those who graduated from higher education in 2018/19, approximately 15 months after they completed their studies (i.e. the responses can show activity between December 2019 and September 2020 – before and after the COVID-19 pandemic restrictions in the UK).[8] These figures indicate that approximately 68% of cyber security graduates enter full- or part-time employment, with 12% blending employment and further study. This means that of the 3 600 students who graduated in cyber security courses in 2018/19, 80% were in employment 15 months after obtaining their degree.

Cyber security graduates are slightly more likely to engage with further study than graduates from other computer science courses (DCMS, 2019[7]), which may be linked to the need for regular updating of technical skills and knowledge in a rapidly-changing field in addition to the level of specialisation and specific training required for some of the job opportunities in this field. 18% of cyber security graduates pursue further study (6% full-time further study and 12% combined with employment) compared to 16% of their peers in computer science (see Figure 3.14). This proportion has increased compared to the previous year (15% in 2017-18).

Figure 3.14. Higher education graduate outcomes in cyber security in 2018-19

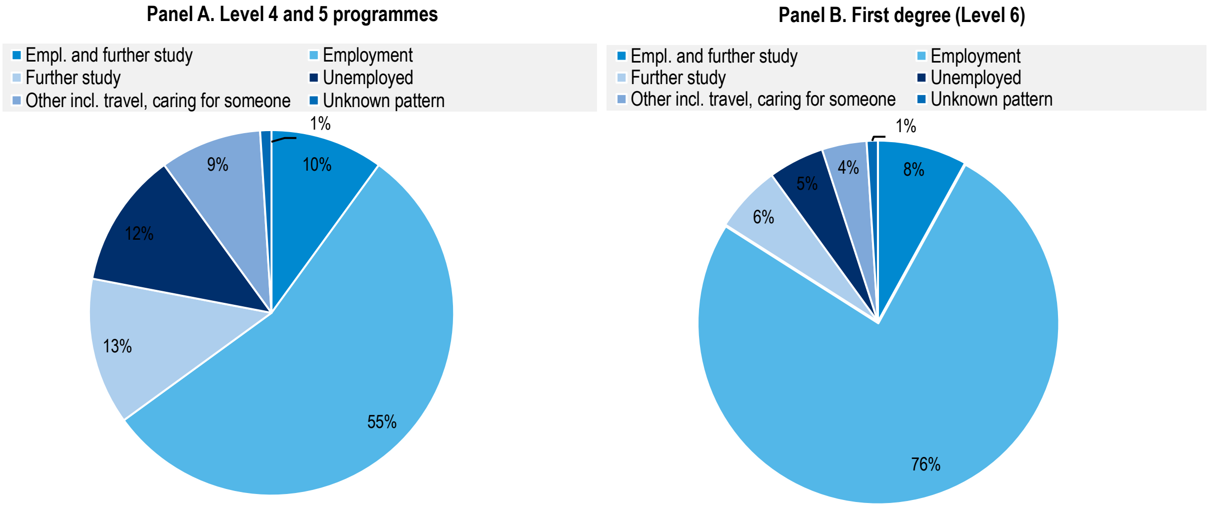
Distribution of graduates by destination after completing studies



Note: Graduates from programmes below the master's level are asked for information about their activities approximately 15 months after they complete their studies, so the responses received can show activity taking place between December 2019 and September 2020.
Source: HESA, https://www.hesa.ac.uk/news/18-06-2020/sb257-higher-education-graduate-outcomes-statistics.

Looking at outcomes of recent graduates in computer sciences by level of qualification, which includes cyber security graduates, the share of Level 6 graduates in employment (including those in work and further study) is significantly higher (84%) than those from Level 4-5 programmes (65%) 15 months after obtaining their qualification (see Figure 3.15). Level 4-5 computer science graduates have more chances to pursue further studies (without work) (13%) than Level 6 graduates (6%) but are also more likely to be unemployed (12% vs 5%).

Figure 3.15. Higher education graduate outcomes in computer science, by level of qualification in 2018-19

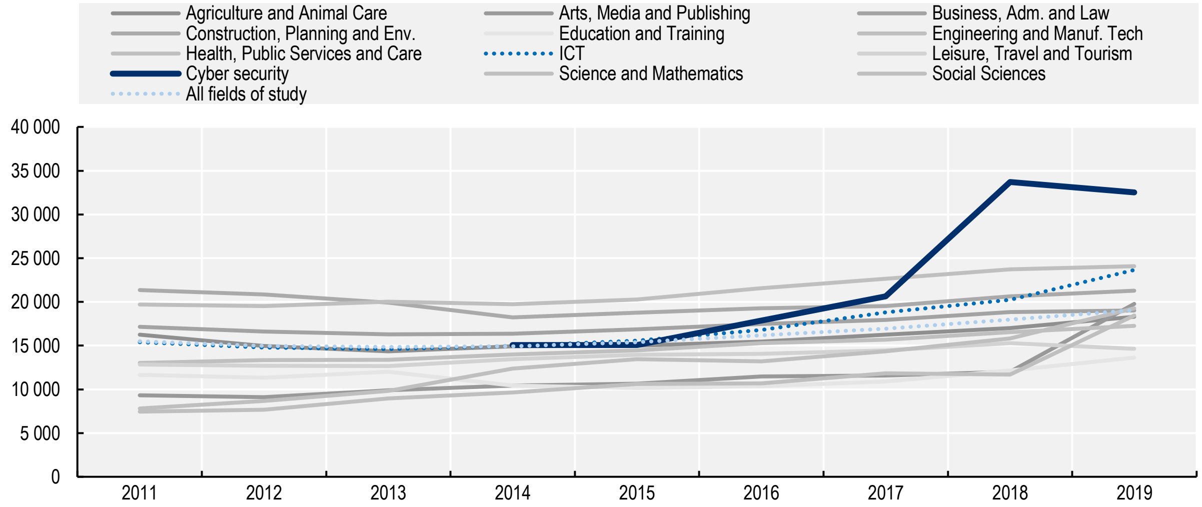


Note: Graduates are asked for information about their activities approximately 15 months after they complete their studies, so the responses received can show activities taking place between December 2019 and September 2020.
Source: HESA, https://www.hesa.ac.uk/news/18-06-2020/sb257-higher-education-graduate-outcomes-statistics.

The earnings potential in this field is high, even at entry-level positions. This signals the high demand for professionals in the cyber security field. Figure 3.16 shows the evolution of the average annual earnings one year after finishing a Level 6 (first degree) training programme. According to these data, the yearly earnings of ICT graduates have increased by 54% between 2011 and 2019. In cyber security, this increase has been even stronger: since 2014, the annual earnings of recent graduates have doubled from GBP 15 000 per year in 2014 to GBP 32 000 in 2019. Cyber security salaries vary depending on experience level and role. Table 3.10 shows annual earnings for selected cyber security roles by years of experience. For instance, penetration testers have the lowest annual earnings among the ten cyber security roles with available data when workers have less than two years of experience (GBP 30 000), and at the same time have among the highest yearly earnings when workers have more than five years of experience (GBP 105 000).

Figure 3.16. Evolution of cyber security first-degree annual earnings compared to other fields

Median earnings of graduates one year after obtaining their first degree (Level 6) in GBP



Note: This figure shows median earnings (real wages) across HEIs one year after graduation of UK-domiciled male and female first-degree (Level 6) graduates from HEIs. Cyber security programmes were identified using HECoS codes for 'Computer and information security'.
Source: UK Department for Education, https://explore-education-statistics.service.gov.uk/find-statistics/graduate-outcomes-leo-provider-level-data.

Table 3.10. Annual earnings for selected cyber security roles by years of experience in 2022

Median annual earnings in GBP

Cyber Security Role	1-2 Years of Experience	3-5 Years of Experience	5+ Years of Experience
Governance, Risk and Compliance (GRC)	43 700	56 500	85 000
Security Operations Center	45 000	65 000	90 000
Security Engineering	45 000	65 000	90 000
Security Architecture	70 000	84 000	97 000
Cloud Security	55 000	66 000	81 000
Information Security Management	71 500	90 500	120 000
Application Security	31 000	82 000	122 000
DevSecOps	76 000	89 000	115 000
Penetration Tester	30 000	47 500	105 000
Chief Information Security Officer (CISO)	110 000	150 000	200 000

Note: The salary guide provides the median salaries across ten major job roles in the sector according to experience.
Source: Infosecurity group, https://www.infosecurity-magazine.com/news/large-salary-rises-cyber security/.

Information on outcomes of non-formal education and training is limited. However, since the introduction of Skills Bootcamps in September 2020, starting with the digital sector, the DfE has compiled some figures in this area. Out of 2 550 applicants, 822 learners participated in digital Skills Bootcamps, including cyber security courses, during the academic year 2020-21 (Department for Education, 2021[16]). Providers collected participation indicators, such as whether learners dropped out early or completed the course, completed all their assessments and assignments, and passed all their assessments. Table 3.11 shows that the average attendance rate of digital Skills Bootcamps was 64%. Nonetheless, 84% of learners completed all their assessments and assignments, and 81% successfully passed their assessments, meaning that even though attendance did not appear very high, a large proportion of learners still managed to complete their courses and meet the planned learning outcomes successfully. Even though most learners actively engaged with the assignments and passed their assessments, 11% dropped out of their courses before completion.

