Department for Digital, Culture, Media & Sport

Centre for Strategy & Evaluation Services

Department for Digital, Culture, Media and Sport

Identifying the Role of Further and Higher Education in Cyber Security Skills Development

Lead authors: Jack Malan, Eugénie Lale-Demoz, James Rampton

Acknowledgments

The Department for Digital, Culture, Media and Sport (DCMS) commissioned the Centre for Strategy and Evaluation Services (CSES) to undertake this study. The lead authors from CSES were supported by members of Cyber Security Oxford, Maria Bada, Arnau Erola, Ioannis Agrafiotis and Jason Nurse.

The authors extend special thanks to all those who have contributed to this study, particularly the many representatives of Further and Higher Education institutions, Government Departments, companies and other organisations who agreed to be interviewed, responded to the online survey or who helped organise focus groups with students.

We would like to thank those who worked with us at DCMS for their support to the research team.

Table of Contents

Tables

Figures

Boxes

Glossary of Terms

Term	Definition
A Levels	A Levels are subject-based qualifications that can lead to university, further study, training or work and are usually assessed by a series of examinations.[1]
Apprenticeship	Apprenticeships provide hands-on experience, a salary and the opportunity to train while working. They enable students to earn a wage while learning at the same time, gain certification equivalent to a qualification from Level 2 to Level 9 and/or to start a career path.[2]
Association of Colleges (AoC)	The AoC is the national voice for Further Education, sixth form, tertiary and specialist colleges in England, with members making up 95% of the sector. It is a not-for-profit member organisation established in 1996 by colleges, for colleges.[3]
Career Pathway	A career pathway (in this research) is a series of structured routes that enable students to advance over time from their education to either training or to an entry-level job.
Courses with a Cyber Security Module	A course with a cyber security module includes courses in a subject area that is not cyber security, but that contains a specialism or module in cyber security. The subject area can be technical (e.g. STEM subject with cyber security) or non-technical (e.g. management with cyber security).
Cyber Security	Cyber security comprises processes, technologies and controls to protect systems, networks and data in the cyber space from cyber-attacks, damage or unauthorised access.[4]
Cyber Security Related Course	A course offered in England at Further Education and Higher Education levels with 'cyber security' in the course title. This also includes course titles that combine cyber security with another technical (e.g. computer science with cyber security) or non-technical subject (e.g. management with cyber security).
Cyber Security Skill	'We define cyber security skills as the combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills that allow organisations to: • Understand the current and potential future cyber risks they face; • Create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation; • Implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face; • Meet the organisation's obligations with regards to cyber security, such as legal obligations around data protection; • Investigate and respond effectively to current and potential future cyber-attacks, in line with the requirements of the organisation

[1] UCAS, 2018, A Levels
[2] Get In Go Far, 2018, About Apprenticeships
[3] Association of Colleges
[4] IT Governance, 2018, What is Cyber Security?

Term	Definition
	This defines the core set of knowledge and skills that organisations need to either have within their workforce, or seek externally (for example, if they outsource their cyber security or take on external consultants). Those working in the wider cyber security industry – developing cyber security products or services, or carrying out fundamental research – may require additional skills, such as the technical expertise and skills needed to research and develop new technologies, products or services.'[5]
Degree-Apprenticeship	Degree apprenticeships are a new type of programme offered by universities, where students can gain a full Bachelor's degree (Level 6) or Master's degree (Level 7) as part of an apprenticeship. These involve students combining work with part-time studies. These programmes are being developed by employers, universities and professional bodies working in partnership. Apprentices are employed throughout the programme, and spend part of their time at university and the rest with their employer. This can be on a day-to-day basis or in blocks of time, depending on the programme and requirements of the employer. They can take between three to six years to complete, depending on the course level.[6]
Entry-Level Job	An entry-level job is the first job a person takes upon completing a Further Education or Higher Education course. An entry-level position may not require some level of work experience and can also refer to the entry point into a given career.
Further Education (FE)	Further Education includes any study after secondary education that is not part of higher education, so that is not part of an undergraduate or graduate degree. This includes courses from basic English to Maths to Higher National Diplomas (HNDs). FE also includes different types of technical and applied qualifications (Levels 2 and 3) to continue general education at advanced level through applied learning.[7]
Higher Education (HE)	Higher education institutions provide a range of courses and qualifications, such as first degrees, Higher National Diplomas (HNDs) and foundation degrees. It includes any qualification at Level 4 and above. A BA or BSc (Hons) degree is a Level 6 qualification. Most courses are taught at universities, but many are also delivered by colleges and specialist course providers, such as conservatoires, business schools and agricultural colleges. Students can take these courses full-time or part-time, in a class-based format, through distance learning, blended learning courses or accelerated degree programmes.[8]
Higher Education Statistics Agency (HESA)	HESA collects and publishes detailed information about the UK higher education sector.
Non-technical Cyber Security Position	A non-technical cyber security position involves tasks that do not require applying specific learned technical abilities. In a non-technical role, an understanding of some knowledge and concepts in cyber security is expected but individuals are not required to create, build-in and use software for their employer. Instead, they use their specific learned abilities in other areas (e.g. project management or policy)
Qualification Levels	There are eight qualification levels that are equivalent to: • **Level 1:** GCSE (grades 1 to 3)

[5] Pedley, D., McHenry, D., Motha, H., Shah, J., 2018, Understanding the UK cyber security skills labour market, Ipsos MORI

[6] UCAS, 2018, Degree Apprenticeships

[7] Gov.uk, 2018, Further Education Courses and Funding

[8] UCAS, 2018, Thinking About Uni?

Term	Definition
	• **Level 2:** GCSE (grades 4 to 9) • **Level 3:** A Levels, access to HE diplomas, advanced apprenticeship, applied general, AS Level, T Levels • **Level 4:** Certification of Higher Education (certHE), higher apprenticeship, Higher National Certificate (HNC) • **Level 5:** Diploma of Higher Education (DipHE), foundation degree, Higher National Diploma (HND) • **Level 6:** Degree apprenticeship, Bachelor's degree • **Level 7:** Master's degree • **Level 8:** Doctorate.[9]
Science, Technology, Engineering, and Mathematics (STEM)	Refers to any subject that falls under the disciplines of science, technology, engineering and mathematics. Cyber security and computer science are included in this category.
Technical or Specialist Cyber Security Position	A technical or specialist cyber security position involves an individual applying specific learned abilities or practical knowledge on software, processes and networks. Skilled cyber security specialists must apply a mix of artistry and technical expertise as they constantly need to be one step ahead of cyber criminals. Typical duties include: building-in security during the development stages of software systems, networks and data centres; looking for vulnerabilities and risks in hardware and software; and building firewalls into network infrastructures.[10]
Technical Levels (T Levels)	T Levels were announced by the government in May 2018 and will be introduced in 2020. T Levels will be equivalent to A Levels and will provide young people with a choice between a technical and an academic education. The only difference being that they will combine provision at an FE institution with a compulsory three-month industry placement. [11]

[9] Gov.uk, 2018, What Qualification Levels Mean
[10] Target Jobs, 2018, Cyber Security Specialist: Job Description
[11] Department for Education, 2018, New T Levels Mark a Revolution in Technical Education

Executive Summary

1. Introduction

With the UK economy becoming increasingly digital, cyber security has become a key priority for national security and is vital to ensuring that the UK is a safe and attractive place to do business. However, cyber security threats are growing both in number and sophistication – it is estimated that around 43% of businesses in the UK experienced a cyber security breach or attack in the last 12 months (2017-18).[12] There is consequently an increasing need for well-trained cyber security professionals, yet supply is not meeting demand for skilled professionals in this field. This reflects a shortage of cyber security professionals worldwide, which was estimated at one million in 2014,[13] and rose to three million in 2018.[14] In the UK, it is thought that more than half of cyber security-related jobs are unfilled at present.[15]

This study aims to understand the role and function of Further and Higher Education institutions in the development of cyber security skills for entry-level jobs. The research was limited to England. The research looked at the educational building blocks available to students wishing to study cyber security and the different career pathways to entry-level jobs available to them. The research also sought to establish the degree of involvement of industry in the development of cyber security courses, as well as the gender diversity/balance at Further and Higher Education levels and in the building blocks for an entry-level job in this field.

2. Methodology overview

The fieldwork for the study started in April 2018 and lasted until September 2018. The research involved a review of academic and grey literature, as well as other material produced by the Government and other organisations to understand what is already known about the cyber security skills gap at the Further and Higher Education levels. This desk research also helped to develop the conceptual framework for the study, namely a typology of cyber security skills and qualifications, the different career pathways, and an insight into the provision of cyber security courses and other courses containing cyber security modules.

An interview programme was conducted with 63 Further and Higher Education representatives, Government Departments, employers and other experts. In addition, an online survey was undertaken, which elicited a response from 91 Further and Higher Education institutions in England. Four focus groups hosted by different FE and HE institutions were held with students to obtain their views on the key research questions. Data on courses and students were obtained and analysed from the Higher Education Statistics Agency (HESA) and the Association of Colleges (AoC) for the past three academic years. Towards the end of the research, a stakeholder workshop was organised to present and discuss the findings from the study with many of those who contributed to the research.

3. Summary of Key Findings

While the provision of Further and Higher Education courses and modules in cyber security is increasing, the research confirms that these types of courses are not sufficiently available to develop the cyber security skills needed to fill entry-level cyber security vacancies in the market.

[12] Department for Digital, Culture, Media and Sport, 2018, Cyber Security Breaches Survey
[13] CISCO, 2018, Annual Security Report
[14] ISC², 2018, Cyber Security Professionals Focus on Developing New Skills as Workforce Gap Widens
[15] CISCO, 2018, Annual Security Report

3.1 Cyber security courses and educational building blocks

The Further Education (FE) sector plays an important role in providing the building blocks for courses in cyber security at the Higher Education level. A number of generalist courses that contain a cyber security module are available to students. However, relatively few FE institutions provide courses purely in cyber security. This is particularly the case at Level 3, since courses are meant to be more generalist at this stage. At the FE level in general, this is often the first-time students come across cyber security as a subject.

At the Higher Education (HE) level, students can opt for a technical or non-technical route into cyber security. The options are to: undertake either a course in computer science and specialise in cyber security; take a generalist or specialist cyber security course; or opt to combine cyber security with another STEM-subject, the most common ones being Mathematics or Engineering. The majority of students who study cyber security have a background in STEM subjects. This is mainly because employers know extra training and skills development for graduates is required, so they look for Maths and Science graduates to fill the gaps left by those without a cyber security academic background.

In the academic year 2016-17, there were 670 FE students on cyber security courses, whilst 47,417 took a course in a field relating to ICT.[16] In the same academic year, there were 5,827 HE students on cyber security courses, whilst 79,905 HE students studied computer science.[17] Around two-thirds of graduates from cyber security degree courses progress to an entry-level role in cyber security or IT.[18]

Students who pursue a non-technical pathway can combine cyber security with a degree in other subjects such as Law, Business or Social Sciences. The multidisciplinary nature of cyber security means there are both technical and non-technical roles available in the cyber security field. However, the skills gaps tend to be greatest for technical roles, reflecting in part the fact that employers face stiff competition for STEM graduates. It is also important to note that it can take many years for an individual to reach the standards required for a highly technical role in cyber security, particularly those identified under CyBOK.[19] Therefore, even if students do pursue cyber security at the FE or HE level, they will need to develop their technical training even further.

More research is needed to understand the extent to which FE and HE institutions have difficulties in recruiting and training researchers, lecturers and other staff with expertise in cyber security. However, there is evidence of difficulties in competing with industry to attract people with the required expertise who can teach the subject.[20]

3.2 Career pathways to entry-level jobs

The research identified six main pathways into entry-level cyber security jobs. It is important to note that these pathways overlap with and are inter-linked across the FE and HE sectors.

For all pathways, employers are aware that they may need to train graduates who are recruited into entry-level jobs to develop the specialised know-how required by cyber security positions. Due to the technical nature of cyber security, highly technical job positions require a lot of training, both as part of FE and HE courses and subsequently as part of a job, even more so if the candidate does not have a cyber security background.

[16] Source: Association of Colleges.
[17] Source: Higher Education Statistics Agency.
[18] Source: Higher Education Statistics Agency.
[19] CyBOK (The Cyber Security Body of Knowledge) is an ongoing project to bring cyber security into line with the more established sciences by distilling knowledge from major internationally-recognised experts.
[20] Source: Interview programme with FE and HE representatives.

As such, to fill the skills gap, a consideration for employers is to recruit 'rounded' individuals with a basic foundation in cyber security, which can be built on to develop more specialised skills. Most employers are open to different types of backgrounds for entry-level technical positions to fill this gap. Some employers reported that there is a preference for STEM degrees. and, indeed, a degree specifically in cyber security is not essential in the market currently. This is not only due to the current shortage of skills in the labour market but also because employers value a solid background in how networks, software and systems work more generally. Students from other STEM disciplines develop specific skills and a type of mindset that is applicable to the cyber security field, particularly since it is a relatively new discipline.

According to HESA, around two-thirds of those studying cyber security progress to a role in cyber security or IT more generally. The remaining tend to go into management, academia or other jobs in a different field un-related to cyber security. Employers still need to look to those outside of this pool to fill their skills gaps.

3.3 How cyber security courses are developed and industry's role

The decision by FE and HE institutions to provide courses and/or modules in cyber security is mainly driven by demand and the capacity they have to deliver these courses.

When considering whether or not to apply for an FE or HE course in cyber security, many students consider the provider's links with industry as an important factor influencing their decision to pursue a given course (e.g. NCSC certification). The nature of industry involvement ranges from being closely involved in delivering modules and certification, providing placements, apprenticeship schemes and industry seminars and events, to simply recruiting cyber security graduates.

There are conflicting perceptions on how FE and HE establishments keep up with cyber security developments. Students sometimes feel that the equipment and software they use is out of date. For their part, even though employers are generally happy with the content of courses, some claim that academia is unable to keep up-to-date with the latest cyber security developments and the threats facing businesses, Government and other organisations. Some of those representing FE and HE establishments argue that employers have unrealistic expectations regarding the skills that students can learn on a course given the duration of courses, the specialised technical knowledge needed in cyber security and rapid technological advances in the field.

3.4 Gender balance in cyber security

The research for this study indicates that the gender imbalance in cyber security is still a significant issue, despite measures to encourage more women into the field. Most of the feedback confirms existing research, namely that cyber security is still dominated by stereotypes and widely perceived as a male-dominant field.

At the FE level, 13.1% of students that identify as female undertook A Level 3 class-based course in the ICT subject area in 2016-17 according to data from the Association of Colleges (AoC). The data indicates that 16.6% fewer women enrolled in those courses in 2016-17 compared to 2014-15. According to the HESA data, approximately 16% of students that undertook a cyber security degree in 2016-17 identified as female. The percentage of female enrolment in these courses has remained steady, at these levels over the past three academic years.

The situation with regard to the gender imbalance in cyber security courses reflects the wider situation for STEM-related degrees more generally. According to the HESA data, only 17.5% of female students in England were studying engineering and 16.5% studied computer science in 2016-17. This suggests that the gender imbalance is a characteristic of the student population enrolled in other subjects that can also lead to a career in cyber security. The study suggests that one important factor leading to the gender imbalance is the perception that cyber security is male-orientated and 'geeky'. The low participation of female students in courses relevant to cyber security and the low awareness of the career opportunities in the field (which affects both women and men), limits the flow of female recruits into cyber security roles.

The research highlights the importance of the terminology that is used to define cyber security courses, modules and extra-curricular activities. Some FE and HE institutions have been able to attract more female applicants by rebranding what a career in this field is really like. Namely they use more gender-neutral language in their course descriptions and marketing materials.

1 Introduction

1.1 Study objectives and scope

The purpose of this study has been to examine the current role and function of Further Education (FE) and Higher Education (HE) in supporting the flow of students into entry-level cyber security jobs in England. The research also examines the gender balance among students enrolled in FE and HE courses that form the building blocks of a career in cyber security. The four specific research questions investigated were:

Key Research Questions
• What are the **educational building blocks** and cyber security related skills/associated knowledge that are currently being taught in FE and HE? • Is there is a **gender imbalance** amongst men and women in the building blocks, stated above, and what is the scale and scope of any imbalance? • What are the various **career pathways** that are available to students to enable them to access an entry-level role in a cyber security team? • **How are cyber security courses and modules developed** (e.g. with/without industry) and what are the different audiences' ideas on the skills/length of training/education required for an entry-level cyber security job?

There are 280 FE institutions and 109 universities in England, which means a total of 389 FE and HE educational establishment fall within the scope of this study. The study suggests that 26 FE institutions are unlikely to have a role in the development of cyber security skills in the future because they focus on other subjects[21]. This brings down the total of FE and HE establishments to 363.

In this study, **cyber security** has been defined as a set of techniques designed to protect systems, networks and data in cyber space. It comprises processes, technologies and controls to protect such systems, networks and data from cyber-attacks, damage or unauthorised access.[22] **Further Education** has been defined as any study after secondary education (not part of Higher Education or a graduate degree). FE can also include different types of technical and applied qualifications (Levels 2 and 3) that allow students to continue to general education at an advanced level.[23] **Higher Education** institutions provide a range of courses and qualifications, such as first degrees, Higher National Diplomas (HNDs) and foundation degrees. HE includes any qualification at Level 4 and above after completion of secondary education.[24] An **entry-level job,** in the context of this research, refers to a position that does not require previous experience in a given field and is often one of the first positions that is taken upon completing a degree or diploma. However, an entry-level position can also refer to the entry point into a given career.

[21] Two-thirds (186) of the 280 FE institutions are described as 'general' FE; almost a quarter (68) are sixth form colleges; and the remainder are either land-based colleges (14), (two) specialise in art, design and the performing arts; the remainder (10) are 'specialist designated'.
[22] IT Governance, 2018, What is Cyber Security?
[23] Gov.uk, 2018, Further Education Courses and Funding
[24] UCAS, 2018, Thinking About Uni?