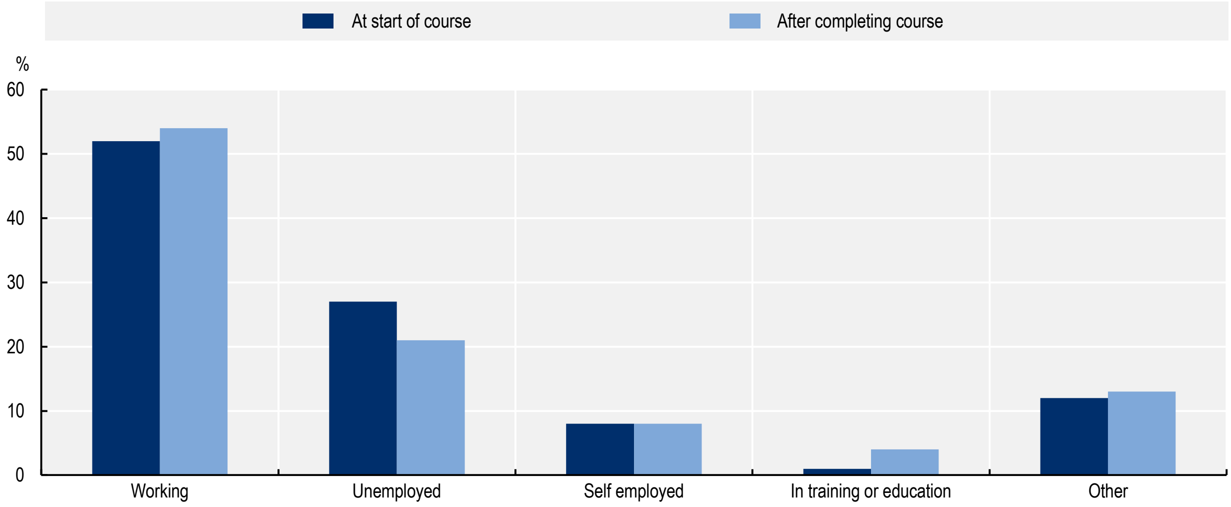
Table 3.11. Digital Skills Bootcamps participation indicators (2020)

Indicator	Percentage
Average attendance rate	64%
Completed all assessments/assignments	84%
Passed all assessments	81%
Exited course before completion	11%

Note: Average attendance rate is relative to the total number of participants. The proportion of students that completed all assessments passed all assessments, and exited the course before completion is relative to the average attendance.
Source: Department for Education (2021[16]), Skills bootcamps process evaluation, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1027163/Bootcamps_wave_1_final_evaluation_report.pdf.

Digital Skills Bootcamps participants improve their outcomes after finishing their training on average (see Figure 3.17). At the start of the training, 27% of participants were unemployed, which fell to 21% once the course was completed – with a higher proportion of learners in employment (54%) and in training or education (4%). Among those who reported working after completing a course, the vast majority (89%) indicated their current job was the same as the one they held when they started the course, while 11% changed jobs.

Figure 3.17. Changes in employment status of digital Skills Bootcamps participants before and after the course (2021)



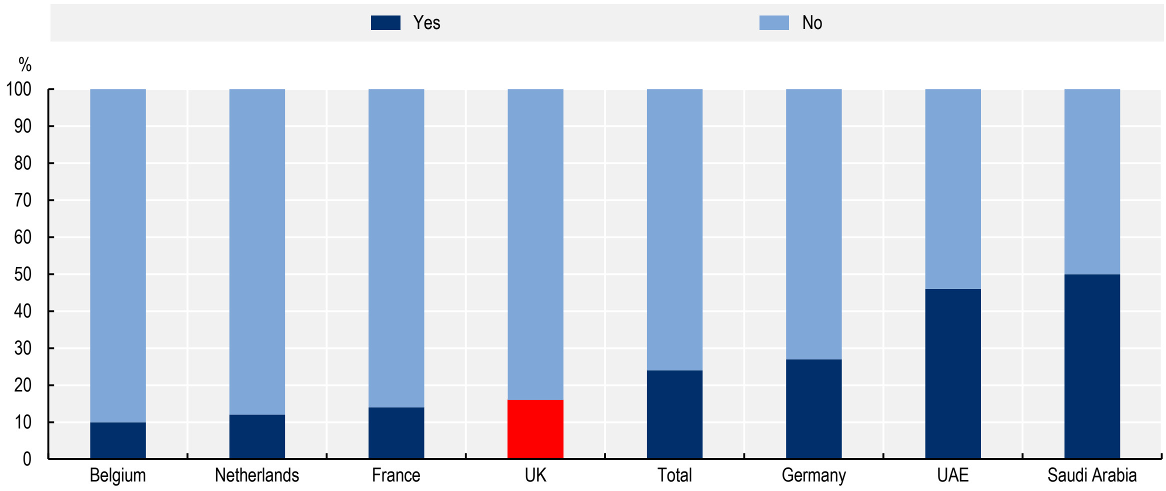
Note: Other category includes 'Caring responsibilities' and 'Waiting to start work'. 'Retired' and 'Not answered'. Based on the learner's survey. The number of respondents was 354.
Source: Department for Education (2021[16]), Skills Bootcamps process evaluation, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1027163/Bootcamps_wave_1_final_evaluation_report.pdf.

Inclusion and flexibility of cyber security programmes and training

As highlighted above, enrolment in cyber security programmes in England remains relatively low despite the strong and growing demand for professionals in this field. At the same time, certain groups of learners are underrepresented in cyber security education and training programmes and careers – in particular female learners. Figure 3.18 shows that only 16% of young people aged 14 to 18 in the United Kingdom report to have considered a career in cyber security. This percentage is relatively low compared to countries such as Germany (27%) or Saudi Arabia (50%). One of the potential reasons for the limited enrolment and interest in the field is that some individuals may have a limited understanding of cyber security as a field and the related areas of knowledge, which may impede identifying the right training opportunities. Consulted stakeholders state that learners have limited information on the learning pathways directly linked to cyber security occupations, as well as on the career pathways within the field.

Figure 3.18. Interest in pursuing a career in cyber security

Percentage of students aged 14 to 18 who have considered a career in cyber security



Note: Survey collected in September/October 2018 questioning 4 000 students aged 14-18 across Europe Middle East, and Africa (EMEA). The research explored both awareness of and opinions on cyber security among that age group, as well as, more specifically, asking students for their views on cyber security as a potential career.
Source: SANS EMEA (2018), Survey in cyber security, https://www.sans.org/igen-cyber-security-research-report?msc=PR.

Moreover, the lack of diversity in the sector may affect the enrolment of people from diverse backgrounds. Evidence from the STEM sector suggests that a lack of diversity can be perceived as a hostile environment by prospective learners from these diverse backgrounds (Breda et al., 2021[39]). Role models can provide youth with valuable motivation and information on pursuing their career goals (Valero, Keller and Hirschi, 2019[40]).

Multiple policies and strategies have been implemented in England to overcome these challenges and expand access to cyber security programmes, especially among young and adult learners from different backgrounds. The efforts have been focused on providing clear information about cyber security education and training and careers and guidance on how to engage with the distinct learning pathways available to pursue a career in the field. Similarly, financial incentives and subsidies have been provided to increase participation in cyber security education and training, especially targeting the most disadvantaged young people and adults.

Providing information and career guidance on cyber security programmes

Promoting participation in cyber security education and training requires people to be better informed about the field. Cyber security is a fairly complex and relatively new field; therefore, it requires more effort to inform (prospective) learners about what it entails. Effective career guidance enables people of all ages to develop informed, critical perspectives about the relationship between education and employment, helping them to visualise and plan their transitions through schooling or current jobs and into more attractive work opportunities (OECD, 2019[41]). As described in the previous Chapter, various cyber security roles exist and these can be found across various industries, and this requires supporting students to navigate them. This is especially relevant for newcomers in the field who may find it hard to understand the entry requirements and the competencies needed.

In England, several career guidance initiatives have been set up to support people interested in engaging in cyber security education and training. Some focus on providing targeted career guidance to introduce people from diverse backgrounds, mostly young people, to the cyber security world and the relevant learning opportunities in the field. At early ages, the efforts have been focused on raising awareness about cyber security issues in general and cyber security as a career.

The NCSC leads the implementation of the CyberFirst programmes, designed to identify and nurture a diverse range of talented young people into a cyber security career. CyberFirst includes multiple activities intended to inspire and encourage students from all backgrounds to consider a career in cyber security (NCSC, 2021[33]). This includes ‘CyberFirst courses’, which aim to introduce the young generation to the cyber security world and provide information on the relevant training pathways in this field (see Box 3.4). In 2020-21, more than 4 300 young students participated in these courses, of which 40% were ethnic minorities and 55% were females. For older cohorts, CyberFirst includes a scheme oriented to complement career education available in schools and colleges through the CyberFirst Schools/Colleges programme, which aims to encourage young people to engage with computer science and the application of cyber security in everyday technology use (see Box 3.4).

Multiple websites and platforms are available to provide young people and adults with relevant information about the cyber security sector. They play an important role in improving the understanding of the field and facilitating participation in cyber security learning opportunities (see Table 3.12). One interesting tool comes from the UK Cyber Security Council, the self-regulatory body for the UK’s cyber security profession that is in charge of developing, promoting, and awarding nationally recognised standards for cyber security in support of the UK Government’s National Cyber Security Strategy to make the UK the safest place to live and work online. The Council has developed a portal, ‘the careers route map’, which provides details about the 16 specialisations in cyber security and suggests pathways into, through and between them. Currently, the Council is mapping all the initiatives offered at the national and sub-national levels that seek to diversify the cyber security profession (including supporting more neurodiverse workers into the profession, increasing the number of women and facilitating non-traditional routes). The objective is to develop a website that centralises this information to make it accessible to users that can benefit from these initiatives.

Some initiatives take a more general approach by providing relevant labour market information about priority sectors – including cyber security – to inform young people and adults about jobs and learning. Several career guidance services in England, while typically sector and occupation agnostic, provide relevant information on labour market needs and training opportunities, especially at the local level. Since 2019, the National Careers Service has worked with Sector Delivery Lead (SDL) departments[9] to provide information that best reflect labour market needs. A key principle of careers information, advice and guidance is that it works in the best interests of the individual, and the DfE’s National Careers Service and Careers & Enterprise Company can help industry sectors to disseminate key information to career leaders in schools/colleges and careers advisers in the community. This is a joint partnership as it requires input from industry to ensure that content is accurate and up to date.

Box 3.4. CyberFirst: Introducing young people to the cyber security world

CyberFirst is a programme led by NCSC which aims to develop the UK's next generation of cyber security professionals through bursaries, free courses for 11-17 year-olds and competitions. The programme provides opportunities for young people to explore their passion for tech applied to the fast-paced cyber security sector. This programme was created as part of the NCSC's mandate, established through the initial cyber security skills strategy (HM Government, 2016[42]), to support young people to pursue a career in cyber security. CyberFirst covers a broad range of activities:

- **Cyber Explorers** (Cyber Explorers, 2023[43]) is an immersive, gamified learning experience showcasing how the skills taught in classes are linked to real-world situations. This initiative aims to raise awareness about the importance of (basic) ICT skills, including cyber security skills (e.g. data protection, phishing, etc.). Through a mix of engaging activities (e.g. games, quizzes, puzzles, challenges), young people learn how to broaden their thinking, make smarter choices and develop essential cyber security skills. The activities aim to help young students discover how digital, computing and cyber security skills are integral to successful career paths in cyber and other ICT-related careers.
- **CyberFirst courses** (NCSC, 2022[44]) are designed to introduce the young generation to the world of cyber security. Trailblazers and Adventurers courses provide insights into how Computer Science can play a key role in future career prospects and highlight the varied roles and jobs that exist and involve technology in the workplace. These courses are aimed at students who have not yet made their GCSE choices so that they get the opportunity to see how studying computer science could potentially augment and enhance their future career paths. Defenders, Futures and Advanced courses build more advanced cyber security skills, such as building and protecting small networks and personal devices, implementing digital forensics and understanding penetration testing.
- **CyberFirst Schools and Colleges** (NCSC, 2022[45]) programme is a scheme to recognise schools and colleges that provide a structured approach to excellence in cyber security education. Schools and colleges participating in this scheme have the opportunity to engage with local and national companies seeking to invest time, expertise and resources in promoting cyber security education. They also become focal points for other CyberFirst activities.
- **The CyberFirst Girls Competition** (NCSC, 2022[46]) aims to support girls interested in a career in cyber security. This NCSC's flagship cyber security contest for schools opens annually to girls across the United Kingdom. The aim of the competition is to introduce young girls to the world of cyber security and inspire them to consider careers in this industry.

CyberFirst also offers students support to progress to cyber security undergraduate programmes in higher education through **CyberFirst Bursary** (NCSC, 2022[47]), financial assistance of GBP 4 000 per year and paid cyber security training each summer to help kick start their career in cyber. This initiative is for young people who do not necessarily have a background in coding but care about technology and are willing to learn about computer science.

Source: NCSC (2022[48]), CyberFirst overview, https://www.ncsc.gov.uk/cyberfirst/overview.

Moreover, the National Careers Service offers multiple industry- and occupation-specific resources and tools for youth and adults to make more informed education and training decisions. For example, the 'explore careers' portal provides detailed information by occupation, including cyber security professionals, on expected salary, the ways to get into this role and its skills requirements. The website also lists the current education and job opportunities available.

Table 3.12. A sample of websites and platforms providing relevant information on the cyber security field

Platform/Website	Description
Cyber security career route map (UK Cyber Security Council)	This website provides detailed information about the different areas of specialisation in cyber security. It also suggests learning pathways for individuals interested in a specific field. The information shown for each area of specialisation includes characteristics of the role, skills and knowledge required and helpful information to enter the specialisation.
Cyber security Skill roadmap (SANS institute)	Interactive training roadmap to find suitable courses for immediate cyber skill development and long-term career goals. The platform is connected to more than 60 courses delivering critical skills in cyber defence, digital, forensics, cloud security, penetration testing, and management practice areas of cyber security.
Institute of Coding website	The Institute of Coding is a collaborative national consortium of industry, educators and outreach providers working together to respond to the UK's digital skills gap through the delivery of employer-led digital skills education. Its website centralises more than 200 courses offered by multiple providers in the digital field, including cyber security.
The Skills Toolkit (National Career Service)	Free courses to help learners get new skills or change jobs. Including general skills that apply to all sectors and more specialised skills.

Source: UK cyber security council careers road map, https://www.ukcybersecuritycouncil.org.uk/qualifications-and-careers/careers-route-map/; SANS cyber security skills road map, https://www.sans.org/cyber-security-skills-roadmap/; The skills Toolkit https://nationalcareers.service.gov.uk/find-a-course/the-skills-toolkit; Institute of Coding website – https://instituteofcoding.org/; National Career Service, The Skills Toolkit, https://nationalcareers.service.gov.uk/find-a-course/the-skills-toolkit.

Overcoming barriers to increase diversity in the cyber security field

Addressing individuals' financial and non-financial barriers is important to boost participation in cyber security education and training, especially among people from vulnerable backgrounds (OECD, 2019[49]).

Cyber security education can be expensive in England. For nationals, tuition fees of formal education courses can range between GBP 3 500 and GBP 9 250 per year depending on the type and level of programme, representing a significant share of individuals' or households' income. Multiple policies and initiatives have been implemented in England to help overcome financial constraints and support participation in cyber security education and training. For instance, high-performing students can apply for a CyberFirst bursary, a programme that provides financial assistance to students interested in studying undergraduate education in cyber security, which also covers cyber security training each summer to help them to start their career in cyber (see Box 3.4). Since 2015, more than 1 000 young people have benefited from this bursary. According to data from the summer training, 47% of beneficiaries identified as female, and 35% as Black, Asian or Mixed (DCMS, 2021[50]).

Subsidised training programmes are also available for adults (aged 19 or older) from diverse backgrounds across England. For example, Skills Bootcamps in the digital field, including cyber security, are offered at no cost to learners. For Skills Bootcamps in which an employer is training their employees, the employer contributes 30% (large businesses) or 10% (SMEs) to the cost of the course. Some commercially delivered bootcamps providers in cyber security implement specific funding schemes to remove financial barriers and expand the enrolment of more disadvantaged learners. For instance, at CAPSLOCK (i.e. a cyber security training provider), learners have the option to attend full or part-time courses and pay nothing up-front. Instead, learners are required to pay back a percentage of their income after completing the course, but only if they land a job with a good salary (See Box 3.5).

Box 3.5. Removing financial barriers to retraining: The CAPSLOCK case

About CAPSLOCK's income share agreement

Commercially delivered bootcamps can be difficult to afford, especially for people from disadvantaged backgrounds. Thus, some training providers offer financing alternatives to their students (besides the subsidies provided by the government). This is the case for CAPSLOCK, a government-backed educational institution focused on re-skilling adults and kick-starting their cyber security career in as little as four months. They provide cyber re-training programmes, delivered online by industry professionals, via a curriculum built around in-demand job roles and employer needs.

CAPSLOCK provides financing options to students to remove the financial barriers to retraining. CAPSLOCK uses a financial model known as an Income Share Agreement (ISA), which gives learners the option to attend the full-time (16 weeks) or part-time (26 weeks) course and pay nothing up-front. Instead, learners are required to pay back a percentage of their income after completing the course, but only if their income exceeds a certain threshold. The ISA model requires that students pay back 13% of their monthly income for 48 months after the course, but only once students earn over GBP 25 000 a year. Students do not pay back more than GBP 19 000, and ISAs are paused if students' income drops below GBP 25 000. The Financial Conduct Authority has backed CAPSLOCK to pilot this model in 2021. This financial model is an alternative for people who need to re-skill but cannot afford up-front fees or traditional loan debt. Students also have the option to pay upfront if they can, in which case the tuition fee amounts to GBP 9 000 (including VAT). There are other funding options too, such as student loans. Among CAPSLOCK's first cohort of 85 students, 77 opted for an Income Share Agreement, meaning over GBP 700 000 in tuition fees were deferred so learners could join with no up-front costs.

About the training and additional support students receive

CAPSLOCK emphasises mentoring and career guidance. Over the duration of the course, learners receive tailored advice about transitioning into the world of cyber and help to find the right role for them. They also access the CAPSLOCK cyber employer network, which features companies keen to interview CAPSLOCK graduates. The course includes four industry-recognised certifications.

Source: CAPSLOCK: Enrol with no up-front costs, https://capslock.ac/the-cost.

Various publicly-funded programmes exist to increase diversity in specific sectors, such as the digital sector. This is, for example, the case for the Mayor's Academies Programme (MAP) developed by the Mayor's Office of London as part of its London Recovery Programme. This initiative aims at supporting the learners who have been the hardest hit by the COVID-19 pandemic into good work in key sectors for recovery and long-term economic growth. The programme co-ordinates quality marks training in London and provides support to help newly skilled people to work in priority sectors. It also builds on the Mayor's Workforce Integration Network (WIN) work to address structural barriers as part of the Mayor's Strategy for Social Integration. The WIN programme supports young Black men aged 16 to 24 years into living wage employment in London. It currently focuses on the construction and digital sectors and will engage other sectors and groups over time.

Another common barrier to training participation is a lack of time due to work and family responsibilities. Such time constraints may affect learners' chances to enrol in cyber security training and therefore call for training opportunities to be compatible with busy working or family life. For these reasons, in 2018, the DCMS launched the Cyber Skill Immediate Impact Fund (CSIIF), which is designed to encourage providers to develop and scale up effective and more suitable initiatives to identify, train and place untapped talent from different backgrounds into targeted cyber security roles quickly (DCMS, 2019[51]). For instance, the training provider QA has created a training programme with Women Tech Jobs to support women's placement into cyber security roles. The programme focuses on women who are heads of household or with family responsibilities wanting to return to work; thus, the classroom training is blended with e-learning and complemented with additional guidance and support (see Box 3.6). Similarly, through CSIIF, the DCMS has also sponsored providers offering cyber security training suitable for neurodiverse learners. For example, Immersive labs, a training provider, has developed *The Neurodivergent Digital Cyber Academy*, designed to help neurodiverse candidates develop their cyber security skills through hands-on practical challenges and courses. Box 3.6 provides more details about these programmes as well as other examples.