1.1.1 Background to the research

With the UK economy becoming increasingly digital, cyber security is vital to national security and has an important role to play in ensuring that the UK is a safe and attractive place to invest and do business.[25] Breaches of cyber security can be very detrimental, with one estimate suggesting that around 43% businesses in the UK have experienced a cyber security breach or attack in the last 12 months (2017-18).[26]

Moreover, the threat to the UK's cyber security is growing. Cyber-attacks are increasing at a rapid rate.[27] They pose significant threats to businesses, such as lost revenues and intellectual property, data theft, disrupted communications and being unable to operate effectively as a business.[28] More broadly, with people sharing more personal information, conducting more of their lives online and interconnecting their everyday objects with the Internet, cyber-attacks are a threat to privacy and how we conduct our daily lives.

The UK's ability to defend itself in cyber space depends on a strong and appropriately sized skills and knowledge base in the cyber security field. Although difficult to quantify, there appears to be an agreement amongst most observers that the UK faces a growing shortage of cyber security professionals. For example, a survey by Ipsos MORI in 2018, found that 54% of businesses, 54% of charities and 18% of public sector organisations have a basic technical cyber security skills gap.[29] Regarding the reasons for these skill gaps, the IISP Cyber and Information Security Profession survey revealed that the availability of experience, resources, new entrants and skills were of significant concern amongst professionals in the industry in 2017-18.[30] Similarly, the Shadbolt Review of Computer Sciences Degree Accreditation and Graduate Employability (2016) found that one of the major issues that impacts the employability of recent graduates of computer science in the UK is the lack of specific skills, soft skills and project management skills.[31] It seems many potential job applicants with the necessary technical skills often lack the wider skillset required in many cyber security roles. Indeed, the 2016 CSIS survey of IT decision-makers found that skill shortages were acute for technical skills, particularly intrusion detection, attack mitigation software development, as well as for non-technical skills, particularly effective communication.[32]

The shortage of cyber security qualified professionals worldwide was calculated at one million in 2014[33] and at three million in 2018.[34] This shortage is projected to grow to 1.8 million by 2022.[35] The UK is not an exception to this trend. According to CISCO, more than half of cyber security related jobs go unfilled in the UK[36] and there could be a shortage of 100,000 cyber security professionals by 2022.[37] The Tech Partnership has estimated that vacancies increased by 18% in 2017 compared with 2016 to around 7,000 per month. The same source indicates that there were some 58,000 professionals working in the cyber security field, up from 22,000 in 2011 but still not meeting demand.[38] The shortage of cyber security experts is partially explained by the gap

[25] Department for Digital, Culture, Media and Sport, 2017, Policy Paper, A Safe and Secure Cyberspace – Making the UK the Safest Place in the World to Live and Work Online
[26] Department for Digital, Culture, Media and Sport, 2018, Cyber Security Breaches Survey
[27] Symantec, 2018, Internet Security Threat Report
[28] FSB, 2016, Cyber Resilience: How to Protect Small Firms in the Digital Economy
[29] Pedley, D., McHenry, D., Motha, H., Shah, J., 2018, Understanding the UK Cyber Security Skills Labour Market, Ipsos MORI
[30] IISP, 2018, The Cyber and Information Security Profession in 2017/2018
[31] Shadbolt, 2016, Shadbolt Review of Computer Sciences Degree Accreditation and Graduate Employability
[32] Centre for Strategic and International Studies, 2016, Hacking the Skills Shortage, McAfee. Quoted in Pedley, D., McHenry, D., Motha, H., Shah, J., 2018, Understanding the UK Cyber Security Skills Labour Market, Ipsos MORI
[33] CISCO, 2014, Annual Security Report
[34] ISC², 2018, Cyber Security Professionals Focus on Developing New Skills as Workforce Gap Widens
[35] ISACA, 2015, Global Cyber Security Status Report – UK data
[36] Indeed Blog, 2017, Indeed Spotlight: The Global Cyber Security Skills Gap
[37] Centre for Cyber Safety and Education, ISC², 2017, Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk, A Frost & Sullivan Executive Briefing
[38] Tech Partnership, 2018, Tech Partnership Legacy

between the skills demanded by employers and those that graduates have after completing their studies.[39] More generally, the shortage of cyber security professionals should be seen in the context of the digital divide, in which up to 12.6 million of the adult UK population lack basic digital skills.[40]

1.1.2 UK cyber security context setting

The 2016 Government's **National Cyber Security Strategy (NCSS)** sets the vision of ensuring that by 2021 'the UK is secure and resilient to cyber threats, prosperous and confident in the digital world'.[41] To support the NCSS, some of the funding, totalling £1.9bn, is being made available over the period 2016-21 to help ensure that the UK has the next generation of cyber security professionals.

Within this, the establishment of the **National Cyber Security Centre (NCSC)** in 2016 is a key part of the strategy. The NCSC provides a 'single, central body for cyber security at a national level', which acts as the public face of the Government's action against cyber threats.[42] It works closely with industry, academia and international partners to help protect the UK against cyberattacks. It is also playing a key role in helping to ensure that the UK has the skills needed to tackle cyber threats.

1.1.3 Collaboration between public sector, education and industry

The NCSS places a lot of emphasis on the need for education and training providers, and industry, to work together to tackle the problem of a shortage of cyber security skills. There are already a number of initiatives bringing together the public sector, industry and academia to help address the shortage of cyber security skills. The 'Cyber Security Skills: A Guide for Business' publication provides guidance to industry on how firms can collaborate with academia in order to contribute to the development of skills.[43] This work has been furthered by the creation of the government-backed schemes **Cyber Essentials** and **Cyber Aware** to help industry protect itself from cyber-attacks.

One initiative linking industry and academia – the **Cyber Security Body of Knowledge (CyBOK)** – aims to codify the foundational and generally recognised knowledge in the area of cyber security following a broad engagement with academia and industry. Funded by the National Cyber Security Programme (which underpins the NCSS) and led by cyber security experts, CyBOK has published a list of 19 key knowledge areas (KAs), which will be developed in more depth leading to the publication of a CyBOK document in 2019.[44]

Another initiative is the **Institute of Coding**, which is supported by the Higher Education Funding Council for England (HEFCE).[45] The Institute of Coding is a community of learners, businesses and educators creating new ways to develop the digital skills needed at work and beyond. The institute aims to develop and deliver innovative, industry-focused Higher Education across the UK. It helps to develop accredited degree schemes and short courses for professionals across a wide range of sectors. The Institute of Coding also works to increase the participation of women, returners to work and hard-to-reach groups.

---

[39] The Information Assurance Advisory Council's (IAAC) report into the cyber security profession explains that cyber security addresses security and privacy on computer networks, online services and other technical aspects of computing, but also involves a wider appreciation of human behaviour and the environment we live and work in. Source: IAAC, 2017, The Profession - Understanding Careers and Professionalism in Cyber Security

[40] House of Commons, 2016, Digital Skills Crisis – Second Report of Session 2016-17

[41] Cabinet Office, 2016, National Cyber Security Strategy 2016 to 2021

[42] Ibid.

[43] HM Government, 2014, Cyber Security Skills: A Guide for Business

[44] CyBOK (The Cyber Security Body of Knowledge)

[45] Institute of Coding

Other initiatives in the UK link industry with teaching professionals, such as the **STEM Ambassadors.**[46] This scheme provides volunteers from a variety of STEM disciplines across the UK to provide mentorship and support to teachers engaging with young people.

CyberFirst is a government-led cyber security skills initiative to develop the UK's next generation of cyber professionals via a series of student bursaries, graduate apprenticeships, courses for 11-18-year olds and competitions.[47] Another part of CyberFirst is **Cyber Discovery**, which consists of four phases, all involving challenges, tasks and games designed to improve the cyber security knowledge for students aged 14-18 years.[48] There are also a range of similar initiatives across Europe[49] and the USA.[50]

The rapidly evolving threat landscape demands continuous learning and adaptation by professionals. The 'Roadmap for NIS Education Programmes in Europe' highlights the importance of continuous education in Network and Information Security (NIS) and provides various roadmaps of how this could be implemented.[51] The NIS focuses on large organisations that are a part of a country's critical national infrastructure.

Internationally, work has also taken place to understand what cyber security involves through the **Joint Task Force on Cyber Security Education** (JTF). The JTF promotes collaboration between international computing societies to develop comprehensive curricular guidance in cyber security education for use by academic institutions worldwide (e.g. United States, Israel). The result of this collaboration is the Cyber Security Curricula 2017 (Curriculum Guidelines for Post-Secondary Degree Programmes in cyber security).[52] The guidelines highlight the emergence of cyber security as a discipline but also its interdisciplinary nature encompassing subjects such as risk management, human factors, ethics, law and public policy. It is recommended that curricular content should combine theoretical knowledge with opportunities to apply this knowledge. An analysis by Cabaj et al. (2018) has found that Master's programmes offered by a number of top universities are aligned with the Cyber Security Curricula 2017 and highlighted that areas such as human, organisational and societal security are of increasing importance within such programmes.

1.2 Methodological approach

The study started in April 2018 and was completed over a six-month period. The research plan was divided into three main tasks:

- **Task 1:** Preparatory Tasks (April 2018);
- **Task 2:** Field work - Survey, interviews and focus groups (April 2018 – September 2018);
- **Task 3:** Final report and workshop (October 2018).

[46] STEM Ambassadors
[47] CyberFirst
[48] CyberDiscovery
[49] Facebook Newsroom, 2018, Training 1 Million People and Small Businesses in Europe by 2020
[50] National Institute of Standards and Technology, U.S Department of Commerce, 2017, National Initiative for Cyber Security Education (NICE) – Cyber Security Workforce Framework
[51] European Union Agency for Network and Information Security, 2014, Roadmap for NIS Education Programmes in Europe
[52] Cyber Security Curricular Guidelines – CSEC 2017

The preparatory tasks included a kick-off meeting and interviews with the steering group. It also involved a **literature review,** which examined material on the existing provision of cyber security courses and other courses containing cyber security modules.[53] The degree and quality of cyber security and cyber security elements within computer science or other STEM subjects was not looked at in this research. The review summarised existing initiatives undertaken by industry and Government to help reduce the cyber security skills gap. It also helped to develop a typology of cyber security skills and qualifications, the different career pathways, and provided an insight into the provision of cyber security courses and other courses containing cyber security modules. The **desk research** continued into Phase 2 of the assignment. Data on FE cyber security courses and ICT enrolment over the past three academic years (2014-2017) was obtained from the Association of Colleges (AoC). Data on HE cyber security courses and trends in cyber security enrolment over the past three academic years (2014-2017) was obtained and analysed from the Higher Education Statistics Agency (HESA).

Interviews were conducted with FE and HE representatives, Government Departments, employers and other key stakeholders. The FE and HE interviews involved course directors, senior lecturers and professors teaching cyber security. Lecturers and professors were generally recommended by course directors and/or identified online in staff directories or through a telephone call to the institutions. Employers and other key stakeholders were often contacts recommended by FE or HE representatives, Government Departments or identified online. Other employers were identified at the Manchester CyberUK Conference in April 2018, which was attended by members of the study team. In total, 63 people were interviewed either face-to-face or by telephone.[54] Members of the study team also participated in a meeting of the Association of College's Technology Group.

An important element of the research was an **online survey of FE and HE institutions.** It was launched on 12 June 2018 and elicited a response from 91 FE and HE institutions across England.[55] The objective was to obtain responses from a representative sample of institutions in each of the three groups making up the typology of cyber security course providers (see Section 2.2).[56] In some cases, the necessary contact details (i.e. email address) could be obtained online on staff directories but in many cases – especially in relation to the FE sector – it was necessary to contact the institutions individually by telephone. Heads of department, senior lecturers, lecturers and professors were targeted in the survey to obtain different perspectives on the development of cyber security skills at FE and HE levels. A summary of the interview and survey coverage is provided below.

Table 1.1: Summary of the interview programme and survey

Target groups	Interviews	Survey	Total
Higher Education	27	61	86
Further Education	8	16	24
Employers	10	0	8
Other experts	18	14	32
Total	**63**	**91**	**151**

Note: In the survey, 76 respondents identified their institutions. 14 FE and HE respondents have been classified as 'other' because it is not clear which institutions they represented or whether they were from FE or HE establishments.

[53] Approximately 50 documents were reviewed including articles from academic journals, private industry and Government reports. These sources were selected because they answered the four research questions and were within the scope of the study. Sources were also selected based on how updated the information was.

[54] 180 stakeholders were contacted during the course of this study but not all were able to contribute to the research.

[55] A total of 482 contacts were identified and subsequently invited to complete the online survey.

[56] The three groups making up this typology of courses include: (1) NCSC-certified degrees; (2) other providers of cyber security courses; (3) providers of courses that include a cyber security module or speciality.

To investigate certain issues in more depth, four **focus groups** were held with students. These were hosted by Exeter College; Ada, the National College of Digital Skills in London; and the University of Oxford. Another focus group was held in conjunction with a CyberFirst Advanced course for 16 to 17-year-olds which took place at Imperial College London. The focus groups were each typically attended by between 10-15 young people. The discussion focused on the students' perspective on the four key research questions.

Towards the end of the research, the research findings were triangulated and a **stakeholder workshop** was organised in London. This was attended by approximately 20 representatives of FE and HE institutions, employers, Government Departments and other experts in the cyber security field. The workshop provided an opportunity to present the emerging findings from the research and to discuss the draft conclusions and recommendations in relation to each of the four research questions.

2 Cyber Security Courses & Educational Building Blocks

2.1 Cyber security courses in the Further Education sector

A significant proportion of those who work in the cyber security field start by studying for a qualification at an FE institution. Pupils aged 16 to 18-years-old or older enter FE institutions where they can study for A Levels, an applied general qualification or a technical qualification. Pupils on the FE route can pursue a Higher National Diploma (HND), a Higher National Certificate (HNC), a BTEC or continue on to HE. For many FE students on relevant courses, an FE course is the first time that they undertake any formal learning in cyber security. In that way, FE can serve as the first step and a key building block towards a career in cyber security.

Many FE students who participated in the focus groups chose to study cyber security because they thought it would be fun and a hands-on discipline. Many also quoted recent stories covered in the news as a source of inspiration to pursue cyber security.

> *"Cyber security is very relevant in today's world – most banks use apps, we can pay with our phones, etc. You read a lot about it on the news, so it is exciting field to get into" –*
>
> FE Student (focus group)

> *"I chose to do the HND diploma in IT Systems & Networks because it is general enough to provide a broad understanding on cyber security"*
>
> FE Student (focus group)

FE typically provides 16 to 18-year-olds with the qualifications (e.g. A Levels) needed to go on to study at HE level, for example to pursue a degree at university in a cyber security-related field. A considerable number of other FE courses also include cyber security as a module in other generalised courses (e.g. computer science). Many FE students undertake apprenticeships, which can also lead on to entry-level jobs in cyber security.

There are some courses specifically on cyber security for students at Levels 2 and 3. For example:

- BTEC Level 2 Technical Diploma in Digital Technology (Networking and Cyber Security) (Awarding body: Pearson), which covers topics such as common practices in network security and ethical hacking;[57]
- IT (Networking and Cyber Security) - Level 3 Extended Diploma (Awarding body: Edexcel; Provider: Newcastle College). This course has been specifically designed for companies training their employees;[58]
- BTEC Level 3 90 credit Diploma/Extended Diploma in IT - Cybercrime & Security (Awarding body: Edexcel; Provider: Uxbridge College);
- BTEC Level 3 Computing and Cyber Security (Provider: South & City College Birmingham);[59]
- Level 3 Extended Project Qualification (EPQ) in Cyber Security (Awarding body: City & Guilds; Provider: Qufaro).[60]

[57] Pearson, 2018, BTEC Level 2 Technicals – Digital Technology
[58] Hotcourses, 2018, IT (Networking and Cyber Security) – Level 3 Extended Diploma (Full-Time)
[59] South & City College Birmingham, 2018, Computing and Cyber Security Level 3
[60] Qufaro, 2018, Extended Project Qualification in Cyber Security

Box: 2.1: Case example: Qufaro remote provision of cyber security further education

- Qufaro is a not-for-profit organisation created by representatives of Raytheon, BT Security, the Institute of Information Security Professionals and the National Museum of Computing. The vision of Qufaro is to create a National College of Cyber Security based at Bletchley Park and serving residential and day students but also providing education remotely via an online platform.
- For three years, Qufaro has provided a Level 3 Extended Project Qualification (EPQ) in cyber security, which is certified by City and Guilds. Topic areas are based on the National Occupational Standards in cyber security and reflect requirements as defined by industry experts. The EPQ consists of a one-year course leading to a Level 3 vocational qualification that can help students gain employment or progress to university (through the award of UCAS points). Students learn about a broad range of cyber security issues (e.g. law, supply chain, human resources, psychology, commercial considerations) before focussing on one topic in-depth through an essay and a project. The EPQ is recognised by the Institute of Information Security Professions (IISP).
- The first pilot was launched in 2016 with 60 students. In 2017, a total of 80 students followed the course, which was provided free of charge thanks to sponsorship by Deloitte. Heart of Worcester College hosts the EPQ online platform, which includes videos from the National Crime Agency (NCA), industry and academia. The course is delivered online with additional support provided by supervisors. Schools and FE institutions supervise about two-thirds of the students, who are typically doing the EPQ alongside 3 A Levels. In those cases, the schools and FE institutions pay Qufaro for access to the platform. The other students are independent learners who are supervised by PhD students at Royal Holloway. Some of those independent learners are employees, whose employers have paid for them to do the course.
- In September 2018, Qufaro signed an agreement with GK Apprenticeships (GKA) regarding a proposal to jointly develop and deliver apprenticeships with a cyber security dimension at Levels 3 and 4. The proposed apprenticeships would be offered to employers of all sizes and be delivered by a mix of on-line learning and on-site provision at Bletchley Park.[61]

Evidence from interviews with FE representatives and data from the Department for Education (DfE) suggests that a majority of FE students go on to universities to study for a degree at some point, either straight after completion of secondary education, via a top-up course or a foundation degree.[62] Very few students go straight from an FE institution into an entry-level cyber security-related job.