Box 3.6. Improving diversity in cyber security: Initiatives from the Cyber Skill Immediate Impact Fund

Youth Fed (Cyber Threat Hub Academy)

Youth Fed is a Cyber Security Operations Centre (SOC) based in Salford that provides real-world work experience for young people aged 14-25 interested in a career in cyber security in the North West of England. The programme has three main focuses: to inspire potential talent, create a pipeline for the cyber security industry to respond to the skills gap, and make people safer in the digital world. Participants have the chance to participate in workshops to do some live threat hunting and cyber security simulations on real-time cyber attacks, engaging in an exercise designed to get them thinking like cyber security professionals.

The Neurodivergent Digital Cyber Academy (Immersive Labs)

The Neurodivergent Digital Cyber Academy is designed to help neurodiverse learners develop their cyber security skills through hands-on practical challenges. It features a browser-based, practical learning environment that caters for those with a range of skills. Based on their skill level, participants can apply for cyber jobs with employers signed up for the platform.

Diversity in Cyber Security (Crucial Academy)

This initiative based in Brighton looks to retrain veterans in cyber security, in particular focusing on women, neurodiverse candidates and BAME individuals. Successful applicants will undergo training, including a three-week intensive cyber security course in a state-of-the-art virtual lab environment. During the training, Crucial Academy will engage with employers to place individuals into jobs.

Hands-on Hacking Training and Employer Portal (Hacker House Ltd)

Hacker House has developed an online entry-level penetration testing course called "Hands-on Hacking". The programme is primarily targeted towards individuals who are interested in career in cyber security, particularly in the field of ethical hacking. CSIIF funding will make the course available as an 'on demand' service. As students graduate, they will be part of a community forum and mentorship programme to match them with employers.

HACKED (Blue Screen IT)

This Plymouth-based initiative will scale up an existing programme which identifies, trains and places individuals into a cyber security career. Participants include neurodiverse candidates, those with special needs and those from disadvantaged backgrounds. The training will be supported through Blue Screen IT, running its own Security Operations Centre (SOC) to provide practical experience and real-life exposure for candidates.

QA and Women Tech Jobs

Working in collaboration with Women Tech Jobs, QA is creating a new training programme to identify, train and place women into cyber security roles. The training blends classroom training with e-learning and will be shaped by industry employers in line with their required skill sets.

Source: DCMS, https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund.

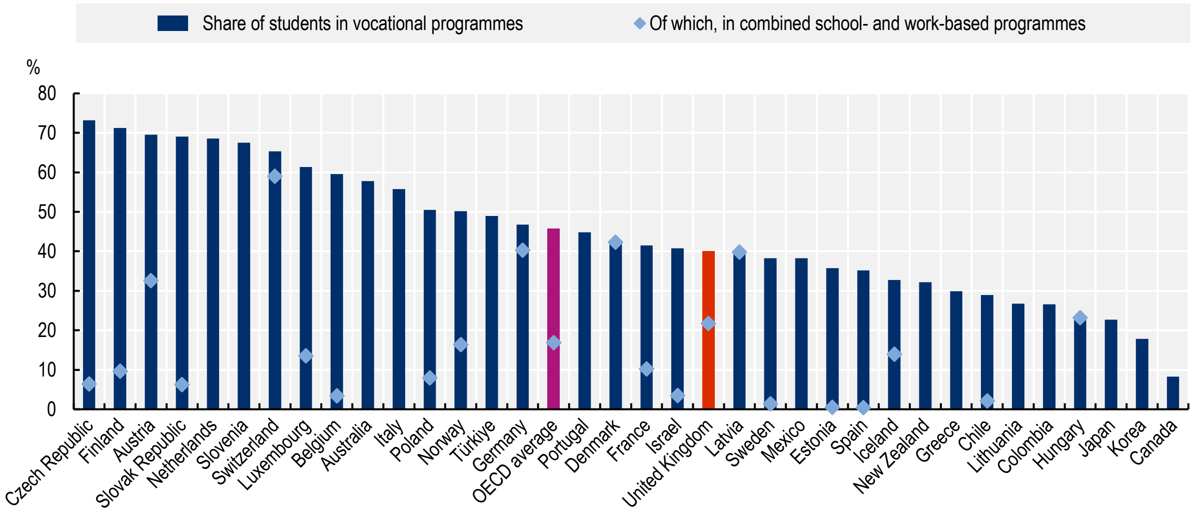
The role of employers in the design and delivery of learning opportunities in cyber security

Involving employers in the design of cyber security education and training programmes is imperative to understand and develop the knowledge and skills that learners need, especially in such a fast-changing sector. While formal education programmes may take longer to adjust, programs such as bootcamps can be more flexible and tailored to employer needs. Moreover, employers can participate in the provision of work-based learning opportunities in cyber security, which are key given the high levels of skills shortages. In this way, students improve their employability, transition to the labour market faster, and access job opportunities that better align with their professional development. For employers, work-based learning provides benefits in terms of increased productivity (ILO, 2018[52]), more efficient hiring processes, and staff with job-specific technical skills. The use of work-based learning in VET is relatively common in the United Kingdom, with just over half of the learners in upper-secondary VET enrolled in programmes with a substantial work-based component (see Figure 3.19). However, according to stakeholders consulted, the supply of work-based learning opportunities in cyber security remains insufficient.

Policies and strategies can increase employer participation in the design and delivery of cyber security education and training programmes. In England, the government has played an important role in facilitating the interaction between the education sector and the world of work so that the education and training provision is more aligned with the concrete needs of the cyber security sector both nationally and regionally. Likewise, initiatives have been implemented to encourage companies to offer cyber security apprenticeship opportunities and provide support in delivering them.

Figure 3.19. Share of enrolment in upper-secondary VET and work-based programmes

Share of students enrolled in upper secondary VET, 2015, 2017



Note: Countries ranked in descending order of the share of students in vocational programmes. Missing values indicate the absence of combined school- and work-based programmes or a lack of data.
Source: OECD (2020[53]), Education at a Glance 2020: OECD Indicators, OECD Publishing, Paris, https://doi.org/10.1787/69096873-en.

Boosting employers' participation in the design of cyber security programmes

Education and training providers in the cyber security field often work closely with employers to help students find career paths and benefit from their knowledge and other resources in delivering courses. Successful employer engagement is founded on long-lasting, mutually acceptable and beneficial relationships between schools and businesses. There are substantial advantages when these collaborations are systematic and scaled up as they bring coherence to education and training provision at a local and national level (Department for Business Innovation and Skills, 2015[54]).

Training providers are eager to include employers in the design of cyber security courses and modules so that they can meet employers' skills requirements and provide students with jobs (DCMS, 2019[7]). The development of courses in industry liaison panels or advisory groups that guide course content are examples of this. For instance, De Montfort University has developed cyber security training programmes with Deloitte, Airbus, BT and Rolls-Royce, with students being assessed by cyber security professionals from the industry (DMU, 2018[55]).

Programs such as cyber security bootcamps typically have the active participation of employers in designing and establishing the structure and content of the programmes since the training aims to equip learners with the skills required to fill a specific cyber security position. For instance, Generation, a cyber security Skills Bootcamps provider, works with employers throughout the entire programme design, delivery and placement (see Box 3.7). Also, for apprenticeship employer engagement is crucial. Employers in England work with the Institute for Apprenticeships to create and develop occupational standards.[10] These standards are the components of an apprenticeship, along with the End-point Assessment Plan (EPA) (i.e. assessment to evaluate apprentice performance) and a funding band (i.e. funds can be used to pay for apprenticeships training and assessment for apprentices) (IfATE, 2023[56]). Employers developed these standards to describe duties, and 'Knowledge, Skills and Behaviours' (KSBs). Employer groups (referred to as Trailblazer groups) participate actively in developing apprenticeships. For instance, IfATE approved the 2021 'cyber security technologist', a Level 4 apprenticeship standard, which involved the participation of multiples employers such as QineitQ (i.e. high-tech company focused on defence), Siemens (i.e. company focused on industry, infrastructure, transport, and healthcare), FoxRedRisk (i.e. Information Security and Data Protection consultancy), as well as the DCMS (IfATE, 2021[57]). In 2018, Global Knowledge UK, a worldwide leader in IT and professional training, in partnership with relevant cyber security players, including QUFaro (i.e. IT training provider) and GKA (i.e. IT and business training provider), collectively formed a trailblazer group for creating a Level 3 apprenticeship standard to address the need for a broader choice of qualifications to fulfil the skills gap in the cyber security profession and meet the demands of employers (Global Knowledge, 2018[58]).

Box 3.7. Responding to employers' immediate needs for cyber security skills: Generation

Generation is a global training provider that prepares adults of all ages for jobs. Their goal is to prepare, place and support people into life-changing careers. Generation offers programmes for placement into 38 occupations across five sectors: customer service and sales, technology, healthcare, skilled trades and green jobs. In the United Kingdom, within the technology sector, Generation provides courses in 'IT support with cyber security'.

In defining the courses to offer and their content, Generation involves employers throughout the creation process. Generation's course provision is employer-led, which indicates that employers are involved in designing the course portfolio, as reflected in the first component of the Generation approach, 'Jobs and employers' engagement from the start' (see Table 3.13). Before opening a course, employers' requirements for a specific profile and the characteristics of that profile are evaluated. Also, labour market trends are analysed in order to test if the training needs can be extrapolated to other sectors or employers. Course content is established based on continuous dialogue with employers and their recruitment teams.

Table 3.13. Components of generation's approach

Component	Description
1	Jobs and employer engagement from the start
2	Learner recruitment based on intrinsics, effort, and employment standards for the profession
3	4-12 weeks of technical, behavioural, mindset & professional presence skill training, with social support services provided
4	Interviews with employer partners for immediate job placement
5	Mentorship during and after the programme and an alumni community that follows graduates into the workplace.
6	Return on investment for employers, students, and society
7	A data-centred approach at every step

Source: Generation, https://www.generation.org/about/.

Generation's ongoing collaboration with employers has allowed it to understand skills needs better. This is reflected concretely in the fact that three-quarters of graduates across all their programmes can find a job during the first three months after completing the course. Additionally, employers recognise the impact Generation's model has on the preparation of their students. Nearly 91% of employers report that they would hire Generation graduates again, and 85% of employers think that Generation graduates perform at least as well or better than their peers. In 2021, Generation engaged with more than 2 400 employers and trained almost 12 000 students in 18 countries (including the United Kingdom).

Source: Generation (2021[59]), Annual report 2021, Moving forward, https://www.generation.org/wp-content/uploads/2022/06/Generation-Annual-Report-2021.pdf.

To some extent, the level of employer involvement is influenced by geography and the degree to which training providers are located in areas of England with strong technology-based firms. Having employers nearby helps to improve the links that training providers can develop with industry. For example, Nexus, an IT support and consulting company with headquarters in the outskirts of Exeter, has built a close relationship with Exeter College to engage with the design of cyber security undergraduate programmes, among other ICT programmes. Additionally, Nexus employees regularly go to the college to speak to students about ICT careers.

The extent of the links between industry and the FE and HE sectors also depends on the nature of employers' activities. Not surprisingly, firms that specialise in providing cyber security services (IT companies, major consulting companies, etc.) have the closest links with training providers (DCMS, 2019[7]). However, companies in parts of the economy that are especially vulnerable to cyber attacks (e.g. financial services, advanced manufacturing, defence-related) are also major recruiters of cyber security graduates. There is a strong mutual interest in developing close links in those sectors. For example, the University of Warwick collaborates closely with Jaguar Land Rover and other automotive firms in the West Midlands for the design and delivery of its courses, including in cyber security (Warwick University, 2018[60]).

Cyber security clusters have an important role in promoting employer participation in cyber security learning opportunities in England. Sectorial clusters, in general, provide a networking environment that facilitates the interaction of all stakeholders – including training providers, think tanks, companies and regional and local authorities (The European watch on cyber security and privacy, 2022[61]). In cyber security, clusters of employers enhance co-operation and co-ordination of actions to establish synergies to move forward relevant matters and address issues that directly affect cyber security at the regional level. For instance, Cyber East, the East region cyber cluster in England, is an industry body that works alongside the government to develop the cyber security industry. Cyber East works with businesses across Norfolk, Suffolk, and Cambridgeshire and expands to other areas, encouraging collaboration with multiple stakeholders, including training providers. Co-operation among clusters also contributes to identifying and sharing good practices for managing cyber security skills shortage. For instance, UKC3, a cyber security cluster collaboration hub, supports cyber security clusters to drive growth in the sector within their nations and regions. UKC3 champions activities to support businesses, academia and other skills or talent development organisations to promote cyber skills development and careers in the cyber security industry (see Box 3.8).

Increasing the provision of work-based learning opportunities in cyber security

Employers have a key role in providing work-based learning opportunities in cyber security. Through apprenticeships, students can access training combining classroom and work-based learning, allowing them to acquire practical skills and knowledge relevant to employers in the sector (OECD, 2014[62]). Nonetheless, the number of cyber security apprentices remains low (see above). This may be due to multiple reasons. Learners may have limited awareness about the options available. Companies, especially SMEs, may need more support to provide apprenticeship opportunities, as implementing apprenticeships has time and cost implications. One barrier that is, in particular, important for SMEs is that assigning staff to oversee training impedes them from carrying out the core business activities related to cyber security – and this may be even more problematic in the cyber security sector than in other sectors given the prevailing labour shortages and associated risks.

Box 3.8. Bridging employers and training providers around cyber security: UKC3

UK Cyber Cluster Collaboration (UKC3) supports cyber clusters to drive the growth of the cyber sector within their nations and regions. UKC3 promotes collaboration, knowledge exchange and sharing of best practices between cyber clusters in order to develop the ecosystem, promote innovation and grow cyber skills. UKC3 supports cyber clusters through funding and by enabling opportunities for networking and knowledge exchange. As a national body, UKC3 works across public and private sectors and academia and provides a single entity for an organisation wishing to engage with the UK cyber cluster community. UKC3 works with clusters to support and, where appropriate, fund their work, looking for opportunities to join up and amplify activities to deliver impact on a national scale.

UKC3 has established three working groups aimed at bringing together cluster leads and sector expertise to drive forward initiatives aimed at growing the cyber sector in the United Kingdom: (1) Ecosystem development, (2) innovation join-up, and (3) Cyber Skills Growth. Regarding the latter, UKC3 champions activities to support cyber skills growth, working with industry, academia, and other skills or talent development organisations to promote cyber skills development and the attractiveness of careers in the cyber security industry. The UKC3-recognised cyber clusters have been working closely with local and regional businesses to understand their cyber skills needs and identify skill shortages while collaborating with growth actors that can support talent development in the industry. Cyber clusters organise monthly or regular networking events and workshops to promote cyber skills growth across their respective regions, contributing to strengthening the cyber security sector in the United Kingdom.

Table 3.14. List of UKC3 recognised clusters

Clusters	
Bristol and Bath Cyber Cluster*	North West Cyber Security Cluster*
Cyber East*	ScotlandIS Cyber
CyberNorth*	South West Cyber Security Cluster*
Cyber Wales	Surrey Cyber Security Cluster*
CyNam (Cyber Cheltenham)*	Swindon and Wiltshire Cyber Cluster*
Midlands Cyber*	Yorkshire Cyber Security Cluster*
NI Cyber (Northern Ireland)	

Note: * Clusters located in England.
Source: UKC3, https://ukc3.co.uk/cyber-skills-growth/.

In order for employers to see the value of offering apprenticeship opportunities, they need to be aware of their specific cyber security skills needs. On average, 54% of businesses in England report understanding at least reasonably well their cyber security training needs – but few outside the cyber security sector report they understand these need very well (14%) (DCMS, 2022[29]). Even though a higher proportion of businesses in the cyber security sector report understanding very well their cyber security training needs (68%), only 36% of SMEs in the cyber security sector do so (DCMS, 2022[29]). Companies' limited understanding of their cyber skill requirements can hinder the implementation of cyber security apprenticeship programmes. The NCSC provides cyber security advice for businesses, charities, clubs and schools with up to 250 employees on many issues, including training delivery. Most of the resources available from the NCSC focus on assessing cyber security needs and identifying cyber security risks. SMEs can get access to the Small Business Guide and Exercise in a Box, tools that provide key information to identify the security bridges, evaluate the level of resilience to cyber attacks and determine the capacity of the organisation to deal with cyber threats with current resources (infrastructure and human capital).

Successfully engaging more employers is necessary for realising the potential benefits of work-based learning and making work-based learning accessible for young people and adults with diverse needs and aspirations, including those without jobs or learning opportunities (Kis, 2016[63]). In England, policy makers have implemented various strategies and policy tools to unlock engagement by shifting the cost-benefit balance for employers and making the provision of apprenticeships more attractive and manageable for businesses. Introduced in 2017, the apprenticeships levy is a government initiative to encourage companies to hire apprentices and help reduce skills gaps in the United Kingdom (see Box 3.9). The levy's introduction has increased focus on training new and existing employees for the highly skilled roles the economy needs by covering the full cost of training and assessment for levy payers and covering partially for non-levy payers (covering 95% of tuition fees). Since 2022, a new portable flexi job apprenticeship-sharing arrangement has been piloted, allowing apprentices to undertake a series of shorter contracts with a number of employers while completing their training in preparation for end-point assessment. The pilot is running across 38 standards in the creative, digital, adult care and construction sectors. These Flexi-Job Apprenticeships have been designed to ensure that those sectors and occupations where short-term contracts or other non-standard employment models are the norms can access the benefits of apprenticeships.

Box 3.9. Funding the provision of work-based learning opportunities: The apprenticeship levy

Introduced in April 2017, the apprenticeship levy is a Government initiative to fund apprenticeships. The government committed to 3 million apprenticeship starts in England by 2020, and the levy was created to support this. This incentive aims to encourage more employers to hire apprentices – and help reduce skills gaps in the United Kingdom.

The levy funds are made available to help subsidise apprentices' training costs. It applies to those with a payroll of more than GBP 3 million and is used solely to fund apprenticeship training. The levy is charged at 0.5% of an employer's total payroll. The levy is withheld on a monthly basis alongside income tax and national insurance contributions and appears in the employer's digital apprenticeship account. When an employer takes on an apprentice, the training provider (for the off-the-job component) is paid out of the employer's digital account every month. Apprenticeship levy rules state that the levy must only be used to pay for apprenticeship training and End-point Assessment and cannot be used to pay apprentice wages. The apprenticeship levy can be used to train newcomers or existing staff.

Evidence suggests that the Apprenticeship Levy has had positive, yet heterogeneous, effects on the number of apprenticeships undertaken. After the introduction of the levy, there was a marked decline in apprenticeships starting at the intermediate and advanced levels. However, higher-level apprenticeship (Level 4 and above) starts showed a rapid increase. Enterprises paying the levy experience a positive trend in all apprenticeship levels compared to non-levy enterprises (Patrignani et al., 2021[64]).