Feedback from the different focus groups suggested that in general, students want to pursue a degree following the completion of their FE course. Many students are keen to pursue a top-up degree course, which is generally completed after one year at university. One student who took part in a focus group was disappointed because two highly-ranked universities wanted to extend their top-up course to two years:

> *"My HND diploma was not considered to be good enough to study cyber security at these two universities, so I wasn't accepted by the universities to do a one-year top-up course"*
>
> FE Student (focus group)

A new qualification at Level 3, or equivalent to A Levels, was announced by the government in May 2018. These are called T Levels and will combine provision at FE institutions with a compulsory three-month industry placement. The course content will be developed by an expert

[61] Qufaro, 2018, Bletchley Park Qufaro and GK Apprenticeships Work in Partnership to Deliver Cyber Security Apprenticeships

[62] Department for Education, 2016, Adult Further Education: Outcome-Based Success Measures

panel of employers, whilst standards will be assured by the Office of Qualifications and Examinations Regulation (Ofqual) and the Institute for Apprenticeships (IfA). Pilots of T Levels are expected to start from September 2020 at 54 selected institutions across England.[63] The intention is that T Level qualifications will be broken down into a number of specialisms which students can select to build the appropriate skills for their chosen careers.

Digital skills are one of the first areas in which T Levels will be offered (the others being construction and education and childcare). Digital T Levels are being developed with the support of three employer panels: Data and Digital Business Systems; IT Support and Services; and Software Design and Development. The first digital T Level will be in Software Applications Design, which may therefore include a focus in cyber security. As T Levels have not yet been piloted, there was no concrete evidence available when the research for this study was conducted regarding their likely impact on the cyber security profession and the skills gap. The consultees for this study were broadly in favour of the principles underpinning T Levels. However, a few of the FE representatives consulted for this study highlighted the potential difficulty in ensuring a sufficient number of industry placements in cyber security, particularly in geographical areas with few employers in this field.

Within the FE sector, students have the choice to undertake a course in the ICT subject area, which includes generalist IT, Computer Science and Technology courses that may contain some elements in cyber security. These can help students gain the basic skills to pursue further studies or work in the cyber security field, however, it is important to note that a background in a generalist ICT subject is not enough to close the skills gap for technical cyber security professionals. Since the skills gap tends to be greater for technical roles, other STEM graduates are in high demand from employers in many fields. Often, it is from this generalist background that the first-time students come across and are able to understand 'what is cyber security'.

Data obtained from the Association of Colleges indicates that in 2016-17, a total of 47,417 students were undertaking class-based courses for a qualification in the ICT subject area.[64] Table 2.1 indicates that the number of students on class-based courses in computer science and related subjects has fallen by nearly 10% in recent years. Some 95% of FE institutions are represented by the AoC. Based on the Individualised Learner Record (ILR), which FE institutions use to collect, return and check learner data, Table 2.1 provides a breakdown of students on Level 3 class-based courses in fields relating to ICT.

Table 2.1: Students on Level 3 class-based courses in the ICT subject area

Year	2014-15			2015-16			2016-17		
Qualifications	Female	Male	Total	Female	Male	Total	Female	Male	Total
Access to HE	76	570	**646**	87	599	**686**	101	646	**747**
Certificate	776	2,592	**3,368**	847	2,957	**3,804**	706	2,664	**3,370**
Diploma	3,254	28,501	**31,755**	3,161	27,680	**30,841**	2,806	25,219	**28,025**
A Level	3,071	11,736	**14,807**	2,609	10,778	**13,387**	2,106	9,818	**11,924**
Other[65]	245	1,731	**1,976**	207	1,668	**1,875**	469	2,882	**3,351**
Totals	**7,422**	**45,130**	**52,552**	**6,911**	**43,682**	**50,593**	**6,188**	**41,229**	**47,417**

Source: Association of Colleges[66]

[63] Education & Skills Funding Agency, 2018, Providers Selected to Deliver T Levels in Academic Year 2020 to 2021

[64] The data did not look at other types of courses.

[65] This includes BTEC's and Foundations. In 2016-17, there were 1,107 students (141 female; 966 male) taking a BTEC course. In the same year, 25 students took a foundation course (2 female and 23 male). It is important to note that BTECs and foundations have been available for many years, but were only added on the learning database aims in 2016-17.

[66] Table 2.1 categorised Level 3 courses into seven groups based on qualification type. These include diplomas, certificated, foundations, A Levels, BTECs and others (e.g. other regulated and other non-regulated).

For students taking a Level 3 course, just over 6% were taken in ICT, with 670 studying for a qualification specifically in cyber security at all levels. A total of 23 courses made up the 670, which largely focuses on cyber security, with subject titles including 'IT for users', 'Computer Security and Privacy' and 'Network Security'.

In 2016-17, the majority of FE students on courses that are relevant to this research were studying for either a Diploma or an A Level qualification (45.3% and 25.1% respectively). A total of 13.1% of the pupils were female. In addition to class-based courses, data from the Department for Education indicated that in 2016-17, a total of 15,470 students were undertaking apprenticeships in the ICT subject area. In 2017-18, provisional figures show that 18,030 students were taking an apprenticeship in the ICT subject area. This suggests that there has been a 14% increase in students starting an apprenticeship in ICT at all levels from 2016-17 to 2017-18.

Table 2.2: Apprenticeships in ICT

Apprenticeship type	2016-17 Full Year	2017-18 Full Year (Provisional)
Intermediate Apprenticeship	3,630	3,710
Advanced Apprenticeship	9,520	10,300
Higher Apprenticeship	2,330	4,020
Totals	**15,470**	**18,030**

Source: Department for Education

According to the AoC data, the number of FE students classified as 'ICT practitioners' has increased sharply from 1,495 (2015-16) to 9,565 (2016-17). A total of 15% of students identified as female in 2016-2017. These courses are at different levels and represent reformed apprenticeships.

Table 2.3: ICT practitioners attaining standards in cyber security related fields at various levels

Year	2015-2016			2016-17		
Standards	Female	Male	Total	Female	Male	Total
Infrastructure Technician (Level 3)	10	280	290	300	4,020	**4,320**
Digital and Technology Solutions Professional (Level 6)	130	570	700	340	1330	**1,670**
Network Engineer (Level 4)	50	460	500	80	1180	**1,260**
Digital Marketer (Level 3)	0	*5	*5	510	510	**1,020**
Software Development Technician (Level 3)	0	0	0	40	330	**370**
Unified Communications Technician (Level 3)	0	0	0	*5	330	**335**
Cyber Security Technologist (Level 4)	0	0	0	30	190	**220**
Data analyst (Level 4)	0	0	0	50	100	**150**
IT Technical Salesperson (Level 3)	0	0	0	30	50	**80**
Software Tester (Level 4)	0	0	**0**	20	60	**80**
IS Business Analyst (Level 4)	0	0	**0**	30	10	**40**
Cyber Intrusion Analyst (Level 4)	0	0	**0**	0	20	**20**
Total	**190**	**1,315**	**1,495**	**1,435**	**8,130**	**9,565**

*Source: Association of Colleges data (*The data for less than 5 is deliberately suppressed. The numbers are rounded due to publication rules.)*

There is a limited number of specific cyber security courses available at this level. Some of these include the:

- Level 3 Extended Project Qualification (EPQ) in cyber security (Qufaro);
- Level 4 Cyber Intrusion Analyst;
- Level 4 Cyber Security Technologist;
- Level 6 Cyber Security Degree Apprenticeship.[67]

This demonstrates that at this level, students tend to build up the background knowledge needed in subjects, such as Computer Science, Maths, or other ICT courses, which are all an important route for students to start developing some of this foundational knowledge before undertaking a specific cyber security course. It is important to highlight that a generalist Computer Science, Maths or ICT course does not give students the specialised technical skills or training in cyber security for an entry-level role. These provide a potential pool of students, that can develop cyber security knowledge and skills at a later stage through training or further study.

2.2 Cyber security courses in the Higher Education sector

At the HE level, there is a number of HE courses and modules that focus on or that can be combined with cyber security at undergraduate and postgraduate levels. Degrees in cyber security-related fields include: generalist computer science courses with a module or specialism in cyber security (e.g. 'Computer Science with Cyber Security'); cyber security generalist or specialist courses (e.g. Cybernetics, Digital Forensics); STEM subjects with a module or specialism in cyber security (e.g. Engineering with Cyber Security); or non-technical courses with a cyber security module or specialism, such as Management, Business Studies or Psychology with Cyber Security. It is also important to note that the degree and quality of cyber security and cyber security elements within computer science or other STEM subjects was not looked at in this research.

A typology of HE cyber security courses was developed as part of this study to reflect the different type of course provisions:

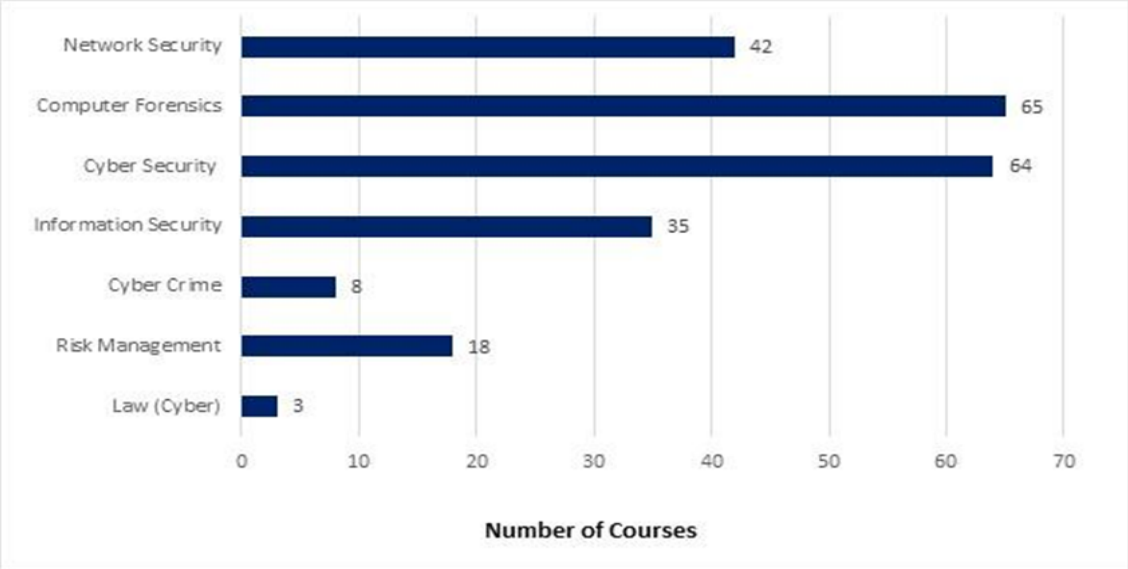
Box: 2.2: Typology of Cyber Security Courses

- **Group 1: NCSC-certified degrees in cyber security:** At time of writing, this includes 23 one-year postgraduate Master's degrees, 19 of which are in England. At undergraduate degree-level there are three Integrated Master's courses and two Bachelor's courses, all of which are in England. Applications for universities certification are assessed by a panel of experts from across industry, academia and government. The panel assesses whether the courses offer a well-defined and appropriate degree content, and are delivered to the highest standard. The purpose of certification is to help employers to recruit and develop skilled staff, help universities to attract high-quality students and to enable students to make better-informed choices when applying for a course.[68]
- **Group 2: Other providers of cyber security courses** - UCAS suggests that there are 43 HE institutions in total that provide degree courses at both Bachelor's and Master's levels in cyber security in England. This also includes degrees certified by the NCSC. UCAS only identifies one Higher National Diploma (HND) HE course in cyber security at Coventry University. Other courses in cyber security are available outside England.
- **Group 3: Providers of courses that include a cyber security component** – this includes: (a) courses labelled as 'computer science' but that offer cyber security as a core or optional module; (b) other courses offering a cyber security component but that do not carry the label as such (e.g. engineering, or other STEM subjects). The number of HE institutions in this group is difficult to estimate precisely but many of the other bodies not included in Groups 1 and 2 provide computer sciences, information technology and other courses that might include a cyber security component.

[67] There is currently no data for this apprenticeship as it was launched in September 2018.
[68] National Cyber Security Centre, 2018, NCSC-certified degrees

Figure 2.1 shows the number of Bachelor's and Master's degrees in the cyber security field. As can be seen, the vast majority of degrees with a cyber security module are STEM-based. It is worth noting that degrees in Business Administration (i.e. risk management class) have a high number of modules which include cyber security.

Figure 2.1: Categorisation of HE cyber security courses and courses that have a cyber security module or component at undergraduate and postgraduate levels in England (2014-2017)



Source: HESA

2.3 Profile of cyber security courses and students

Many of those who go on to entry-level jobs in cyber security study subjects in IT or in a related field. UCAS identifies 2,369 HE courses in computer science at undergraduate and postgraduate levels in England and 110 in cyber security.[69] It is worth noting that many cyber security professionals originate from other disciplines, mainly in STEM-related areas, such as maths or engineering. This is because students develop specific skills and a type of mindset that is applicable to the cyber security field and also due to the relatively new nature of the discipline. The following table provides a breakdown of the number of cyber security and computer science courses in England in the last academic year:[70]

Table 2.4: Number of cyber security and computer science courses in England (2017-18)

Qualifications	Cyber Security	Computer Science
Foundation degrees	5	121
HNC or CertHE	0	9
HND or DipHE[71]	1	30
Undergraduate	46	1,493
Postgraduate	59	716
Total	**110**	**2,369**

Source: UCAS. Some courses in the table include cyber-crime and forensics as they may lead to an entry-level cyber security role.

[69] These numbers are based on UCAS' course finder.
[70] Table 2.4 reflects the number of courses at the time when the research was undertaken.
[71] Coventry University offers a Cyber Security course (HND Diploma).

2.3.1 Students studying cyber security

Table 2.5 shows that **15,356 students graduated from an HE institution with a degree in a cyber security-related field in England over the past three academic years.** Of these students, 10,384 were undergraduates and 4,972 were postgraduates. Over this period, there was a 22% increase in the number of postgraduates and a 31% increase in the number of undergraduates undertaking a cyber security-related course.

Table 2.5: Number of students graduating from a cyber security related course by degree level

Level of study	2014-15	2015-16	2016-17	Total
Postgraduate	1,508	1,629	1,835	4,972
Undergraduate	3,057	3,335	3,992	10,384
Total	**4,565**	**4,964**	**5,827**	**15,356**

Source: HESA.

Over the past three academic years, 80% of students graduating from a HE institution with a degree in a cyber security related field in England were from the UK, 5% from the EU and 15% from outside the EU. Over this period, the percentage of students from the UK has increased, the percentage from the EU has been stable and the percent from outside the EU has dropped. This is mainly driven by an increase in UK students from 3,513 in 2014-15 to 4,851 in 2016-17, although non-EU student numbers dropping from 818 to 679 over this period also contributed to this trend.

Table 2.6: Percentage of students graduating from a cyber security related field by domicile

Domicile	2014-15	2015-16	2016-17	Total
UK	80.2%	79.2%	83.5%	80.2%
Other-EU	4.9%	4.9%	4.9%	4.7%
Non-EU	14.6%	15.9%	11.7%	14.9%

Source: HESA.

As noted in Section 1, **the provision of HE cyber security courses has increased in recent years, reflecting growing demand.** This was confirmed by representatives of HE Institutions who indicated that the demand for places to study cyber security has increased and that this trend is likely to continue in the future. This trend has been seen in course-enrolments but also in other evidence of an increased interest in the topic of cyber security, for example through increased attendance at open days.

The demand for places to study cyber security has been partly stimulated by the publication of the UK's National Cyber Security Strategy, which has led to a growing awareness of cyber security in the public and private sectors, as well as increased demand for skilled workers. This was further confirmed by the survey responses. In fact, one HE representative claimed that:

> *"The UCAS points for the entry to their university has not changed, yet the size of cyber security classes has doubled".*
>
> Higher Education representative

Common survey responses also revealed that the demand increased due to "raised public awareness and visibility" and it being "a current hot topic in the media".

> *"More interest from students, more media coverage regarding cyberattacks and more funding from government has created this demand."*
>
> Higher Education representative

"The skills in cyber security are in demand, so I was really interested to focus in cyber security"

Student (focus group)

There is a small number of HE institutions that do not offer cyber security-related degrees. Although some of these HE institutions plan to do so in the future, many face difficulties in attracting lecturers and researchers with expertise in cyber security. The findings from the survey clearly show that there is insufficient staff expertise in many universities and difficulty in recruiting suitable staff to teach cyber security. This is partly due to a risk that skilled lecturers are poached by higher-ranked universities or industry.

Alongside their studies, students can develop additional skills or knowledge through interactive websites and platforms. An example is Immersive Labs, which allows students doing part-time or full-time courses to register free of charge with their university or college email address and to then use the platform to develop cyber skills. Another example is the Digital Cyber Academy which is free to ex-Armed Forces personnel wishing to develop their cyber security skills and neurodivergent individuals that want to pursue a career in cyber security.

2.3.2 Types of cyber security courses

As noted earlier, there is a range of cyber security programmes being offered in HE institutions across England. Below we examine the courses available at different levels.

2.3.2.1 Undergraduate courses

Applicants for BSc degree course in cyber security are usually, but not always, required to have at least one A Level (or equivalent qualification) in a STEM subject. A review of a selection of courses showed no consistent pattern on this point and no particular distinction between the pre- and post-1992 universities. Some, such as Coventry University require applicants to have at least one A Level (grade 6 or above) in Mathematics, Physics, Chemistry, Design Technology or Computing. Some state a preference, but not a requirement for STEM subjects, which is the case at the University of Warwick. Others do not state any requirement or explicit preference for A Levels in STEM subjects, such as the University of Wolverhampton and Aston University. This is broadly similar to the situation for first degrees in computing science, some of which require A Level Mathematics, whilst others do not.

There has been an increase in provision of undergraduate level degrees in cyber security. Some universities (e.g. the University of Warwick and Royal Holloway) have had their undergraduate degrees provisionally certified by the NCSC. The course at the University of Warwick is an interesting case as it focuses heavily on security, while at Royal Holloway, the course allows students to take a number of general computing modules. Other degrees (e.g. those offered by the University of Portsmouth, De Montfort University and the University of Bournemouth) adopt similar approaches, with a typical approach being to offer broad computing modules initially and to focus on cyber security in the second and third years of the course. This is mainly because students need to be taught basic foundation skills and knowledge before studying cyber security. Computer Science is a common foundation for cyber security but is not sufficient in providing the required skills and knowledge for a career in cyber security.

In addition to courses specifically in cyber security, there are some examples of undergraduate courses covering not only technical areas such as assessment and testing, but also project management, data protection and privacy. A few universities, such as the University of Brighton and the University of Winchester, also have core modules on legal and governance issues in cyber security.