Source: Skills for security, https://www.skills4security.com/funding-and-incentives; Patrignani et al., (2021[64]), The Impact of the Apprenticeship Levy on Apprenticeships and other training outcomes, Centre for Vocational Education Research, https://cver.lse.ac.uk/textonly/cver/pubs/cverdp034.pdf.

Some training providers offer support to employers for effectively providing apprenticeship opportunities. For instance, CyberPro, an organisation grounded on providing accessible resources to individuals and companies interested in developing cyber security learning ecosystems, offers online information on how apprenticeships in this field are established and how to benefit from the different schemes and support provided by the government to fund the cyber security apprenticeships programmes. Similarly, some training providers provide key information and raise awareness about the benefits of employing a cyber security apprentice. Escalla, a global workplace and digital skills provider, is accompanying employers with guidance and information on apprenticeship benefits. It also supports employers on how to make the most of providing apprenticeship programmes in cyber security (Escalla, 2022[65]).

Additional initiatives come from joint efforts from trade associations and the higher education sector to increase the provision of apprenticeship programmes in the tech sector. For instance, Techskill, a partnership between employers and educators for developing digital since 2021, recognises talent from within the digital degree apprenticeship sectors through the National Tech Industry Gold Digital Degree Award. The objective of providing this recognition is to highlight employers and training providers that contribute to developing the relevant skills for sectors through apprenticeship programmes and incentivising more employers to deliver digital skills apprenticeship programmes. Some universities have started incorporating digital apprenticeships into their degree programmes in partnership with enterprise conglomerates. The curricula of higher-level digital apprenticeships typically cover a variety of digital skills, including cyber security, big data, software engineering, digital banking, IT skills for the automotive industry, etc. For example, Warwick Manufacturing Group, as part of the University of Warwick, provides degree-level apprenticeship modules embedded in undergraduate courses, including one in cyber security engineering (see Box 3.10). Another example is the partnership of J.P. Morgan, a multinational investment bank and financial services company, with the University of Exeter in October 2018 to offer the UK's first degree apprenticeship programme in applied finance and cyber security. The programme covers areas ranging from securities to IT in investment operations and prepares apprentices to become financial services professionals with the essential skills for using digital banking products. A large proportion of the programme takes place at the workplace through projects linked to academic content, while some modules can also be completed by distance learning.

Box 3.10. Joining efforts for providing apprenticeships in cyber security: Warwick Manufacturing Group

As a part of the University of Warwick, Warwick Manufacturing Group (WMG) was founded in 1980 to improve the competitiveness of industries through innovation and the development of new technology and skills. Currently, WMG provides apprenticeship programmes at different levels in the field of technology – five higher-level apprenticeships and three degree apprenticeships programmes. The five higher-level apprenticeships are in Applied Engineering, Cyber Security, Digital Healthcare Science, Digital and Technology Solutions and Engineering, with three to four years of duration. Apprentices are employed by companies such as Dyson and Jaguar Land Rover, where they can develop skills on the job. The three degree apprenticeship programmes are in Engineering Business Management, Senior Leadership and Systems Engineering Technical Leadership, with a duration of two-and-a-half to three years. Apprentices complete some of their postgraduate modules through on-the-job training in companies like GE Aviation and Royal Mail Group.

Apprentices do not pay fees to the universities, and instead, they receive between GBP 16 000 and GBP 25 000 per year as part of their salaries. The details of two WMG undergraduate courses are provided below:

- Apprenticeship in engineering with Dyson: a four-year programme that covers essential skills for the digital economy, including agile software development, cyber risk in organisations, data science and machine learning, and electronics manufacturing and assembly.
- Apprenticeship Applied Engineering with Jaguar Land Rover: a four-year programme focusing on high-level digital skills, primarily through courses such as computer-aided design (CAD), computer-aided manufacturing (CAM) and electrical and electronic systems.

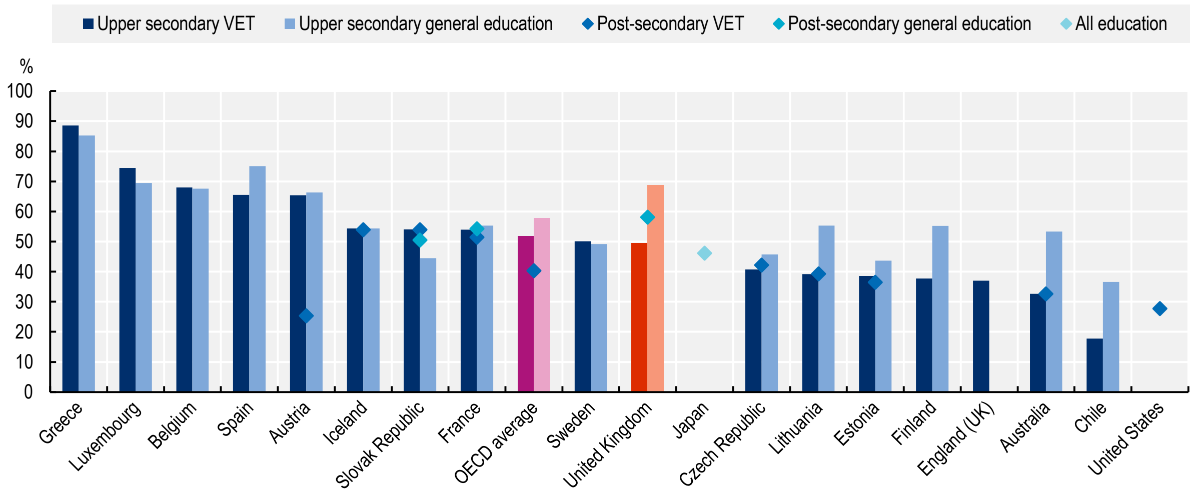
Source: Warwick University, https://warwick.ac.uk/fac/sci/wmg.

Investing in the quality of cyber security education and training programmes in England

Teachers and trainers are at the heart of quality education and training provision. When providing education and training in areas that face shortages in the labour market, it can be difficult to find the workforce to teach those skills. This, in turn, may affect the quality and relevance of the education and training provided. Teachers typically account for an important share of expenditures in education (see Figure 3.20). In the United Kingdom, expenditure on teachers is equivalent to almost half of the total VET expenditure (49%). Teacher shortages have important implications for the provision of education and training programmes, which may affect any strategy or policy aimed at expanding training provision. Moreover, fast-changing sectors, such as cyber security, call for regular changes to curricula and, therefore, also to teacher training and professional development. It could also imply changes to teachers' recruitment strategies if more industry experience is desired.

Figure 3.20. Share of expenditure for compensation of teachers, 2019 or latest year

Teachers with active teaching responsibilities are included in all public and private institutions



Note: In the case of the United Kingdom, VET institutions are all government dependent private institutions. Data for England (UK) refer to all staff costs in further education colleges (2016-17). Japan (2018) refers to total school education expenditure, excluding expenses for public universities, junior colleges and subsidies to private schools.
Source: OECD (2020[53]), *Education at a Glance 2020: OECD Indicators*, OECD Publishing, Paris, https://doi.org/10.1787/69096873-en.

Ensuring the quality of cyber security education programs is crucial to expanding enrolment and tackling shortages. Generally, well-recognised programmes tend to attract more students (UNESCO, 2020[66]). Cyber security is no exception; based on evidence from the computer science field, good quality ICT programs attract more students, not only those who already have knowledge or experience in the sector but also those completely external to the field. Moreover, cyber security issues require standardised practices, methods and knowledge that students must develop in their cyber security education and training programmes. For this reason, the UK Government has focused part of its efforts on developing strategies to ensure that formal education and training programmes in cyber security are provided at the highest quality.

Tackling teacher shortage in cyber security education

Teachers in FE are unique in terms of how they are recruited and trained. They are expected to have not only the subject and pedagogical knowledge but, in many cases, work experience in their industry. Moreover, FE teachers' skills can be in high demand in occupations other than teaching, making it harder to recruit and retain teachers in related subjects (OECD, 2021[67]). Given the shortages of skilled cyber security professionals, the cyber security field may be particularly difficult to attract and retain teachers.

Despite the relevance of understanding teacher shortages, regularly and systematically collected comprehensive data focused on FE teachers, including the number of teachers, hiring needs and shortages across OECD countries, is limited (OECD, 2021[67]). In England, the Staff Individualised Record (SIR) data has information on teachers in the FE sector. Table 3.15 shows that the proportion of staff teaching ICT subjects is 2.1%, which is low compared to other fields, and it is not aligned with the percentage of FE students in the field, potentially reflecting a lack of teachers and trainers in the field. However, information on teacher shortages by sector is not readily available. Teacher information for the narrow field of cyber security is particularly hard to come by, and the DCMS has already recommended collecting more data in this area to enhance cyber security training provision (DCMS, 2019[7]).

Table 3.15. Proportion of FE teachers and students by subject (2018-19)

Subject	Distribution of FE teachers (% of total)	Distribution of FE students (% of total)
Business, administration and law	17.6	20.0
Humanities	13.0	3.0
Health, public service and care	11.2	15.5
Arts, media and publishing	10.7	5.9
Combined and general studies	9.7	36.0
Science and Mathematics	9.4	1.2
Engineering and manufacturing technologies	8.9	6.4
Construction, planning and the built environment	7.5	3.5
Agriculture, horticulture and animal care	4.0	1.2
Education and Training	2.6	1.4
Information and communication technology (ICT)	2.1	6.0
Social Sciences	1.6	0.5

Note: Teaching staff only. This measures the proportion of staff for each subject. Information on the distribution of FE students refers to academy period 2018-19, https://explore-education-statistics.service.gov.uk/data-tables/permalink/585939df-2c1c-4afd-8663-08dad51ca1cc.
Source: SIR Data insights, https://www.et-foundation.co.uk/wp-content/uploads/2020/06/SIR27-REPORT-FOR-PUBLICATION.pdf.

Teacher shortages can damage the stable provision of specific occupational courses and the sustainable supply of qualified workers for associated occupations (OECD, 2021[67]). Teacher shortages may also increase the costs of training provision. For instance, in England (ACL Consulting, 2020[68]), higher costs during times of FE teacher shortages may be driven by increased use of lower- or less-qualified teaching staff and temporary or agency staff – which is not always cheaper than hiring suitably qualified teachers – and can lead to increased workloads and stress for existing staff.

Signalling the quality of cyber security education and training programmes

The NCSC is the governmental body responsible for recognising and supporting the best cyber security education programs for students and employers. Since 2018, working in partnership with the DCMS, Cabinet Office (CO), UK Research and Innovation (UKRI), the NCSC certifies programmes across higher education institutions that best respond to cyber security standards established by CyBOK and the national cyber security priorities (Cabinet Office, 2022[69]). The NCSC certifies degree apprenticeships, Bachelor's degrees and Integrated Master's degrees in cyber security and closely related fields (see Table 3.16). For the certification of degree apprenticeships, NCSC follows apprenticeship standards established by the Institute for Apprenticeships to conduct the assessment (Institute for Apprenticeships and Technical Education, 2020[70]). Among bachelor's degrees, NCSC assesses computer science for cyber security, computer science and cyber security, and computer science and digital forensics.

Table 3.16. Undergraduate degrees and degree apprenticeships certified by NCSC

Fully certified bachelor's degrees and degree apprenticeships		Provisionally certified bachelor's degrees	
Institution	Degree course	Institution	Degree course
Edinburgh Napier University	BEng Cyber security and Forensics	Cardiff Metropolitan University	BSc Computer Security
Oxford Brookes University	BSc Computer Science for Cyber Security	Leeds Beckett University	BSc Cyber Security
Oxford Brookes University	BSc Computer Science for Cyber Security (with a year in industry)	University of Bradford	BSc Computer Science for Cyber Security
Royal Holloway, University of London	BSc Computer Science (Information Security)	University of Greenwich	BSc Computer Security and Forensics
University of the West of England (in partnership with Gloucestershire college)	Integrated Degree Apprenticeship in Cyber Security		

Source: NSCS, https://www.ncsc.gov.uk/information/ncsc-certified-degrees.

This certification process has a clear objective: to set the standard for good cyber security higher education in the United Kingdom and better alignment with the priority actions to strengthen the UK's cyber ecosystem (Government, 2021[71]), which may positively affect all stakeholders. Recognition of cyber security education and training programmes benefits training providers, students and employers. For example, NCSC certification helps universities attract additional numbers of skilled students from the United Kingdom and abroad. Since navigating the range of cyber security degree programmes on offer in the United Kingdom may be difficult, NCSC certification can help students to choose a cyber security course which has been evaluated by the NCSC. Students from NCSC-certified degree programmes will be provided with an additional form of recognition (i.e. that the student has successfully completed an NCSC-certified degree), which will help employers distinguish between applicants' qualifications.

Cyber security programme recognition is also granted to schools and colleges through the NCSC's CyberFirst schools and colleges programme (see Box 3.4). Eligible secondary schools or colleges where CyberFirst operates can apply to be part of the CyberFirst Schools and Colleges scheme. Successful applicants receive NCSC recognition and are promoted as leaders committed to providing a structured approach to excellence in cyber security education. Schools and Colleges are certified to become part of the CyberFirst Education eco-system to promote cyber security education among young people.

References

(ISC)² (2022), *Cybersecurity workforce study*, https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx. [1]

ACL Consulting (2020), *Costs and cost drivers in the Further Education sector*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_dat. [68]

Breda, T. et al. (2021), *Do Female Role Models Reduce the Gender Gap in Science? Evidence from French High Schools*, https://halshs.archives-ouvertes.fr/halshs-01713068v5. [39]

Cabinet Office (2022), *National Cyber Strategy 2022*, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#:~:text=Vision-,The%20UK%20in%202030%20will%20continue%20to%20be%20a%20leading,in%20support%20of%20national%20goals.&text=1.,2. [69]

CAPSLOCK (2022), *Capslock cybersecurity blended training model*, https://capslock.ac/the-course. [18]

CISCO (2019), *Annual security report*, https://www.cisco.com/site/us/en/index.html#tabs-ca9b217826-item-1b113ceb83-tab. [2]

Cyber Explorers (2023), *Cyber Explorers*, https://www.cyberexplorers.co.uk/ (accessed on 2023). [43]

CyBOK (2021), *Introduction to CyBOK*, The National Cyber Security Centre, https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf. [8]

CyBOK (2019), *The Cyber Security Body of Knowledge*, The National Cyber Security Centre, https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf. [6]

DCMS (2022), *Cyber security skills in te UK labour market*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf. [29]

DCMS (2021), *CyberFirst Evaluation*, https://www.gov.uk/government/publications/independent-evaluations-of-cyber-discovery-and-cyberfirst-programmes/cyberfirst-evaluation#summer-courses. [50]

DCMS (2021), *DCMS sector economic estimates 2021: employment 2019 to June 2021*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf. [31]

DCMS (2019), *Cyber Skill Immediate Impact Fund (CSIIF)*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825141/CSIIF_Third_Round_Guidance_for_Applicants.pdf. [51]

DCMS (2019), *Identifying the Role of Further and Higher Education in Cyber Security Skills Development*, Department of Digital, Culture, Media and Sport, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767425/The_role_of_FE_and_HE_in_cyber_security_skills_development.pdf. [7]

DCMS (2018), *Initial National Cyber Security Skills Strategy - Increasing the UK's cyber security capability*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949211/Cyber_security_skills_strategy_211218_V2.pdf. [23]

Department for Business Innovation and Skills (2015), *Understanding the link between employers and schoos and the role of the National Career Service*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/386030/bis-14-1271-understanding-the-link-between-employers-and-schools-and-the-role-of-the-national-careers-service.pdf. [54]

Department for Education (2023), *Introduction to T Levels*, https://www.gov.uk/government/publications/introduction-of-t-levels/introduction-of-t-levels. [10]

Department for Education (2022), *Education and training statistics for the UK*, https://www.gov.uk/government/statistics/announcements/education-and-training-statistics-for-the-uk-2022#full-publication-update-history. [9]

Department for Education (2022), *Find a Skills Bootcamp*, https://www.gov.uk/guidance/find-a-skills-bootcamp/eligibility. [15]

Department for Education (2022), *Skill Bootcamps training providers*, https://www.gov.uk/government/publications/skills-bootcamps-training-providers. [5]

Department for Education (2021), *Skills bootcamps process evaluation*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1027163/Bootcamps_wave_1_final_evaluation_report.pdf. [16]

Department for Education (2020), *Higher technical education reforms*, https://www.gov.uk/government/publications/higher-technical-education-reforms/higher-technical-education-reforms. [12]

DMU (2018), *UK cyber skills to receive breakthrough boost with pioneering new training course*, https://www.dmu.ac.uk/about-dmu/news/2015/november/uk-cyber-skills-to-receive-breakthrough-boost-with-pioneering-new-training-course.aspx. [55]

EdX (2021), *Accelerating our movement: 2021 EdX impact report*, https://www.edx.org/assets/2021-impact-report-en.pdf. [21]

Escalla (2022), *Employing a cyber security apprentice*, https://escalla.co.uk/employing-a-cyber-security-apprentice/. [65]

Fry, R., B. Kennedy and C. Funk (2021), *STEM Jobs See Uneven Progress in Increasing Gender, Racial and Ethnic Diversity*, https://www.pewresearch.org/science/2021/04/01/stem-jobs-see-uneven-progress-in-increasing-gender-racial-and-ethnic-diversity/. [28]

Generation (2022), *Skills Bootcamp on IT support with cyber security*, https://uk.generation.org/london/itsupport-cyber/. [24]

Generation (2021), *Annual Report 2021: Moving Forward*, https://www.generation.org/wp-content/uploads/2022/06/Generation-Annual-Report-2021.pdf. [59]

Global Knowledge (2018), *Qufaro sponsors trailblazer group for level three cybersecurity apprenticeship in partnership with global knowledge UK*, https://www.globalknowledge.com/en-gb/company/news/press-releases/qufaro-sponsors-trailblazer-group-for-l3-cybersecurity-apprenticeship-in-partnership-with-gk. [58]

Government (2021), *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy. [71]

HM Government (2022), *T-Levels in the UK*, https://www.tlevels.gov.uk/students/subjects/digital-support-services. [11]

HM Government (2016), *Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability - A Call for Views*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949211/Cyber_security_skills_strategy_211218_V2.pdf. [42]

Hosting Data UK (2022), *Best Online Learning Platforms*, https://hostingdata.co.uk/best-online-learning-platforms/#:~:text=Coursera%20and%20Udemy%20are%20two,companies%20to%20offer%20corporate%20training. [19]

Houston, R. et al. (2022), *Recognising and overcoming barriers to participation in STEM*, https://aerospaceamerica.aiaa.org/departments/recognizing-and-overcoming-barriers-to-participation-in-stem/#:~:text=Barriers%20to%20participation%20in%20STEM%20education%20%E2%80%93%20including%20socioeconomic%2C%20self%2D,or%20ethnicity%2C%20gender%2C%20. [4]

IET (2018), *Women in STEM*, https://warwick.ac.uk/fac/sci/eng/about/athenaswan/edit-contents/women_in_stem_bro.pdf. [26]

IfATE (2023), *Developing an occupational standard*, https://www.instituteforapprenticeships.org/developing-new-apprenticeships/developing-occupational-standards/. [56]