Universities, such as Canterbury Christ Church University and the University of Salford, have a strong emphasis on teaching students the ethical implications of cyber security (this is different from ethical hacking, which is a technical skill), with the University of Salford making their students sign an ethical code of behaviour.

Many HE courses are accredited by the British Computing Society (BCS) and the Chartered Institute for IT, with other accreditations including the Defence Undergraduate Technical Scheme (DUTS) and the Institute of Information Security Professionals. Interviewees mentioned that students found the NCSC certification to be especially important in their decision to select programmes of study. As such, many interviewees and universities (who did not already have it) are likely to begin seeking NCSC certification for their programmes related to cyber security.

2.3.2.2 Degree apprenticeships

Apprenticeships in cyber security or that include a cyber security dimension have recently been introduced at degree level. Degree Apprenticeships were introduced by the Government with effect from September 2015.[72] They are available to any adult, but particularly targeted at 18 and 19-year-olds leaving school or college. Degree apprenticeships combine paid work and study, and thus serve as an alternative route to gaining a degree to traditional full-time programmes. Feedback from students at the various focus groups suggests this is a very appealing pathway for those who wish to combine a degree with the development of practical skills. More than half of the students participating in the focus groups at FE level were keen to pursue a degree apprenticeship:

> *"Before I was thinking about going to university after my BTEC, but now I am really interested in degree apprenticeships. You may learn a lot with a degree in tech, but once you have that degree, you can't apply what you learned in the field. With a degree apprenticeship, you learn more on the industry and it's more hands-on"*
>
> Student (focus group)

Students can study for a degree apprenticeship on a full-time or part-time basis during the university term or in blocks of time, depending on the programme and the requirements of the employer. The employer recruits, employs and pays the apprentice, whilst also paying tuition fees and training costs. Whilst employers may choose to retain the apprentice after graduation, but there is no obligation to do so. Degree apprenticeships are funded by the Apprenticeship Levy with additional contributions from the Government.

The study identified one degree apprenticeship in cyber security at Level 6. It also identified the Level 6 and Level 7 MSc Digital and Technology Solutions apprenticeship, which has a specific cyber security dimension. The study did not look into the depth in which cyber security was contained in other degree apprenticeships. The standards for these degree apprenticeships noted here are approved by the Tech Partnership, a network of employers in the digital sector. In 2017-18, a total of 1,130 students started degree apprenticeships in the BSc Digital and Technology Solution Professional. The Institute for Apprenticeships is planning to publish a review of the BSc (Hons) in Digital and Technology Solutions in early 2019 (as part of a wider review also covering 11 digital apprenticeship standards at Levels 3 and 4).[73]

[72] Department for Business, Innovation and Skills, 2015, Government Rolls-Out Flagship Degree Apprenticeship
[73] Institute for Apprenticeships, 2018, Apprenticeship Standards Statutory Review

Box: 2.3: Degree Apprenticeships

- **Cyber Security Technical Professional** (Degree, Level 6). This apprenticeship standard was approved for delivery in September 2018, with the involvement of several employers including: QinetiQ, 3SDL, BAE Systems, Becrypt, BT, CGI, Crest, DWP, HPE, IBM, Transport for London (TfL), Virgin Trains South Coast, NCSC.
- **Digital and Technology Solutions Professional** (Degree, Level 6), which leads to a BSc (Hons) in Digital & Technology Solutions and covers a range of specialisms including Cyber Security Specialist. It was approved for delivery in March 2015. This apprenticeship covers a range of core digital skills, such as undertaking security risk assessments for IT systems and analysing security threats and hazards to information systems or services. It also covers a body of core technical knowledge and a set of core behavioural skills (e.g. written communication, critical thinking, logical thinking, problem-solving). This degree-apprenticeship is not specific to cyber security but contains a module or two instead. Several employers were involved in creating the standard: Accenture, Bright Future, BT, Capgemini, CGI, Ford, Fujitsu, GSK, HMRC, HP, IBM, John Lewis, Lloyds Banking Group, Network Rail, Tata Consulting Services.
- **Digital and Technology Solution Specialist** (Master's, Degree Level 7), which leads to an MSc Digital & Technology Solutions. It was approved for delivery in August 2018. The apprenticeship includes several technical specialisms, including Cyber Security Technology Specialist. Core skills include carrying out security testing strategies, cyber threat intelligence analysis and vulnerability assessment. Several employers were involved in creating the standard: 3ManFactory, Accenture, AMS Neve, BBC, Capgemini, CGI, Connect Software, DWP, IBM, J.P. Morgan, Optimity, TCS, Thales.

Within this overall framework, **there is some diversity in the provision of degree apprenticeships in fields relevant to cyber security**. Some degree apprenticeship courses are developed by universities and then offered to groups of employers whilst other courses are developed for a sole employer. Some employers offer a guaranteed job at the end of the apprenticeship whilst others do not. Examples include the following:

Box: 2.4: Industry-led Degree Apprenticeships

- **NCSC** offers the new cyber security degree apprenticeship from September 2018 and using the new standard, known as the CyberFirst degree Apprenticeship. Apprentices are employed within a number of locations and currently have a starting salary of £17,942. They undertake a mix of university-delivered classroom and lab education along with technical training, mentoring and job shadowing, hands-on, work-based placements and projects. Apprentices also join the CyberFirst Community. Entry requirements include three A Levels in any subjects (4 or above) and a minimum of two GCSE in STEM subjects (6 or above), one of which is maths.
- **BT Security** offers a degree apprenticeship in cyber security for recruits into its Security Operations Centre, security implementation teams, security architects or some of the more specialised security departments. Degree apprentices are based at Bletchley, Ipswich, Manchester, Skelmersdale. Entry requirements include 3 A Levels (minimum of BBC grades, which must include a STEM subject at a minimum grade 6), plus a minimum of 4 GCSEs at grades 4-9 (C or above) including English Language and Maths. Depending on the apprenticeship, four days out of each month will be spent at university.
- **Unilever** offers a Digital & Technology Solutions Degree Apprenticeship with a specialism in cyber security, leading to a BSc in Digital and Technology Solutions after four years. Apprenticeships are based at Port Sunlight (Merseyside). Entry requirements include at least five GCSEs grade (9-4), (English Language, and ideally either ICT or Science) and two A Levels or a Level 3 Apprenticeship or equivalent qualification or experience.
- **PwC** offers a degree apprenticeship in partnership with five UK universities (of which three are in England). Apprentices can study for a BSc in Computer Science with Digital Technology Partnership at the University of Birmingham or a BSc in Computer Science (Digital and Technology Solutions) at the University of Leeds. Both are four-year courses, with the first two years spent full-time at university (with placements at PwC outside of term-time) before a third-year full-time placement at PwC and the fourth year at university. PwC guarantees a job upon graduation.
- **Derby University** offers a degree apprenticeship, including a BSc Hons Digital and Technology Solutions with a specialism as cyber security analyst. The course is open to employees of any employer, provided that they meet the entry requirements and work at least 30 hours per week. Entry requirements include 120 UCAS points at A Level and five GCSEs at grade 4 including Maths and English. Individual employers also set their own selection criteria.
- **Anglia Ruskin University** offers a BSc Digital and Technology Solutions Degree Apprenticeship, including a specialism as cyber security analyst. The apprenticeship includes part-time undergraduate study of one week per semester with the rest of the time spent working. Some modules cover the core material for professional certification, such as CCNA Cisco Certified Network Associate.

As shown by these examples, academic entrance requirements to degree apprenticeships are broadly similar to those of conventional degree programmes, with additional criteria added by employers as part of the recruitment process. Based on these examples, employers tend to seek candidates both with technical aptitude and with good all-round skills, such as attention to detail, communication, problem-solving, work ethic, among others.

2.3.2.3 Postgraduate level

Students can opt to pursue degrees relating to cyber security at both the postgraduate and doctorate levels.

Master of Science (MSc)

The majority of cyber security provision at this level leads to a Master of Science (MSc). If students combine cyber security with another STEM subject, these can lead to a Master of Engineering (MEng). MSc courses tend to have a technical focus (i.e. driven by computer science topics) and include modules such as data protection technologies (cryptography and steganography, biometrics, privacy, access control), security risk assessment, cyber threats and vulnerabilities and countermeasures. All courses also include a module on professional development and skills for the workplace, in addition to a research dissertation. However, some universities offer non-technical modules, usually on legal and governance issues. Some other notable examples include the University of Southampton which offers a module on the History of Cyber Crime and University College London which offers a module on the Philosophy, Politics and Economics of Security and Privacy.

Applicants for MSc courses in cyber security are often, but not always, required to hold a first degree in computer science (or in a related field). A review of a selection of courses showed that some are open to graduates of other subjects, provided that they demonstrate relevant experience or a proven interest in cyber security. For example, the University of Warwick's MSc Cyber Security and Management is "ideally suited to those from a computer science or IT background; the programme also caters for non-STEM graduates with a specific interest in cyber security".[74] The University of Liverpool's online MSc in Cyber Security requires a first degree in computing (or equivalent) unless the applicant has at least two years' professional experience in IT and a degree in another subject or five years' experience without a degree.

Some universities also offer MSc level courses that take a more cross-disciplinary approach. For instance, there are MSc programmes in Internet Governance and Regulation, which include courses related to cyber security and a concentration on intervention for political influence. Additionally, there are MSc programmes in Human Centred Computing as well as Business Management which include cyber security and cyber risk management as compulsory modules. This again alludes to the large scope of cyber security in the curriculum. Conversely, MSc programmes on Cybercrime and Digital Investigation also include modules in cyber security alongside regulatory practices, cyber-crime and digital forensics. Rather than offering a course purely in cyber security, these draw on core criminology and security theories, approaches and perspectives to enable the students to discuss relevant and emerging online problems. These focus on the digital forensics and law enforcement entry-level job route of cyber security.

Many of the Master's programmes have a sectoral orientation designed to give students the skills required to work in the cyber security field in a particular industry. A good example of this is the MSc programme on Automotive Electronics, delivered by the University of Warwick and several other universities in partnership with industry. This programme includes modules on automotive cyber security. Furthermore, in response to industry demand, the university has also developed a two-day course on automotive cyber security for experts (typically from the automotive/manufacturing fields).

As well as the full-time options, Master's programmes, such as that offered by Northumbria University, can be taken part time. In many cases, it is possible to undertake part-time study because the classes are taught in blocks, either as morning classes or afternoon/evening classes. This is arranged by HE providers to accommodate the needs of those students who want to study

[74] Prospects, 2018, Cyber Security and Management, the University of Warwick

and work at the same time. This mirrors existing programmes on subjects such as Software Engineering, which typically accommodate students currently working in industry.

Doctorates

In many cases, doctoral programmes, such as PhD, DPhil or Deng, are industry-driven or industry-funded. Some doctoral programmes include options to undertake technical courses such as penetration testing, cryptography or systems design. There are, however, also a growing number of non-technical options including modules on International Relations, Law (computer misuse, act-data), and human-centred computing. Multidisciplinary programmes at this level are usually found within doctoral training centres where the first year of the doctorate consists of students undertaking a range of courses to build a foundational knowledge of cyber security and the breadth of topics its spans. Typically, doctoral programmes are full time with some exceptions being made for DEng studies, which require the sponsorship of a company.

2.4 STEM and non-STEM perspective in cyber security

In addition to cyber security courses focusing on purely technical aspects of the subject and which require STEM knowledge, there are other HE courses that are relevant to non-STEM aspects of cyber security.

2.4.1.1 STEM-related perspective

In most cases, students that undertake cyber security courses have a STEM background. This suggests a general inclination towards the more technical nature of cyber security (a conclusion also supported by the HESA data). The qualities that are desirable for technical degrees include knowledge of Science, Mathematics and/or Computing. Due to the highly technical nature of cyber security, a degree in a STEM-related subject with cyber security is not enough to develop all the skills and knowledge required for a technical cyber security entry-level job. Indeed, employers recognise the need to provide training for new graduate recruits, as the technical expertise to be a cyber security professional can take some years to acquire. Nonetheless, STEM-related subjects are regarded as key because they help students develop a logical systematic approach to reasoning and computational thinking. As noted above, several BSc degrees in cyber security or computer science do not require applicants to have an A Level (or equivalent qualification) in a STEM subject.

Feedback from the interview programme and the online survey indicates that the majority of FE and HE respondents consider computer science and mathematics to be the key building blocks of cyber security degrees offered by their institutions. In cases where students do not have a STEM background, the research suggests that it may be difficult for them to grasp some of the topics covered in specialist or technical courses. Only a small number of respondents indicated that a strong background in STEM-related courses is not a requirement for their courses. This is because students could develop basic knowledge for the first time through their degree course. According to the survey work, skills that are seen as essential for students studying cyber security include teamwork (86% of the survey respondents considered this to be essential), problem-solving abilities (85%) and communication skills (75%).[75] These survey findings support the interview feedback, which emphasised that cyber security experts must be able to work in teams, articulate arguments in relation to threat-sharing and think laterally to identify new threats.

2.4.1.2 Non-STEM-related perspective

In addition to the technical options, there are HE courses relating to cyber security that are more multidisciplinary and do not require a STEM background. A key consideration that this research highlights is that cyber security is not only a technical subject or technical area of study and

[75] Source: Survey feedback.

work. Different sectors and roles need to take different approaches as they each have unique requirements, and therefore skill-needs. It is important that these needs are catered for by a range of courses open to a variety of individuals, from both STEM and non-STEM backgrounds. Thus, an important requirement for some cyber security roles is to be able to undertake a risk assessment or to understand human behaviours, where a background in Psychology, Social Media Analysis, Behavioural Economics, and Law can be more relevant than purely technical knowledge. For example, within a Criminology programme, students will acquire some knowledge in cyber security during the different modules on cybercrime but they may also choose optional modules that focus more on regulatory practices and policing cybercrime and that concentrate on legislation, strategies, policing and cyber security.

Many of those consulted for this study also highlighted that cyber security should be offered across the full breadth of degree courses. Students need to be able to apply general cyber security knowledge in their everyday life. Several also argued that courses in online behaviour, use of social media, fake news and ethical hacking should be offered from an early age.

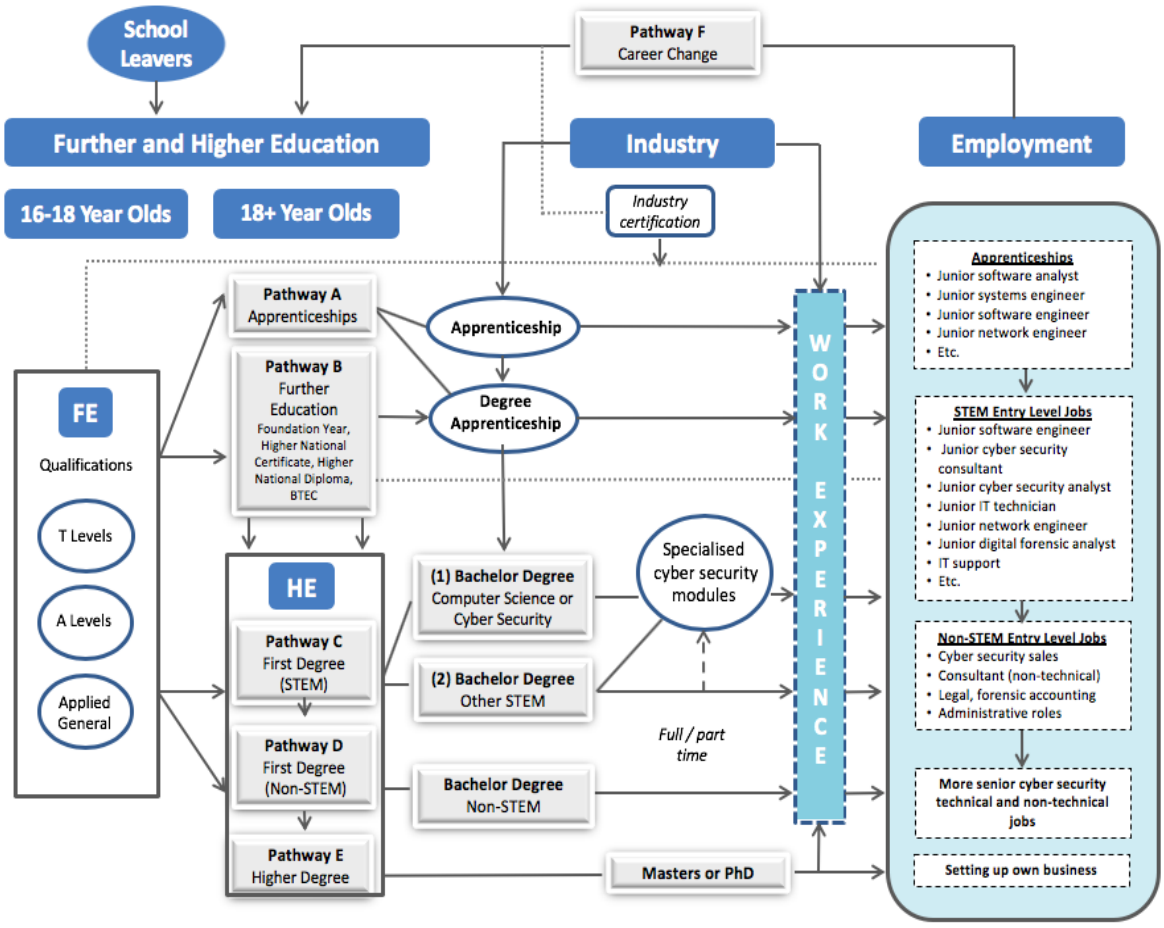
3 Pathways to Cyber Security Jobs through FE or HE

3.1 Identifying the main pathways

This research identifies six main pathways involving FE and HE that can lead to entry-level jobs in the cyber security field. There are other ways of obtaining a cyber security job that do not involve FE and HE routes, such as developing technical skills outside HE and FE, but these pathways were beyond the scope of the research.

To help map the FE and HE pathways, four main sources of information were used: feedback from interviews with employers on their requirements and recruitment methods; an analysis of AoC and HESA data on cyber security courses and student destinations for the period 2014 to 2017; an analysis of the requirements for entry-level cyber security jobs advertised via three recruitment portals (Indeed, Glassdoor and CV Library); and an analysis of the profiles of LinkedIn users who described themselves as having entry-level jobs in the cyber security field. The following chart summarises the main pathways into an entry-level cyber security job.