IfATE (2022), *Aproved Higher Technical Qualifications*, https://www.instituteforapprenticeships.org/qualifications/higher-technical-qualifications/approved-higher-technical-qualifications-cycle-one/. [13]

IfATE (2021), *Cyber security technologist occupation standards*, https://www.instituteforapprenticeships.org/apprenticeship-standards/cyber-security-technologist-2021-v1-0. [57]

ILO (2018), *Investing in work based learning*, https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---ifp_skills/documents/publication/wcms_565923.pdf. [52]

Immersivelabs (2022), *Arming Organizations Against Cyber Threats Since*, https://www.immersivelabs.com/our-story/. [17]

Institute for Apprenticeships and Technical Education (2020), *Standards for cyber security technical professional (Integrated degree)*, https://www.instituteforapprenticeships.org/apprenticeship-standards/cyber-security-technical-professional-integrated-degree-v1-0. [70]

Kis, V. (2016), *Work-based learning for youth at risk: Getting employers on board*, OECD publications, https://www.oecd.org/education/skills-beyond-school/Work-based_Learning_For_Youth_At_Risk-Getting_Employers_On_Board.pdf. [63]

Learn21 (2022), *What is a bootcamp and is it useful in learning new skills?*, https://learn21.in/blog/what-is-a-bootcamp-how-is-it-useful. [14]

LinkedIn Learning (2022), *Workplace Learning Report - The transformation of learning and development*, https://learning.linkedin.com/resources/workplace-learning-report. [22]

Malcom, S. and M. Feder (eds.) (2016), *Barriers and Opportunities for 2-Year and 4-Year STEM Degrees*, National Academies Press, Washington, D.C., https://doi.org/10.17226/21739. [3]

NCSC (2022), *Bursary and Degree Apprenticeship*, https://www.ncsc.gov.uk/cyberfirst/bursary-and-degree-apprenticeship (accessed on 8 March 2023). [47]

NCSC (2022), *CyberFirst courses*, https://www.ncsc.gov.uk/cyberfirst/courses (accessed on 8 March 2023). [44]

NCSC (2022), *CyberFirst Girls Competition*, https://www.ncsc.gov.uk/cyberfirst/girls-competition (accessed on 8 March 2023). [46]

NCSC (2022), *CyberFirst overview*, https://www.ncsc.gov.uk/cyberfirst/overview (accessed on 8 March 2023). [48]

NCSC (2022), *CyberFirst Schools and Colleges*, https://www.cyberfirstschools.co.uk/ (accessed on 8 March 2023). [45]

NCSC (2021), *CyberFirst annual report 2020 - 2021*, https://www.ncsc.gov.uk/files/CF-Annual-Report-2020-21-Final-Version.pdf. [33]

NCSC (2021), *Decrypting Diversity: Diversity and Inclusion in Cyber Security*, https://www.ncsc.gov.uk/files/KPMG-and-the-NCSC-Decrypting-Diversity-2021-report.pdf. [32]

OECD (2021), *Teachers and Leaders in Vocational Education and Training*, OECD Reviews of Vocational Education and Training, OECD Publishing, Paris, https://doi.org/10.1787/59d4fbb1-en. [67]

OECD (2020), *Dream Jobs? Teenagers' career aspirations and the future of work*, https://www.oecd.org/education/dream-jobs-teenagers-career-aspirations-and-the-future-of-work.htm. [37]

OECD (2020), *Education at a Glance 2020: OECD Indicators*, OECD Publishing, Paris, https://doi.org/10.1787/69096873-en. [53]

OECD (2019), *Getting Skills Right: Engaging low-skilled adults*, https://www.oecd.org/els/emp/engaging-low-skilled-adults-2019.pdf. [49]

OECD (2019), *Investing in career guidance*, https://www.oecd.org/education/career-readiness/Investing%20in%20Career%20Guidance_en.pdf. [41]

OECD (2019), *PISA 2018 Results (Volume II): Where All Students Can Succeed*, PISA, OECD Publishing, Paris, https://doi.org/10.1787/b5fd1b8f-en. [36]

OECD (2014), *Skills beyond School: Synthesis Report*, OECD Reviews of Vocational Education and Training, OECD Publishing, Paris, https://doi.org/10.1787/9789264214682-en. [62]

Office for Students (2022), *Two thousand new scholarships available to boost digital skills*, https://www.officeforstudents.org.uk/news-blog-and-events/press-and-media/two-thousand-new-scholarships-available-to-boost-digital-skills/. [34]

Oxford University (2019), *Closing the diversity gap in computer science*, https://www.development.ox.ac.uk/report2019-20/closing-the-diversity-gap-in-computer-science. [35]

Patrignani, P. et al. (2021), *The impact of the Apprenticeship Levy on apprenticeships and other training outcomes*, https://cver.lse.ac.uk/textonly/cver/pubs/cverdp034.pdf. [64]

Royal Society (2020), *Ethnicity STEM data for students and academic staff in higher education*, https://royalsociety.org/-/media/policy/Publications/2021/trends-ethnic-minorities-stem/Ethnicity-STEM-data-for-students-and-academic-staff-in-higher-education.pdf. [27]

SANS (2022), *Upskill in cyber*, https://www.sans.org/mlp/upskillcyber-uk/. [25]

Tech target (2019), *Computer science undergraduates most likely to drop out*, https://www.computerweekly.com/news/252467745/Computer-science-undergraduates-most-likely-to-drop-out. [38]

The European watch on cyber security and privacy (2022), *Engaged clusters*, https://www.cyberwatching.eu/engaged-clusters. [61]

Think Impact (2021), *Skillshare review*, https://www.thinkimpact.com/skillshare-review/. [20]

UK Cyber Security Council (2023), *Outreach and diversity in the cyber security profession*, https://www.ukcybersecuritycouncil.org.uk/outreach-and-diversity/. [30]

UNESCO (2020), *Towards universal access to higher education: International trends*, https://globaleducationforum.org/wp-content/uploads/2021/10/DOC-11-Towards-universal-access-to-higher-education-international-trends.pdf. [66]

Valero, D., A. Keller and A. Hirschi (2019), "The Perceived Influence of Role Models and Early Career Development in Native and Migrant Youth", *Journal of Career Development*, Vol. 46/3, pp. 265-279, https://doi.org/10.1177/0894845318763905. [40]

Warwick University (2018), *Jaguar Land Rover launches Lifelong Learning Academy with WMG as partner*, https://warwick.ac.uk/newsandevents/pressreleases/jaguar_land_rover_launches_lifelong_learning_academy_with_wmg_as_partner1/. [60]

Notes

[1] Level 3 qualifications are a group of courses which are all equivalent to A-Levels (short for Advanced Level) and come after the General Certificate of Secondary Education (GCSE).

[2] T-Levels are an alternative to A-Levels, apprenticeships and other 16 to 19 courses. Equivalent in size to 3 A-levels, a T-Level focuses on vocational skills and can help students into skilled employment, higher study or apprenticeships.

[3] HTQs are an alternative to apprenticeships or degrees. HTQs are existing and new Level 4 and 5 qualifications – that correspond to ISCED 5, i.e. short-cycle tertiary education.

[4] English Level 2 and 3 programmes are both mapped to ISCED Level 3, the main difference being that Level 2 qualifications are considered in the ISCED classification as “Sufficient for partial level completion, without direct access to post-secondary non-tertiary education or tertiary education” and the Level 3 qualifications as “Sufficient for level completion, with direct access to tertiary education”.

[5] ICT education programmes also include ICT for users, which involve all training for developing general competencies on ICT usage and adoption. This may include cyber security training for raising awareness and providing prevention measures.

[6] Qualifications at Level 1 also exist in digital skills, but these do not include cyber security content as they are primarily concerned with equipping individuals with essential digital skills.

[7] Universities and Colleges Admission Service (UCAS) – Information retrieved on 11 of November 2022, https://www.ucas.com/https://www.ucas.com/.

[8] The cyber security course figures are comparable to other computer sciences courses. In both cases, overall employment rates are also similar to the previous year, which suggests that cyber security and computer science graduate employment remained broadly consistent despite the COVID-19 pandemic.

[9] Sector Delivery Leads assess sectors’ needs and drive policy intervention to support workforce supply, retention and progression in their sector. Their approach involves: Collecting and monitoring data on sector needs and supply pipeline; engaging with employers to understand barriers to recruitment, retention and progression; co-ordinating and driving activity across government, ensuring government effort focusses where it will be most effective; economic analysis; and sector engagement.

[10] Occupation standard is a description of an occupation that contains an occupational profile and describes the ‘knowledge, skills, and behaviours’ (KSBs) needed for someone to be competent in the occupation’s duties.

OECD Skills Studies

Building a Skilled Cyber Security Workforce in Five Countries

INSIGHTS FROM AUSTRALIA, CANADA, NEW ZEALAND, UNITED KINGDOM, AND UNITED STATES

As societies become increasingly digital, cyber security has become a priority for individuals, companies and nations. The number of cyber attacks is exceeding defence capabilities, and one reason for this is the lack of an adequately skilled cyber security workforce. This report analyses the demand for cyber security professionals in Australia, Canada, New Zealand, the United Kingdom and the United States using information contained in online job postings. The analysis looks at recent trends in the demand for workers in different types of cyber security roles, the geographical distribution of cyber security job postings, and the changing skill requirements for professionals in this field. The report also looks at the supply side, zooming in on the landscape of cyber security education and training programmes in England (United Kingdom). It describes the different types of programmes provided in further and higher education, the profile of learners in these programmes and their outcomes. Finally, the report also looks at policies and initiatives adopted in England to make cyber security education and training programmes more accessible and relevant. This report is part of a larger initiative examining the evolution of policies and experiences in the cyber security profession around the world.

Microsoft

PRINT ISBN 978-92-64-38124-7
PDF ISBN 978-92-64-33839-5

9 789264 381247