Figure 3.1: FE and HE Pathways to entry-level cyber security jobs



In Table 3.1, the various pathways are presented from the perspective of different levels/types of qualifications and the routes that lead to an entry-level job in the cyber security field. The first column in Table 3.1 lists the six main routes leading to an entry-level position. The second column summarises the types of entry-level jobs with examples in the third column (these job titles are

drawn from common job titles obtained through the HESA data, LinkedIn profiles and web-recruitment websites). Reference should be made to Section 2 for details of the course content.

Table 3.1: Pathways to entry-level cybersecurity jobs

Pathways	Description	Entry-level job examples
Pathway A - Apprenticeship Route A large number of 16 to 18-year-old (and older) pupils study for qualifications at an FE institution. By the time they finish their qualification at Levels 2 and 3, they can opt for an apprenticeship route (degree apprenticeship or higher apprenticeship). FE providers for Levels 2 and 3 provide generalist provisions (e.g. information and communication technology). Students can enter technical or digital FE courses instead, mainly because cyber security is a provision that is not currently available at Level 3. This is because courses are meant to be generalist at this stage. However, students can enter technical or digital FE institutions, where they can specialise in cyber security at a younger age.	A relatively small proportion of FE students take the apprenticeships route directly at 18+ or 19+ years old. If students take this route, they are offered a wide range of technical apprenticeships, which can lead to an entry-level job in cyber security. Students can choose to link their higher apprenticeship to a HE qualification or undertake a degree apprenticeship.	Junior positions, such as: • Computing apprenticeship • Software analyst degree apprenticeship • Systems engineer apprenticeship • IT degree apprentice • Network engineer apprenticeship • Cyber security apprenticeship
Pathway B – Further education route After pursuing secondary education through an FE institution, students can opt to remain on this route. At 18+, students can take a foundation year or degree, an HND or HNC diploma and/or a BTEC. All of these diplomas or certificates allow FE students to access a Bachelor degree, either through a top-up course or directly after a foundation year.	The majority of students on this route pursue a degree, which leads them onto Pathway C. Should students decide to do an apprenticeship, they will follow Pathway A. Currently, few students go straight from an FE institution to an entry-level job in cyber security. Without a degree, students on this route are generally able to take up generalist IT positions that may not require a degree as an entry requirement before entering into a cyber security career.	Generalist IT roles, such as: • Technical support • Web developer • Web designer
Pathway C – First Degree STEM route (1) Computer Science or Cyber Security: the most common pathway is to study for a BSc in Computer Science with a cyber security module. A number of students also take a cyber security specific course. Some students may also decide to take a specialised technical course (i.e. ethical hacking, digital forensics).[76] (2) Other STEM path: many entry-level jobs in cyber security are filled by	Graduates with a Computer Science, Cyber Security or other type of STEM degree tend to start with an entry-level job involving a generalist IT role (e.g. software developer or IT support) but then after 1-2 years, enter a cyber security function either within the same company, or by moving on to another organisation. It is important to note that not all students taking this route end up with a role in cyber security (especially if the student took a	Junior positions, such as: • Software engineer • Cyber security consultant • Cyber security analyst • IT technician • Network engineer • Digital forensic analyst • IT support

[76] It is important to note that this may be the most common pathway due to the lack of awareness regarding other pathways and building blocks that exist. Taking a course in computer science does not provide students with specialised cyber security knowledge required for a highly technical entry-level job. This means further training will be required at industry-level.

Pathways	Description	Entry-level job examples
students who have taken a BSc course in another STEM-related degree, such as Mathematics or Engineering.	generalist computer science or STEM course). Students that study for a specialised cyber security technical course tend to enter specialist roles straight away (e.g. digital forensic analyst, see case studies in Box 3.4)	• Penetration tester • Software developer • IT consultant
Pathway D – First Degree Non-STEM route A number of non-technical entry-level jobs in the cyber security field are filled by graduates who have non-STEM degrees (e.g. History, Law, Psychology, International Relations).[77] In this particular pathway there are also students who have studied for a degree in business and/or management studies.	There are a significant number of entry-level jobs relating to legal, commercial, risk management and other non-technical aspects of cyber security. There are also generalist entry-level roles open to non-STEM graduates that include in-house training designed to open up opportunities in more technical aspects of cyber security or that lead on to managerial roles.	Junior positions, such as: • Cyber security consultant (non-technical) • Network support • Service operation engineer • Network engineer • Cyber security analyst • Cyber security business analyst • Cyber risk management
Pathway E – Higher Degree route Students going through Pathways B and C may study for a Master's degree or PhD in cyber security if this was not their BSc speciality. Alternatively, they may choose to pursue a more specialised course/field of research (e.g. forensic computing).	Those with a Master's degree or a PhD can be recruited into higher positions in the cyber security field, although the majority will also have to go through rigorous in-house training. The career path is similar to Pathways B and C insofar as most recruits will be expected to spend some time in an entry-level position first to go through training. This explains the cross-over of job titles with Pathways B and C (e.g. cyber security analyst or consultant). However, those with a Master's or PhD are likely to progress more rapidly to a more specialised / senior function later on.	Positions, such as: • Information security analyst • Software engineer • Cyber security consultant • Cyber security analyst • IT consultant • Information security manager • Penetration tester • Security engineer
Pathway F – Career change route Another possibility is that some people who have already entered the workforce decide on a change in direction in their career and this can involve an entry-level job in cyber security. They may do so after obtaining a qualification (effectively joining Pathway A, B, C or D). The entry-level job they undertake depends on whether they take a technical or non-technical route into cyber security.	An example of this situation is somebody who leaves the Armed Forces or Police and as part of their resettlement scheme for a qualification in cyber security before taking up an entry-level job. Their age and experience mean they can progress quite rapidly (as in Pathway D). Alternatively, somebody might simply decide to move into cyber security from a different role in a company.	Same technical or non-technical entry-level jobs listed above

Industry representatives consulted for the study commented that the various pathways lead to entry-level jobs but that in all cases, further in-house training by the company is needed to develop cyber security knowledge and skills. This is for both technical and non-technical entry-level positions and those with or without a cyber security-specific qualification. It was noted that those with less exposure in cyber security or specific qualifications, needed more training.

[77] Some examples of cyber security courses combined with non-STEM specialities include: Cyber security and business; Cyber law and society; Cyber security and management; Information security and audit.

In the text that follows, data is presented on the number of students following each pathway, as well as case studies of professionals that have followed some of the pathways. These are based on LinkedIn profiles of professionals who described themselves as having an entry-level cyber security job. The names of individuals with an asterisk are fictional to preserve their anonymity.

Pathways A and B – Apprenticeship and further education route

In relation to Pathway A, a total of 18,030 students were undertaking apprenticeships in 2017-18 in the ICT sector at all levels. These are likely to include some elements of cyber security.

Box: 3.1: Case Study on Pathway A

Pathway A – FE Route: Charles* passed his A Levels at a sixth-form college in STEM subjects before starting an apprenticeship for A Level 3 Diploma in ICT systems and principles. He joined a technology company as an apprentice systems technician and worked in second-line support in the management team. He later became a desktop engineer going to client sites. After almost two years in this organisation, Charles* became a cyber security apprentice, as part of a 12-month placement at a nuclear sector company. Having started in a general IT position, Charles* is now very interested in developing his skills in penetration testing and ethical hacking.

Box: 3.2: Case study: Apprenticeships at the Government Security Profession Unit

The Government Security Profession Unit (GSP) adopted a recruitment scheme for apprentices at the Central Government. The majority of recruits are young students that are still studying (between 18 to 19 years old) and 10-15% are in their 30s or 40s looking for a career change. Students generally have obtained their A Levels, but this is not a requirement. In most cases, students are recruited into Government following the completion of the apprenticeship. Since the beginning of the scheme in 2015, the Department takes in approximately 25 apprentices each year. The trend is to increase the number of recruits and become the main point of entry for cyber security professionals in Government.

The GSP also make efforts to attract candidates from a variety of backgrounds, including neurodiversity. The skills the GSP mainly look for are 'office skills', such as strong communication, team working abilities and attention to detail. The GSP representative highlighted that it is important the candidate demonstrate an interest in cyber security and working for government. The objective of the GSP is to mainstream the recruitment of cyber security entry-level professionals for central government and address the gap of professionals at High Executive Officer (HEO) and Senior Executive Office (SEO) levels that frequently leave after training to work for the private industry.

In relation to Pathway B, there were 47,417 students undertaking FE courses in 2016-17 for qualifications in subject areas that are likely to include aspects of cyber security.[78] Most of these students will have moved on to do a Bachelor's degree (Pathway C) or taken the apprenticeship route (i.e. higher apprenticeship or degree apprenticeship) (Pathway A). Of those students, some will continue in fields related to cyber security (e.g. the 110 degree courses in cyber security or the 2,369 courses in computer science noted in section 2.3), whilst others will study other subjects.

Table 3.2 shows the destinations of students enrolled in state-funded schools or colleges that went into 'sustained' destinations (education, employment or training) after gaining an A Level or a Level 3 qualifications across all subjects. As can be seen, 89% went into a sustained destination, notably education or employment after Key Stage 5. Among those in a sustained destination, 7% were working and studying at the same time through an apprenticeship.

[78] The Association of Colleges data indicates that in 2016-17 there were 700 students in FE Colleges studying for a qualification that focused mainly on Cyber Security. Most of the 47,417 students were studying other subjects such as computer science that included a cyber security module.

Table 3.2: Destination of students after key stage 5 (Level 3) in England across all subjects, 2013/2014 (state-funded mainstream schools and colleges)

Destinations	Number of students	Percentage of students
Education	234,500	65%
Employment	84,790	24%
Destination not sustained	31,270	9%
Activity not captured	8,410	2%
Total	**358,970**	**100%**

Source: Longitudinal Education Outcome dataset, 2016, Department for Education

Box: 3.3: Case Study on Pathway B

Pathway B - First Degree STEM route: Julie* passed her GCSEs (including maths and science) and developed an early interest in the field of technology pre-GCSE. She wrote her extended essay in artificial intelligence and went on to study for a BSc in Computer Forensics and Security Technology at Sheffield Hallam University. After graduating from her BSc, she became a desktop support analyst and provided second line desktop support. In her role, she was required to apply problem-solving, communication and technical skills. Julie* then took up a position as an information security graduate at Network Rail, where she analysed processes and implemented changes. After a year and a half in this position, she did an MSc in Advanced Security and Digital Forensics with Cyber Security before getting a job at HSBC as an IT Security Analyst. Julie has an ITIL Foundation 3 certification and is now specialised in log analysis, incident response, SIEM rule development and integrating security products.

Pathways C, D, E and F – Higher Education

In relation to Pathways C and E, taken together, there were 5,827 students in 2016-17 studying a cyber security relevant course at undergraduate or postgraduate levels. In addition, there were a further 79,905 students undertaking courses at universities in Computer Sciences, 37,350 studying Mathematical Sciences, 130,685 studying Engineering & Technology, and 259,420 undertaking other STEM courses (Pathway C).

Whilst many will choose other careers, with qualifications in these subjects, students are eligible for a highly technical entry-level job in the cyber security field, provided they have developed a strong interest in the field, gained relevant professional experience, obtained certifications and received considerable in-house company training. Recruiters for technical entry-level cyber security jobs value a background in other STEM subjects, especially maths or engineering, because these fields also develop good problem-solving skills and the ability for attention to detail with numbers. However, in most cases, graduates will need to go through further training by the organisations they join to develop cyber security knowledge and skills, especially if they go on to a technical cyber security position. It is also important to highlight that the stream of STEM students going into cyber security is a very narrow group, with other digital careers competing to attract people from these backgrounds. It is not possible to provide an estimate for Pathways D or F.

Table 3.3 provides a breakdown of the number of students studying cyber security or closely related subjects at an undergraduate or postgraduate level for the period 2014-17.[79] Table 3.4 then provides data for 2016-17 for computer sciences and the other subjects that are relevant to Pathway C.

[79] This includes students domiciled in the UK, the EU and non-EU countries.

Table 3.3: Number of cyber security graduates and postgraduates, 2014-17

Year	2014-15	2015-16	2016-17	Total
Postgraduate	1,508	1,629	1,835	4,972
Undergraduate	3,057	3,335	3,992	10,384
Total	**4,565**	**4,964**	**5,827**	**15,356**

Source: HESA.

Table 3.3 shows that the number of students undertaking cyber security-related courses has steadily increased over the 2014-17 period, both at undergraduate and postgraduate levels (in this period there was a 22% increase in the number of postgraduates and a 31% increase in the number of undergraduates). A further analysis of the HESA data shows that 74% of students domiciled in the UK and the EU obtained an entry-level job in a field related to cyber security.[80] Students participating in the focus groups for this study said they mainly rely on teachers, their friends and family to learn about the different pathways and information on careers in cyber security.

> *"Pathways on cyber security are difficult to find. People have different opinions and you need to do some deep online research to get this information. Teachers that have a background in the industry are usually best placed to give information on opportunities in the field"*
>
> Student (focus group)

Table 3.4 shows the number of students undertaking a course in a STEM subject area in England at undergraduate and postgraduate levels in 2016-17. It shows that within the STEM field, there are 507,365 students that could potentially enter the more technical aspects of cyber security. Since the total number of graduates who have specialised in cyber security remains relatively low, these other related fields in technology or STEM help to widen the pool of potential recruits into the cyber security field, although not all students from these subject areas will want to pursue a job in cyber security.

As noted earlier, this research has not looked specifically at the specific skills and quality of cyber security courses in Computer Science and STEM subjects more broadly. Students with a STEM background are also in high demand from employers in other sectors of the economy (i.e. financial services). It is also important to note the technical complexities of cyber security means graduates need to go through considerable training to obtain technical entry-level positions in cyber security. Currently this pool of students is small, but there is scope to further raise awareness of employment opportunities in cyber security.

Table 3.4: Number of students studying STEM subjects at undergraduate and postgraduate levels, 2016-17

Subject areas	2016/2017			
	Female	Male	Other	Total
Biological Sciences	116,170	67,390	50	183,610
Physical Sciences	31,020	44,760	30	75,810
Mathematical Sciences	13,590	23,735	30	37,350
Computer Science	13,295	66,585	25	79,905
Engineering & Technology	22,985	107,675	25	130,685
Total	**197,060**	**310,145**	**160**	**507,365**

Source: HESA.

[80] The remaining pursued a career in an un-related field six months after graduating from their HE institution.

As in other subjects, HE institutions in England are successful in attracting non-UK students onto cyber security BSc and MSc degree courses, which serves to increase the flow of potential recruits into cyber security jobs in England. Indeed, as shown in Table 3.5 below, nearly 20% of students completing graduate or postgraduate degrees at English universities came from outside the UK between 2014 and 2017. Of those, most (14.9%) were from outside the EU, whilst the remainder (4.7%) are from other EU countries. It is not possible to specify the number of non-UK students who remain in England following completion of their studies, or indeed how many UK graduates and postgraduates go abroad to take up jobs.[81] A trend analysis as to how likely this compares with other subjects was not performed.

However, evidence from different universities reported that non-EU students were more likely than UK and other EU students to leave the UK upon graduation. Whilst some non-EU students choose not to remain in the UK, those that do must obtain a Tier 2 visa if they are to take up employment, which requires them to be employed by a licensed sponsor.[82] Whilst more than 27,000 employers are currently licenced sponsors, some firms are reluctant or unable to seek licenced status.[83] Of course, not all non-EU students would be eligible for certain cyber security roles, given the requirements of security vetting procedures.

Table 3.5: Domicile of cyber security graduates and postgraduates, 2014-17

Domicile	2014-15	2015-16	2016-17	Total
UK	80.2%	79.2%	83.5%	80.2%
Other-EU	4.9%	4.9%	4.9%	4.7%
Non-EU	14.6%	15.9%	11.7%	14.9%

Source: HESA.

Table 3.6 breaks down the percentage of students domiciled in the UK (UK or EU nationals) going into the cyber security field by course type. The data is based on 1,892 graduates. A total of 74% of these obtained a position in a field related to cyber security over the past three years. As shown in the table, just over a quarter (26.32%) of all students domiciled in the UK leaving HE that studied a cyber security related subject obtained an entry-level job in the same field. However, the biggest proportion of graduates and postgraduates (38.58%) obtained an entry-level job related to IT.

The HESA data indicates that computer science with a cyber security speciality or module is currently the higher education route that most frequently enabled direct entry into a cyber security or a more general IT role. Analysis of the HESA data suggests it is fairly common for students to enter a more general role that requires on-the-job training from employers before moving on to a cyber security-related position, so a large number of those entering the cyber security field do so at a later stage. This is consistent with the feedback obtained from employers who can be reluctant to put entry-level graduates with little professional experience in positions that can directly influence the security of their clients and/or their organisations. As such, further training and experience are often required before obtaining an entry-level position in a technical cyber security job. A recent UK study found that 28% of cyber security employees accessed their position from another IT-related job, while 68% held a security-related role before.[84]

In the past three academic years, 8.6% of students studying a cyber security-related course were unemployed six months after graduating. A further 1.6% were doing something else (e.g. looking after family) and 1.4% took time out in order to travel.[85]

[81] In the words of the Office for National Statistics (ONS): "There are no official figures that show how many students do not emigrate and remain in the UK after their studies." Source: Fullfact, 2017, How many international students leave after studying in the UK?
[82] Gov.uk, 2018, General Work Visa (Tier 2)
[83] Home Office, 2018, Register of Sponsors Licensed Under the Points-based system
[84] e-skills.uk, 2013, Careers analysis into cyber security: new & evolving occupations
[85] Source: HESA.

Table 3.6: Percentage of students domiciled in the UK and the EU going into the cyber security field by course type at undergraduate and postgraduate levels, 2014-17

Courses//Type of job	Further study[86]	Cyber Security	Other job	IT	Manage-ment	Other profession	Total
Cyber Security (non-technical degree)	0.00	1.43	0.58	1.37	0.74	0.69	4.81%
Cyber Security	0.26	7.82	1.11	7.45	3.22	2.80	22.67%
Computer Science and Cyber Security	0.37	14.01	8.19	25.11	4.02	8.14	59.83%
Specialist Cyber Security	0.37	3.07	1.06	4.65	1.16	2.28	12.68%
Grand Total	**1.00%**	**26.33%**	**10.94%**	**38.58%**	**9.14%**	**14.01%**	**100.00%**

Source: HESA.[87]

Box: 3.4: Case Studies on Pathways C, D, E and F

- **Pathway C – First Degree STEM route:** Harry* did his A Levels in ICT and other non-STEM subjects. He then went on to study at Coventry University, where he earned a first-class BSc in Ethical Hacking and Cyber Security. After graduating, Harry started working in a small company focused in cyber security.
- **Pathway D - First Degree Non-STEM route:** Sara* pursued a BSc in Psychology at Nottingham Trent University. Upon completing her studies, she worked at a real estate company as a team secretary for a few months, then as a roadshow coordinator for another eight months. Sara* then joined a financial services company as an executive assistant. After spending two years in the same company and participating in various in-house training programmes, she became a Cyber Security analyst in the same organisation.
- **Pathway E - Higher Degree route:** Laura* studied Physics at the University of Bath and then worked for a few years in the field of cyber security, defence and management. She then decided to do a MSc in Cyber Security and Management at the University of Warwick. After completing her studies, she went on to become a senior cyber security consultant at Capgemini.
- **Pathway F - Career Change Route:** Edward* spent five years in the British Army, serving as a soldier in the Royal Engineers. During his army career, he had several jobs as a computer operator, dealing with sensitive information on his regiment's deployments. He also developed an interest in cyber security. When he left the army, Edward* was provided with a resettlement package enabling him to study for an HND in Computer Science at Walsall College. He was then able to complete an extra year to obtain a BSc during which he did several cyber security modules. This led him to a job in the IT department of a local company where he hopes to move into cyber security after an initial period of in-house company training.

[86] Further study refers to students that opted to pursue additional studies within six months after graduating.

[87] Note: in Table 3.6, the category '**cyber security non-technical degree'** refers to courses that are combined with another subject such as Management, Business Studies or Psychology. A specialist Cyber Security course is more technical (e.g. a degree in Cyber Security with Criminology, Cybernetics, Digital Forensics or Ethical Hacking). In terms of the type of jobs, job titles were categorised into 5 thematic areas, the first one being Cyber Security. This includes positions that explicitly involve a Cyber Security role within a company, such as Cyber Security consultants, information security analysts, penetration testers or security engineers. The category **'Other job'** in the table are positions that are un-related to Cyber Security and/or IT more generally and include jobs such as those in the service and hospitality sectors that are most likely a temporary occupation whilst applying for more permanent IT or Cyber Security jobs. The category **'IT jobs'** includes job titles that explicitly mention 'IT' (e.g. IT engineers, IT support analysts, IT specialists) or that are closely related (e.g. software developers or software testers). **'Management'** positions refer to functions that involve planning or managing the resources of an organisation (e.g. project managers, security managers, IT managers, directors or operations managers). **'Other profession'** represent students working in a field that is different to their degree course.

3.2 Entry-level requirements for cyber security jobs

The research suggests that many employers will recruit graduates who have studied Computer Science, Maths or Engineering, as opposed to having specialised specifically in cyber security. Due to the shortage of cyber security graduates, it is inevitable for employers to recruit from a pool of graduates that have basic technical competencies and a basic foundation in tools, software or networks. If students have this knowledge, employers know that when technology evolves, entry-level graduates will be able to adapt to technological changes. Students from other STEM disciplines also develop specific skills and a type of mindset that is applicable to the cyber security field, particularly since it is a relatively new discipline. A good grasp of fundamental principles and cyber security knowledge lays the foundations for when graduates go through company training. Generally, a degree in cyber security is needed to achieve this, but as long as students have the necessary competencies, companies will provide in-house training to improve technical skills.

Some entry-level jobs in cyber security do not require a high degree – or indeed any - technical know-how; these are typically non-technical cyber security roles. The research identified no instances of employers recruiting or being open to recruit graduates for technical roles who lack the basic technical competencies. Graduates in non-STEM subjects, e.g. arts or social sciences, will usually have to gain the necessary basic technical competencies via online tools, extra-curricular activities or undertaking a course, if they wish to take up technical jobs in cyber security and do not have a technical background.

However, some employers fill entry-level job vacancies with recruits from a variety of backgrounds, such as the Humanities or Business Studies. Examples of non-technical entry-level jobs include marketing and sales, positions involving the managing of client relationships, jobs dealing with the legal aspects of cyber security, those involved in recruiting cyber security staff and related human resources management functions. Whether a graduate has a technical background or not, they will usually go through in-house training to develop the specific cyber security know-how of a given company.

In recruiting graduates, most employers not only look for technical skills and basic knowledge of cyber security but also want other more rounded competencies including interpersonal skills, such as team working, problem-solving abilities, good writing skills, among others. One interviewee expressed the view that the balance between computing as a technical discipline and literacy skills has shifted too far. Many students are able to apply their computing skills, but are unable to type-up their work in a Microsoft Word document to a reasonable standard of English. The challenge, it is argued, is to restore the balance so students can support their technical skills and knowledge in cyber security with more rounded competencies. Employers also value other personal attributes and good all-round skills as being of great, if not equal, importance to technical know-how. Amongst these attributes are: an inquisitive mind; the capacity to think logically and solve complex problems creatively; having the mind-set to engage with the diversity and complexity of issues associated with cyber security; the ability to communicate clearly and a willingness to be trained.

Typically, basic cyber security knowledge will be taken for granted if a student has or is likely to gain a HE qualification at an acceptable level, but other personal attributes will be examined if they are asked to go to an assessment centre. 'Thinking ability' is the key attribute many companies are looking for rather than just technical skills. Softer skills, such as the ability to think critically, articulate arguments clearly or being able to justify a position in a convincing way are important requirements. A few employers also commented that one of the biggest entry-level barriers is the security clearance required to take up a job. A large IT firm explained that many entry-level graduates were still waiting to be cleared several months after being accepted to the role. Interviews with FE and HE institutions highlighted that they face challenges in providing placements for students in cyber security. Most employers do not want to place students in

positions that can compromise the security of the company without already having a high degree of knowledge and training.

Employers recruiting graduates with a non-STEM background into these sorts of entry-level jobs seek motivated individuals that have the potential to manage teams, who can communicate effectively, contribute to the business-side of the industry and have basic knowledge on the fundamentals in cyber security. The various focus groups with students also highlighted the role played by self-motivation and self-teaching in the cyber security field. Many young people use online website and programmes to deepen their knowledge in cyber security that they may otherwise not learn at school.

> *"At GCSE level we don't learn how to code or how to use other practical tools. Overall, I was not satisfied with what I was learning at school, so I turned to Google and the Internet to learn more"*
>
> Student

For many entry-level or junior cyber security positions, no specific information is usually provided by employers on the qualifications required for these jobs. To obtain further insight into factors influencing pathways into cyber security entry-level jobs, an analysis was undertaken of information on three job advertisement portals.[88] Approximately one hundred job advertisements were analysed, combining key words such as 'cyber', 'junior' and 'trainee'. The analysis indicates that for many entry-level or junior positions, no specific information is provided in the adverts on the qualifications required for entry-level jobs. Some jobs offer the possibility for those who are self-taught in cyber security (e.g. hobbyists) to enter the field outside the FE and HE pathways, including those initiating a career change. This confirms that there is a supply and demand issue and this is how some employers are getting around it. Equally, this suggests that employers often do not put as much emphasis on having completed a FE or HE course because they are more interested in motivated individuals with a real interest in cyber security and who can be trained irrespective of their academic background.

For the positions that do have qualification requirements, the analysis of job advertisements indicates that an undergraduate degree in a STEM subject is usually required. For example, a degree in IT or cyber security-related subject is required for a Junior Support Analyst (cyber security) position; a degree in Computer Science, Information Technology or a related discipline is required for an entry-level as a Cyber Security Analyst; and a Forensic Computing qualification (or similar) is required for a job as an IT Forensic Analyst position. For most entry-level jobs, technical skills are required in addition to soft skills. A small number of positions required industry certifications such as CISSP, GCFA, GCIH, CHFI or SEC+.

Industry certifications (e.g. CISSP, ISO 27001, CISCO) are also highly valued by employers. The most common certification is the Certified Information Systems Security Professional (CISSP). Many BSc and MSc students pursue industry certification before joining a company or do so while they are in an entry-level job. Universities also offer industry certification as part of a student's degree. However, the cost of sitting exams can prove a barrier where this is covered by an individual. For example, the current cost of CISSP is £650.[89] Students holding a degree certified by the NCSC are seen as attractive not only to the NCSC but also other employers. FE and HE representatives also highlighted the need for employers to provide new recruits with additional training, rather than expecting HE to provide the very specific skills needed for particular jobs.

[88] These included Indeed, Glassdoor and CV Library.
[89] ISC², 2018, Exam Pricing

3.3 Factors influencing the pathways

The pathways into different types of entry-level cyber security jobs[90] examined earlier in this section are influenced by a number of factors:

- Awareness of the different careers open to those with an interest in cyber security, including those of a non-technical nature;
- Whether the job requires technical know-how or not;
- If the job is technical, the degree to which specialised expertise is required;
- Employer characteristics, in particular the activity and size of the organisation.

Taking the first point, the research suggests that the pathways available to students who want a job in the field of cyber security are not particularly clear. This was apparent from several focus groups with students and from the survey responses provided by FE and HE representatives, of whom only 30% believed that students were "very aware" of the cyber security pathways open to them.[91]

The six pathways to entry-level jobs (Table 3.1) require varying degrees of expertise in cyber security. Technical expertise or understanding is generally expected for many jobs but is often difficult to attain, so highly technical entry-level roles require a lot of training either at FE and HE levels or through the employer. Indeed, as noted in Section 3.2, graduates of non-STEM subjects, usually have had to gain the necessary basic technical competencies via extra-curricular activities if they wish to take up technical jobs in cyber security. FE and HE representatives indicated that technical skills and theoretical knowledge are the most important (and difficult) competences to master at university, but they are typically the most sought-after employers.

As highlighted earlier, the pathways into entry-level jobs in cyber security are also influenced by the nature of the organisation that recruits personnel into such positions. Companies that specialise in providing cyber security products and services to clients typically recruit employees who have a high degree of specialised technical expertise (i.e. STEM background at the BSc or MSc levels). However, there is also scope in the same type of firms for graduates with non-STEM degrees to obtain entry-level jobs in fields such as customer service or sales. In other sectors of the economy, entry-level jobs usually involve less specialisation with graduates usually spending two to three years undertaking a variety of roles in the IT field before moving, perhaps after receiving in-house training, into a cyber security role. The situation differs in smaller organisations which typically recruit graduates with general IT qualifications but do not have the capacity or scale to allow a high degree of specialisation, whether in cyber security or any other IT field. Cyber security and/or computer science may not be readily available to students, so it can be difficult to get into FE and HE establishments because there is a lack of understanding and information regarding the other routes into the field.

[90] An entry-level job is the first job a person takes upon completing a Further Education or Higher Education course. An entry-level position may not require some level of work experience and can also refer to the entry point into a given career. This means that graduates having worked one or two years in an un-related field before entering cyber security also qualify as entry-level graduates because it is their first step in the field. Further to this, an individual that is at mid-career stage who switches fields will also qualify for an entry-level position although their progression may differ from a recent university student that has limited professional experience.

[91] One-third of respondents (n=33) answered this question.

4 How Cyber Security Courses are Developed and Industry's Role

4.1 How cyber security courses are developed

Cyber security courses have evolved in most cases from existing computer sciences (or similar) courses, initially as a module and then developing in some cases into a separate course in its own right. The decision by FE and HE providers to introduce a course or module (or not) is driven by a combination of factors, with evidence of demand and the capacity to deliver such courses being perhaps the most important considerations. In the case of postgraduate degrees, income generation may also be a factor, although no direct evidence of this was found.

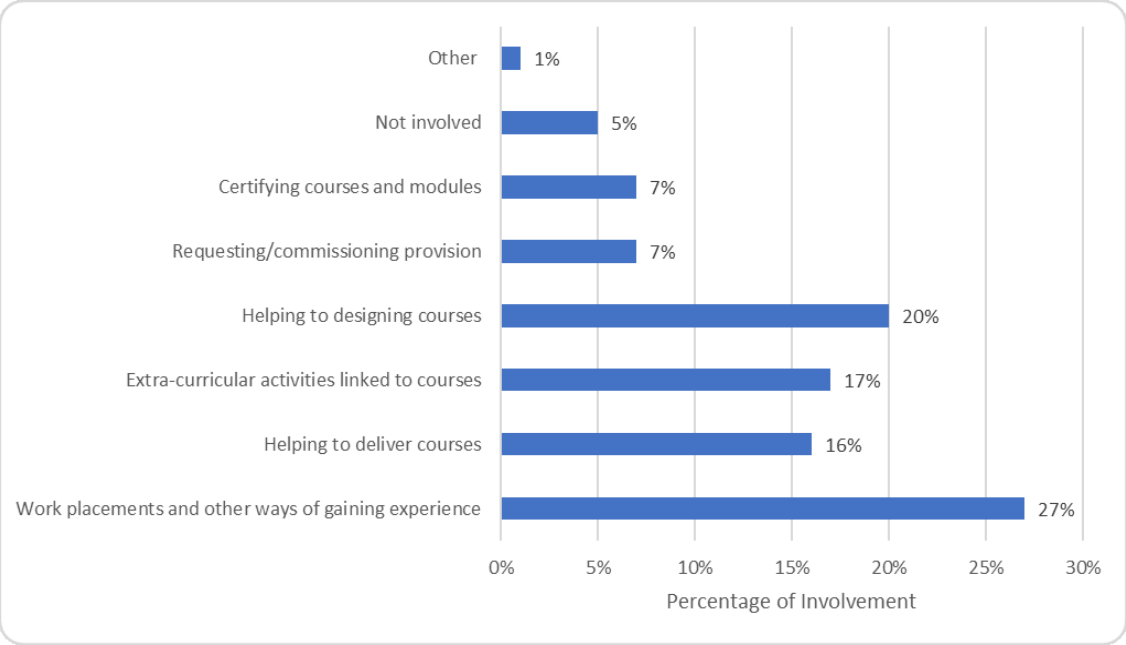
Demand for places on cyber security courses has, as noted in Sections 1 and 2, been growing quickly in recent years, reflecting demand for skilled personnel, the career opportunities open to professionals and the interest of students in the field. Sufficient demand therefore exists, although this is not evenly spread across different institutions in the FE and HE sectors and, as with all subjects, various factors will influence the decision of students to apply for places at particular institutions (content of the courses, location and reputation of the institution, cost in the case of postgraduate degree courses, etc.).

Even if demand exists, this in itself may not be sufficient for an FE or HE institution to introduce a cyber security course or module. As argued in Section 2, one constraint that can exist is not having staff with the required knowledge to teach the subject. This consideration was highlighted in the key stakeholder workshop, with several participants arguing that they could not recruit cyber security staff because they were unable to offer salaries that are competitive with those available in industry. A few FE and HE representatives also explained they had left the industry years ago, so they themselves also feel out of touch with current developments in the industry. The investment in ICT equipment and the provision of professional certifications for some of the more specialised courses was also highlighted as an issue. For these and other reasons, some FE and HE providers do not offer cyber security courses.

In terms of the cyber security course content, academics with specialist expertise in this field will know what should be taught as part of courses or modules. They can also compare their own offering with the courses available at other institutions. In many, if not most cases, FE and HE providers seek to collaborate with industry, either with firms that provide ICT services (Cisco, Microsoft, etc., but also smaller businesses, for example spin-outs from universities that provide cyber security services) and/or with companies in the wider economy (e.g. the automotive sector). The stage at which industry gets involved in the development of cyber security courses, and the nature and extent of such involvement, can vary widely.

Figure 4.1 shows that employers work with FE and HE institutions in many different ways in the cyber security field. Providing work placements, helping to design courses, providing opportunities for extra-curricular activities, and an involvement in delivering courses are all common forms of engagement.

Figure 4.1: Percentage of FE and HE institutions indicating that employers or industry bodies are involved in developing cyber security courses and modules



Source: survey (N=31)

4.2 Role of industry in developing and delivering courses

FE and HE institutions are keen to get industry involved in helping to determine how cyber security courses and modules are developed so that they are geared up to meeting employers' needs and providing students with jobs. The literature suggests that the nature of successful employer engagement is based on long-lasting, mutually acceptable and beneficial relationships between schools and businesses. However, significant benefits occur when these activities are incorporated in the structures and models that allow for a more substantive up-scaling and coherence of provision at a local and national level.[92] For the reasons mentioned above, it is important for FE and HE providers of cyber security courses develop a relationship with employers, not only to help ensure that career pathways exist for students but also to draw on the expertise and other support companies can provide in delivering courses.

[92] Department for Business Innovation & Skills, 2014, Understanding the Link Between Employers and Schools and the Role of the National Careers Service

Box: 4.1: Examples of industry involvement in cyber security courses

- **Ada, the National College of Digital Skills** – has a group of founding partners consisting of Bank of America Merrill Lynch, Deloitte, Gamesys, IBM, King and the Aldridge Foundation. From October 2018, EY (Ernst & Young) will offer students an opportunity to work in its Technology Consulting group as part of a degree apprenticeship in Digital Innovation.
- **Birmingham City University** – offers an MSc in Cyber Security in conjunction with Cisco Systems, Oracle and the Microsoft Academy Centre.
- **Imperial College** – works with an industrial advisory board of companies that can sign up and make suggestions on what the university should include in its course content. All types of companies are registered and although few are specific to cyber security, it does have some representation on the board.
- **University of Warwick** - the BSc Cyber Security is certified by NCSC and is a four-year course with industry involvement through the university's Warwick Manufacturing Group's Cyber Security Centre. There are especially strong links with firms such as Jaguar Land Rover from the automotive sector.
- **Royal Holloway** – has close links with a number of ICT companies that are involved in teaching degree courses, running careers events, on-campus assessment centres and other ways of engaging with students. It is also working with ISC^2 to make it possible to attain the Certified Information Systems Security Professional (CISSP) qualification at the end of the Master's course in cyber security.

The nature of industry involvement ranges from being closely involved in delivering modules and providing placements or participating in apprenticeship schemes, industry seminars and careers events to simply recruiting cyber security graduates. It is apparent that some FE and HE institutions have very close links with industry (e.g. Royal Holloway, University of Warwick, Imperial College) but that this is not the case with many others.

An example of best practice is seen at the University of Plymouth, which shares on its website ways to work with industry to enhance the employability of students. They explain employers can get involved through employer advisory panels, providing work experience, act as mentors, host workplace visits, give lectures or take an active role in assessments.[93] There are also platforms that provide brokering services to link industry and academia, such as Konfer, a platform to promote and showcase the array of research and innovation opportunities that can help businesses grow.[94] By facilitating and enabling university and business collaborations, they want to change opportunities can be searched for by businesses.

Although this study did not specifically examine the role and impact of FE and HE careers services on recruitment, many institutions have careers advice available to students. At the FE level, the Careers and Enterprise Company helps improve schools' careers provision by building a network linking schools and employers.[95] At the HE level, careers advice is usually provided internally to undergraduate and postgraduate students so they can obtain information and guidance on employment opportunities. In some cases, universities organise careers fairs, where recruiters from a variety of organisations meet students to explore different career paths.

The interview feedback revealed that many companies wish to be more involved in general, but simply do not know how to engage with academia. There is considerable untapped potential regarding the links that could be developed between smaller firms and academia. Smaller firms do not have the same resources as larger companies do and so are often unable to get staff involved

[93] University of Plymouth, 2018, Employer Engagement Opportunities
[94] Konfer
[95] The Careers and Enterprise Company

as visiting lecturers or to attend job fairs. As a result, smaller companies are often left out of these processes.

HE providers try to follow the needs of industry and try to tailor their courses to developing the skills and knowledge which are highly sought-after by employers. Examples of this include courses developing industry liaison panels or advisory groups to advise on course content. De Montfort University has developed its course with Deloitte, Airbus, BT and Rolls-Royce, with students being assessed by cyber security professionals from industry. Similar to BSc level, courses are accredited by a wide range of bodies; predominately the British Computing Society (BCS), but also by institutions such as the Institute of Technology and Engineering, and CISCO. These links with industry are likely to be the reason why some universities offer bespoke cyber security programmes, such as the automotive programme cited. In addition to this, for some universities the predominant focus is to prepare students to be able to manage risk at a high-level, and not necessarily focusing on developing the full complement of lower-level technical skills. This is a good approach, as cyber security itself needs individuals in all areas of specialism.

Industry has an especially important role to play in encouraging students into the cyber security sector through talks, showcasing careers or attending career events. In addition, industry can get involved by providing cyber security students with work placements, internships, apprenticeships and other forms of work experience. As noted in Section 3, whilst technical knowledge is important, employers also look for work experience in candidates applying for jobs. In relation to apprenticeships (Section 2), most options involve FE institutions working with employers in their areas to provide placements but in other cases, specifically some of the larger companies, the schemes are initiated and run by the organisations themselves. Industry also plays an important role earlier in the educational process by participating in schemes such as the STEM ambassadors.

Box: 4.2: Cap Geminis Cyber Security Higher Apprenticeship scheme

- Cap Gemini, a multinational management consulting company with 190,000 employees around the world, has introduced an 18-month Cyber Security Higher Apprenticeship scheme. Apprentices earn £10,000 p.a. while working as a Cyber Security Analyst and studying for A Level 4 qualification. The training is described as following a structured development plan covering technical security fundamentals and leads in to roles such as Cyber Security Specialist and Cyber Security Analyst. To be eligible, it is necessary to have 7 GCSEs at A-C or 4-9 including English and Maths, and at least three C's or '4s' at A Level or a minimum of at least one merit at BTEC, preferably in a STEM subject.
- The study programme is designed to fit around full-time employment and uses a blended learning approach that mixes distance learning, work-based study and on-campus study days.
- The Cyber Security Higher Apprenticeship is part of a wider scheme that includes a Digital & Technology Solutions 9-week training course. Since 2011, over 500 young people have undertaken Cap Gemini apprenticeships.

The level of industry involvement is to some extent influenced by geography and the degree to which FE and HE institutions are located in areas of England with strong technology-based firms. For example, the company Nexus has recently moved its headquarters to the outskirts of Exeter. As a result of this, Exeter College is now building a close relationship with the firm and employees at Nexus regularly come to the college to speak to students. Having employers nearby helps to improve the links that FE and HE providers can develop with industry. Another example is the University of Warwick, which collaborates closely in designing and delivering its courses with Jaguar Land Rover and other automotive firms in the West Midlands. By contrast, the research identified several FE and HE institutions that find it more difficult to secure employer engagement

because of the nature of the local economy and absence of companies in their areas with an ICT orientation.

The extent of the links between industry and the FE and HE sector also depends on the employer side and on the nature of their activities. Not surprisingly, firms that specialise in providing cyber security services (IT companies, the major consulting companies, etc.) have the closest links with the HE sector. 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.

> *"Our firm recruits 10-20 cybersecurity personnel each year. We work closely with several universities on their course content (e.g. penetration testing) with a view to trying to get commercial realities into courses."*
>
> Employer in the defence sector

Although they may not be involved in delivering cyber security courses, most of the employers covered by the research recruited students directly from university or via apprenticeships to help fill entry-level jobs. There were some exceptions to this. For example, a consulting company indicated that they only recruited a small number of graduates directly from universities because the specialised nature of its advisory work means that it has to recruit people with more knowledge and experience than those just leaving university are likely to have. However, there is a view amongst FE and HE representatives that employers could do more to attract students to apply for jobs in cyber security. Further to this, there is scope for industry to have a stronger role in providing careers advice to students and enticing students into cyber security, particularly those studying computer science or other STEM-related subjects. This is where initiatives, such as STEM Ambassadors, might help link FE, HE and industry in order to boost the confidence of students to pursue cyber security as a career.

As noted earlier, employers have quite specific expectations with regard to the attributes they look for in entry-level cyber security applicants. There is a widespread view among interviewees that students needed a particular mindset to work in cyber security. Students should be able to think through issues from the perspective of what threats they could face - a 'constructive paranoia.' They also needed to have a good understanding, or as one employer described it 'an empathy' for how humans work; they need to understand how people's behaviour could make them vulnerable to cyber-attacks. Above all, students need to be willing and able to learn new skills and have well-developed problem-solving skills. Also, the constant developments in the field mean that cyber security students should be developing and renewing their skills and knowledge throughout their career.

There is a consensus among cyber security employers that there needs to be a more holistic approach to cyber security training that encompasses people not specifically working in cyber security. Employers consulted for the study spoke of the importance of all employees having a general appreciation of online risks and the steps that can be taken to mitigate them. Consistent with the Ipsos Mori report,[96] this is seen as being particularly important for SMEs as they usually do not have the resources to hire somebody specifically to work on cyber security but, at the same time, are at increasing risk from cyber-attacks.

The research also highlighted the fact that developments in cyber security are happening so rapidly that academia cannot often keep up with the latest software or cyber security skills. This means that a lot of the technical skills students learn can quickly become out of date, which is also why the majority of entry-level graduates go through in-house training. Students in the various focus groups expressed their frustration of having to use old software that is no longer used by

[96] Pedley, D., McHenry, D., Motha, H., Shah, J., 2018, Understanding the UK Cyber Security Skills Labour Market, Ipsos MORI

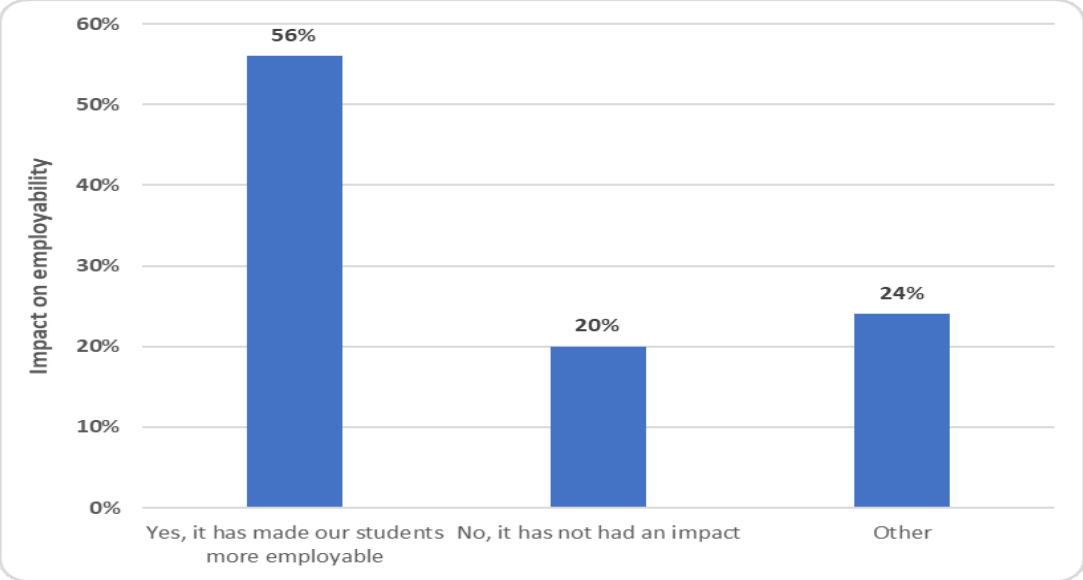
industry. Whilst many roles do require knowledge of a programming language, it is also the case that there are so many different computer software and programmes that is not feasible for students to know all of them. A general understanding of how computer networks operate is seen as necessary skill and a background in STEM is important to develop a logical way of thinking.

A consistent message from this research is that students require certain basic foundational skills that can be applied to new and developing technologies. HE institutions also recognise the importance of developing soft skills as a part of this and argue that their courses develop such skills by teaching students how to make presentations, report writing and participate in group work. They often chose to focus on the foundation technical skills such as understanding computer networks, rather than developing soft skills.

4.3 Industry-recognised professional certifications

As can be seen in Figure 4.2, the majority of survey respondents claimed that accreditation such as NCSC certified degrees, BSc certification or IISP enhance the employability of students completing cyber security courses and modules. This can be helped by ensuring courses are very closely linked to employers' own certification. For example, Birmingham City University's MSc in Cyber Security is linked to the Cisco Systems' specialist certification - Securing Cisco Networks with Threat Detection and Analysis (SCYBER). Likewise, a number of universities have courses certified by the NCSC.

Figure 4.2: In your view, have these accreditations had an impact on employability?



Source: Survey (N=23).

As explained in Section 2, many courses are accredited by the BCS and other bodies such as CISCO, the ORACLE academy, the Institute of Engineering and Technology and Chartered IT Professionals. It should be noted that industry accreditation, such as CISCO, can focus on students just learning how to use products developed by that company and may not equip them with the skills to use other operating systems or networks. Another accreditation body with a strong international character is (ISC)[2].

Box: 4.3: Cyber Security certifications that can be gained as part of FE and HE courses

- Certified Information Systems Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)
- Certified Cloud Security Professional (CCSP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- HealthCare Information Security and Privacy Practitioner (HCISPP)
- Information Systems Security Architecture Professional (CISSP-ISSAP)
- Information Systems Security Engineering Professional (CISSP-ISSEP)
- Information Systems Security Engineering Professional (CISSP-ISSMP).[97]

As noted earlier, a problem that can arise for FE and HE is the cost of providing some industry certification courses that employers want. For example, one university claimed that it costs them around £1,000 per student to run a course leading to CISCO certification (training academic staff, fitting out a computer lab specifically for CISCO purposes, employing several technicians, etc.) but it is only possible to recoup around £600 per student through fees. This suggests that often HE and FE institutions cannot keep up with industry in terms of provision of skills. Many courses offer students a range of industry recognised professional certifications (see Appendix A).

4.4 How well-matched are FE and HE provision to employers' needs?

The research suggests that employers have a generally positive view of the role played by FE and HE in helping to address the cyber security skills gap. The research suggests, however, that there are some conflicting perceptions. Feedback from representatives of the FE and HE sectors suggests that employer expectations can be unrealistic with regard to the skills students are able to develop as part of an FE or HE course. For example, a MSc course typically only involves 200 hours or so of course work, whereas industry often trains entry-level graduates for a period lasting around six months. Another university suggested that the specification they had received for a job vacancy aimed at graduates in cyber security would have been more appropriate for somebody at a midpoint in their career.

At the same time, there is some criticism from industry that universities are not tailoring courses closely enough to their needs. FE and HE courses are seen by some as often too academic with an insufficient grounding in the practicalities and needs of industry. One company consulted for the study was especially critical, arguing that universities are more interested in offering cyber security Master's courses because they can charge high fees for them and that this was the motivation rather than trying to meet future employer needs.

To some extent, the criticism that cyber security courses are too 'academic' is reflected in feedback from the various focus groups undertaken during the course of this study. These suggested that students often find their courses to be too theoretical and not practical enough. As noted earlier, some students have to work on outdated software or computer systems, which means that it is more difficult to develop the know-how that is needed in a job. Since some courses cannot keep up with the ever-changing nature of cyber security, FE and HE providers focus on teaching the basic foundations. Feedback from the stakeholder workshop suggested that employers are happy with students that learn the basic foundations of cyber security because they are needed later on if graduates have to adapt to technological changes in the industry.

[97] ISC², 2018, Our vision

"I think some of the things they (students) learn is outdated. JavaScript is a good foundation, but as industry, we want more big-data skills, more rounded-engineers that don't just develop stuff. For example, the fundamentals of software engineering don't change but familiarity with tools needs to be up to date."

Employer

As an alternative to a full-time degree, and a way of bridging gaps in what HE and FE can achieve with students and what employers expect, the apprenticeships option and part-time degrees seem to have many advantages. The attractions include the more practical approach to cyber security combining 'on the job' and class-based training but also the fact that the costs (in the case of apprenticeships) are covered by the apprenticeship levy. The requirement to spend one day a week studying, often in an individual's free time, is also seen as positive insofar as it demonstrates a commitment to the job and to gaining a qualification. Degree apprenticeships have a similar appeal. But there can also be complications. One company that participated in the research is paying for three employees to do a part-time (cyber security) MSc at Lancaster University. They argued that doing a part-time MSc in cyber security is a big challenge not only for employees but also for the company because of the disruption releasing staff to study for a qualification can cause to the firm's operations. Consequently, it is working with the university to try to find ways of improving how the part-time MSc programme is organised.

Overall, collaboration between the public sector, industry and academia is widely seen as crucial in designing high quality courses as well as promoting the transition of workers from other roles into cyber security. This study did not assess the extent to which the quality of FE and HE cyber security courses is linked in any way to employer engagement with course providers. However, a study by the Department for Business Innovation & Skills finds that the quality of courses is likely to be better where employers are involved in their design and delivery than where they are not.[98] Putting aside the question of how 'quality' should be defined, it is likely that employer engagement leads to courses providing students with better insights to 'real world' cyber security issues and technologies than they are likely to gain otherwise. Insofar as employer engagement helps to ensure that FE and HE provision reflects their needs, this should make it easier for graduates to demonstrate that they have the knowledge required for entry-level jobs in cyber security.

[98] Department for Business Innovation & Skills, 2014, Understanding the Link Between Employers and Schools and the Role of the National Careers Service

5 Gender Balance in Cyber Security

The research for this study indicates that the gender balance in cyber security is still a significant problem. According to other research, at present women only constitute 11% of the global cyber security workforce and 7% in Europe.[99] This percentage has remained steady since 2013.

Part of the reason for this situation is that the field of cyber security is still dominated by stereotypes and widely perceived as a male-dominant field. There is a tendency for the wider population, and particularly women, to view cyber security as a 'geeky', rigid, and isolating field.[100] Often the language adopted when talking about the industry is considered "too opaque, too intimidating, and full of male connotations" and there is a lack of understanding around what the industry is, and what skills are required.[101] Some reports have highlighted the issue of pay gaps between male and female IT specialists as a factor discouraging a gender balance. The difficulty of progressing professionally may also contribute to the poor retention of women in cyber roles.[102] Other studies point to the various forms of discrimination women face in the workplace more generally.[103] There are also cultural biases that inhibit women entering the field. Some studies show that in women's formative years, teachers, parents and mentors may consciously or unconsciously steer them away from fields believed to be more masculine.[104]

An analysis of data relating to FE and HE for the previous three academic years indicates that there has been a slight decrease in female enrolment at the FE level. At the same time, the percentage of female students at the HE level studying cyber security has remained the same. At the HE level, there has been a 28% increase in the number of students undertaking a cyber security course, or course in a relevant subject from 2014 to 2017, but the proportion of female on courses has remained the same across the years.

Table 5.1: Gender breakdown by year across FE and HE in cyber security courses or courses with a cyber security module

Academic year	2014/2015		2015/2016		2016/2017	
	Male	Female	Male	Female	Male	Female
FE	86%	14%	86%	14%	87%	13.1%
HE	85%	16%	84%	16%	84%	16%

Source: AoC and HESA.

The gender imbalance for students entering STEM subjects can be traced back to pupils' subject choice at A level. Data from the Department for Education that is analysed in Table 5.2 indicates that A level Maths and Science participation increased for all subjects in 2017 compared with 2016. However, male pupils accounted for higher increases in Maths and Computer Science compared with female pupils. There is also a higher proportion of male pupils entering computer science than females. A study by Cambridge Assessment revealed that patterns for AS and A Level choice tend to follow gender stereotypes, with male pupils preferring Maths, Physics, Computing

[99] Centre for Cyber Safety and Education, ISC², Executive Women's Forum, 2017, The 2017 Global Information Security Workforce Study: Women in Cyber Security – A Frost & Sullivan White Paper
[100] Jethwani, M., e.t. al, 2016, "I Can Actually be a Super Sleuth" – Promising Practices for Engaging Adolescent Girls in Cyber Security Education
[101] CREST, 2017, Closing the Gender Gap in Cyber Security
[102] e-Skills.uk, 2014, The Women in IT Scoreboard, British Computer Society
[103] Centre for Cyber Safety and Education, ISC², Executive Women's Forum, 2017, The 2017 Global Information Security Workforce Study: Women in Cyber Security – A Frost & Sullivan White Paper
[104] D'Hondt, K., e.t. al, 2016, Women in Cyber Security, Harvard Kennedy School

or ICT, whereas female pupils prefer subjects involving Humanities, such as English, Biology, Psychology, Sociology or Modern Languages.[105]

Table 5.2: Percentage of A Level students entering for Maths and Science A Level by gender, England, (2016-17)

	Female		Male	
Subject area/ Academic year	2016	2017	2016	2017
Maths	17.0%	18.1%	31.8%	33.0%
Further maths	2.2%	2.3%	6.7%	7.1%
Biology	18.0%	18.6%	13.5%	13.5%
Computer Science	0.3%	0.4%	3.3%	4.5%

Source: Department for Education

Since a high number of cyber security professionals come from a STEM background, the research also looked at other STEM subjects that can be combined with a cyber security course. The research suggests that the situation with regard to the cyber security gender balance reflects the wider situation in STEM-related subjects more generally.

Table 5.3 indicates the gender imbalance across STEM subjects also exists at university level. The largest gap in subject areas that are relevant to cyber security in the 2016-2017 academic year is seen in Engineering and Technology, with only 17% female enrolment; and in Computer Science with only 16.5% female enrolment. The percentage of female enrolment is similar when compared to cyber security, which only had 16% female students in the same academic year (2016-17). HESA data indicates that the number of women studying computer science has remained stable in the past three years, but the numbers have slightly increased for women studying Engineering and Technology.

Table 5.3: Gender breakdown for STEM Degrees (2016-17)

Subject area	Female	Male	Other
Biological Sciences	63.0%	36.8%	0.2%
Physical Sciences	40.7%	59.0%	0.3%
Mathematical Sciences	36.0%	63.2%	0.8%
Computer Science	16.5%	83.2%	0.3%
Engineering & Technology	17.5%	82.4%	0.1%

Source: HESA.

Data obtained from Universities UK (UUK) in 2016-17 revealed that 17% of students studying computer science were female at undergraduate level. When excluding international students, the percentage of female UK nationals taking computer science reduces to 14.5%. The numbers tend to improve at postgraduate level, with 26.6% of students taking an MSc Computer Science course being female. The proportion worsens again when looking only at female UK nationals, who made up 22.3% of students taking an MSc Computer Science course. The data obtained through HESA depicts a similar picture, with the percentage of female students domiciled in the UK reducing to 14.5% in 2016-17 at undergraduate level and down to 6% at postgraduate level.

The data obtained by UUK and HESA is consistent with the feedback received from the research. Many FE and HE representatives claimed that in general, the gender balance is worse among UK students studying cyber security than overseas students. A higher proportion of female

[105] Cambridge Assessment, 2007, AS and A Level Choice – Gender Makes a Difference

international students from countries such as Asia and/or the Middle East take courses/modules in cyber security with anecdotal evidence suggesting that they are more likely to get into IT fields back home. Since international students are often over-represented at MSc level in UK universities, this may explain why there are more female students in some MSc courses.

There are some notable exceptions with regard to the gender imbalance with some HE institutions having a high proportion of women on their cyber security courses. At the University of Middlesex, for example, there are more women than men across three separate cyber security courses. No specific reasons were given for this and, in fact, there are slightly more male applicants but female applicants are most likely to accept their university offers. Likewise, at the University of Leicester, two-thirds of students on a specific cyber security module are women and at the University of Oxford, almost half of all cyber security course participants are women. An explanation is that female students choose to apply to prestigious universities as opposed to other universities. At the Centre for Doctoral Training in Cyber Security at the University of Oxford, more than 30% of doctoral students are women. One explanation is that there are female role models within the Department. The balance is better among cyber security doctoral students as opposed to computer science doctorates, because the former field is more multi-disciplinary, attracting a larger pool of potential recruits to draw on.

Box: 5.1: Examples of gender balance on cyber security courses

- **University of Leicester:** 60% of students taking module on data protection are female
- **University of Middlesex:** MSc Cybercrime and Society: 17 students (14 female; 3 male); MSc Regulatory Practices and Policing Cybercrime: 6 students (5 female; 1 male); MSc Cybercrime: 37 students (24 female; 13 male)
- **University of Oxford:** Between 30% to almost half across all Cyber Security students are female. At the Centre for Doctoral Training in Cyber Security, more than 30% of doctoral students are women. One explanation is that there are good female role models within the Department. The balance is better among Cyber Security doctoral students as opposed to Computer Science doctorates, because the former field is more multi-disciplinary, attracting a larger pool of potential recruits to draw on.

Source: Interview programme.

In the online survey, 82% of the 36 representatives of FE and HE providers answering questions on gender issues claimed there were fewer than 30% of women enrolled in their cyber security courses in the 2017-18 academic year. Forty-one per cent of these indicated that there were fewer than 10% of women. Overall, it seems that the gender gap is worse at FE level, at undergraduate level for HE providers and worse among UK nationals.

5.1 Reasons for the gender imbalance

There is already quite a lot of research – both in the UK and other countries – as to why the gender balance in technology-related roles is worse than in the labour market generally.[106] Factors that are known to be important in deterring young women from entering the cyber security sector include a lack of awareness of what cyber security is about, what a career in this field has to offer, and a stereotype that the role is 'geeky' and better suited to men (this perception also applies more widely to STEM-subjects although this depends on the country)[107].[108]

[106] To take an example from outside the UK, PubAffairs Brussels recently hosted a debate on cyber skills gap and whether a more gender-balanced workforce could fill the substantial skills shortage affecting the cyber security field.
[107] For example, according to the 2017 EU gender equality index, the proportion of male graduates to female graduates in STEM subjects is 75% to 25% in the Netherlands, 70% to 30% in Belgium, whereas, it resulted 50% to 48% in Turkey, and 49% to 51% in Bulgaria.

Other reasons include the lack of educational focus and interest at an early age in Science, Technology and Maths, which are all fields that can potentially lead to a career in cyber security. Other research highlights that the problem is also a cultural issue with a stigma that girls do not study Maths, Science or Technology at school.[109] The findings of this study are consistent with the reasons highlighted in the wider literature.

A number of FE and HE representatives consulted for this study suggested that female students are also deterred from taking cyber security courses or modules because the field remains predominantly dominated by male professionals. Moreover, teaching staff at both FE and HE levels are mostly male. This means that female students or prospective female students have few female role models to look up to. This influences the number of women choosing cyber security at university because they do not see the subject as leading to a viable career. This may help explain why the overall proportion of female students doing STEM subjects drops off after A Level compared to males.[110]

> *"Girls are intimidated by the gender imbalance – I was worried that there wouldn't be many girls (at CyberFirst). Girls in general don't want to compete against boys"*
>
> Student

The online survey for this study indicates that 60% of FE and HE academic staff agreed that female students do not perceive cyber security as an attractive career. The gender imbalance in the educational building blocks is mainly due to women not applying to these courses (see Figure 5.1). This was further supported by feedback from the interview programme. For example, an interviewee from one university argued that women think they will not get the same opportunities as men in this field because cyber security has competitive and male-oriented connotations so women assume they will have too many barriers to overcome.

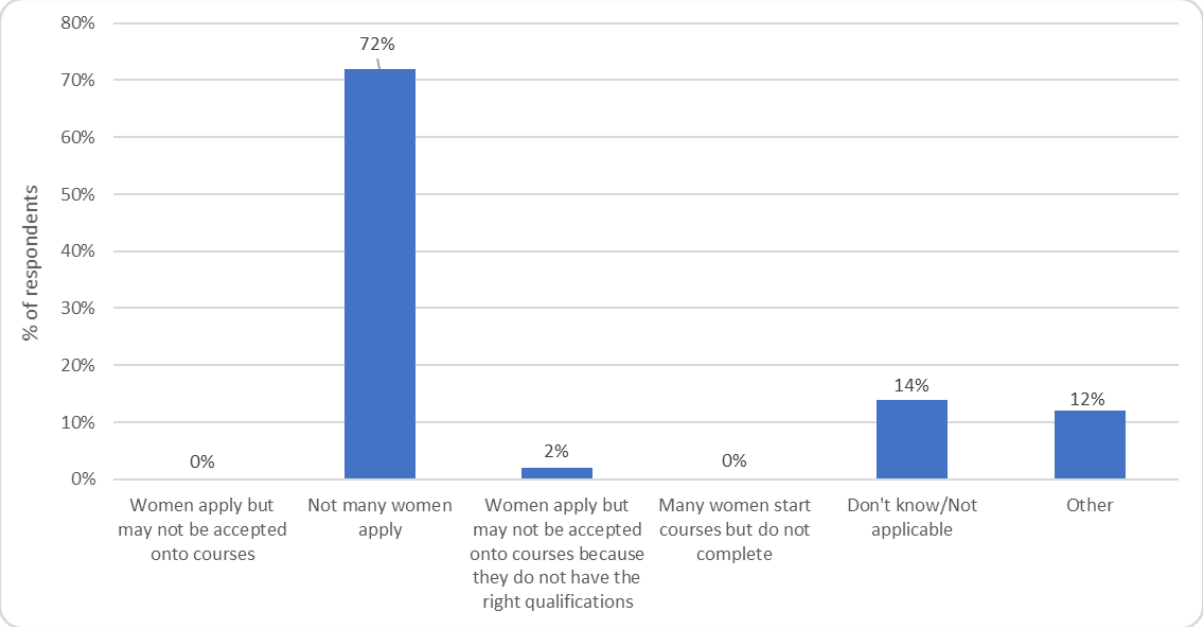
> *"It starts at primary school and the perception of computer science: it appeals only to the male hacker. If girls cannot see that you can be involved with technology-based subjects without being a geek, we are all fishing in a very small pond."*
>
> Higher Education representative

[108] Among the reasons for not selecting a career in cyber security according to a study are: a lack of experience of computer coding (57%); not having any interest in computing as a career (52%); and not being aware of, or knowing enough about cyber security careers (45%), were the most prevalent among women. The study concluded that: there is a need for cyber security to be better positioned as a viable career choice for young women; that the career itself needs to be promoted among young women, by women, and the industry as a whole; and that young women need to be made aware of, and get help developing, the skills required to work in the industry. Source: Kaspersky Lab, 2017, Beyond 11% - A Study into Why Women Are Not Entering Cyber Security

[109] Zahout, M., 2017, Women in Cyber Security, McCloy Fellowship on Global Trends

[110] Women in Science, Technology, Engineering and Maths, 2014, The talent pipeline from classroom to boardroom

Figure 5.1: In your view, what is the reason for the gender imbalance?



Source: CSES survey. N=43

A further consideration is that women are not always aware of the career opportunities available to them in cyber security. There are not many places women can go to for careers advice designed specifically for women in cyber security. Also, women often do not have access to mentors to help develop their interest in cyber security or STEM subjects more generally. A number of FE and HE representatives suggested that more should be done at primary school level to encourage women into the field at a younger age. This reflects the fact that according to the Careers Strategy from the Department for Education, children form views about careers at an early age. By the time girls are 13 or 14 years old, they often already have an idea of the type of career that they want to pursue. At this age, girls already have pre-conceptions of the technology field in general.

Some of those consulted as part of the research claimed that collaboration between FE and HE institutions and local schools is not developed enough to encourage girls into the cyber security field. For example, the University of Birmingham offered Saturday lessons in cyber security and Computer Science to local schools but found that most girls in the 13 to 14 year-old age group were not interested. The university ended up only providing lessons to pupils in private schools and grammar schools which was not the aim of the initiative. This and other research feedback suggest more needs to be done to encourage an interest in cyber security at a young age, for both girls and boys.

> *"Some of this is a flow-through from a gender imbalance in A Level choices - without so many women in STEM A Levels (critically, Maths in particular), there will necessarily be fewer in STEM-related fields later in life."*
>
> Higher Education representative

As noted earlier, the gender gap is not specific to cyber security and instead can be seen across STEM subjects generally. The low enrolment rate amongst female students in cyber security is seen as reflecting a wider problem across England's educational system. Fewer female students choose to study STEM subjects, and according to WISE, women make up only 14.4% of the UK STEM workforce and 17.5% in the ICT sector.[111] A lecturer interviewed for this study commented that all-girl schools tend to offer better access to STEM subjects and generate more applications to universities because there is less negative stereotyping.

> *"There are so many opportunities for girls, but there is a lot of discouragement. Not enough girls are interested and girls are not being pushed into these subjects"*
>
> Student

5.2 Steps being taken to address the imbalance and best practice

At a national level, there are several programmes aimed at attracting women to the cyber field such as the CyberFirst Girls' Competition (NCSC).[112,113] The competition was launched in 2017 and is aimed at schoolgirls aged 12 to 14 years old so they can practice their skills in a simulated real-world environment. The objective of the programme is to serve as a pipeline into FE and HE cyber security courses or modules. **CyberFirst also runs specific girls-only summer courses for 14-18 year olds.** However, despite national interventions to encourage more women into cyber security, the gender gap remains and more initiatives to promote gender balance need to be implemented.[114,115]

The gender imbalance is not the only feature of cyber security, particularly since other socio-economic groups are also under-represented. The Global Information Security Workforce Study (ISC) explored the minorities' representation, not only by gender but also by age, tenure, ethnicity and race.[116] According to this research, minority professionals make up a significant portion of the cyber security workforce but are under-represented across senior roles within their organisations. Mentoring schemes have proved to be a good way to incentivise the enrolment into cyber studies and seem to have more positive effects for women.[117] It is interesting to highlight the related case studies of the Cyber Security Challenge UK.[118] As one report argues, "it is not just about getting more women into the cyber security field", [119] it is about creating diverse workforces with people from all types of backgrounds.

> *"Cyber security is an easy sell for women. However, the difficulty lies in convincing them - it is an attractive field with opportunities for all types of backgrounds."*
>
> Cyber-security expert

Many FE and HE providers have measures in place to attract more women to their cyber security courses or modules. Some steps taken by FE and HE providers to ensure gender balance across cyber security courses include the following.

---

[111] Women in Science, Technology, Engineering and Maths, 2018, Industry-Led Ten Steps
[112] CyberFirst – Girls Competition
[113] National Cyber Security Centre, 2018, 4,500 Young Women Race to Complete CyberFirst Girls Online Challenge
[114] Forbes, 2018, Why so Few Women Work in Cyber Security (and how we can change it)
[115] Centre for Cyber Safety and Education, ISC², Executive Women's Forum, 2017, The 2017 Global Information Security Workforce Study: Women in Cyber Security, A Frost & Sullivan White Paper
[116] Centre for Cyber Safety and Education, ISC², 2018, Innovation Through Inclusion: The Multicultural Cyber Security Workforce, A Frost & Sullivan White Paper
[117] Janeja, V., e.t. al, 2018, Enhancing Interest in Cyber Security Careers: A Peer Mentoring Perspective
[118] Cyber Security Challenge UK, 2018, Women in Cyber Security
[119] Zahout, M., 2017, Women in Cyber Security, McCloy Fellowship On Global Trends

Box: 5.2: Steps to help ensure gender balance

- **At Ada College**, in addition to informal quotas (e.g. admitting four women each academic year), interviews with prospective students tend to brand cyber security courses in a way that appeals to a broader target group. This means that academic staff do not emphasise coding or hacking skills, but rather look for transferable skills that might encourage students from a variety of backgrounds to their courses. The College recently organised a blockchain conference and received help from women working in the industry. The college also found that they received a higher number of female applicants to their less-technical apprenticeship programmes in computer science. Other initiatives have been taken to change how apprenticeships are labelled at the College to attract more female students (section 5.2).
- At **Exeter College**, efforts have been made to develop relationships with local schools to encourage more girls to consider studying for a cyber security qualification. The college has also tried to boost the number of its female IT staff (50% of its IT staff are now women). Despite these efforts, Exeter College has struggled to attract more female applicants to its cyber security and computer science courses.
- **Lancaster University** has worked on removing all masculine cyber security related language from its MSc programmes to attract more women to their courses. So far, this has led to a better gender balance.
- At the **Open University,** all modules, including cyber security, go through a review for equality and diversity issues. Staff members that have in depth understanding of these issues convene to assess what may affect the successfulness of attracting women onto a given module. Steps to remedy these issues include ensuring the course description language is inclusive, welcoming and attractive to all, irrespective of gender. This inclusivity element is done in parallel to everything else in course and module development.
- The **Government Security Profession Unit** found that some aspects of their apprenticeship selection process were deterring many female students. A group exercise required five to six students to sit around a table and engage in conversation with the aim to get a main point across. Due to the confrontational nature of this exercise, women were scoring very badly at this exercise. Recruiters changed the format of this assessment and now allow applicants to pair up in groups of two. A formal assessment has yet to be done, but so far it seems this has helped restore the balance between female and male scores in the overall recruitment process.
- The **University of Portsmouth** follows the steps in the Equality Challenge Unit by appropriately wording the synopsis of courses, including diverse images in marketing materials and having a balanced teaching staff (40% of the teaching staff is female).

Other measures taken to help reduce the gender gap across FE and HE include: the organisation of conferences or talks to emphasise the role of women in cyber security (Anglia Ruskin University, Royal Holloway, Oxford Brooks University); outreach programmes for local schools to attract more female applicants (Exeter College, University of Kent, University of Hertfordshire); and the organisation of networking events (University of Oxford). At Royal Holloway, two female PhD students created the group WISDOM to raise the profile of female staff and students working and/or studying in the field of mathematics and information security.[120] WISDOM's main objective is to encourage more women into these disciplines and offer a strong support network.

> *"Some active promotion of the roles of women already enrolled and teaching on the course: through publicity materials and open days; encouraging women to apply; careful monitoring of data to ensure women's applications are evaluated fairly; gender balance in interview panels."*
>
> Higher Education representative

[120] Women in the Security Domain (and) Or Mathematics – Royal Holloway, University of London

Many of the university departments offering cyber security courses are members of the WISE group which campaigns for gender balance in science, engineering and technology. Some have also received the ATHENA bronze accreditation which recognises commitment to advancing the careers of women in science, technology, engineering, maths and medicine employment in higher education and research. It is unclear whether the universities that have obtained these accreditations actually have a more equal gender balance in cyber security courses than those that do not have the accreditations

> *"The university encourages gender diversity by attending Stemettes conferences; addressing gender in recruitment interviews and open days; as well as outreach to secondary schools."*
>
> Higher Education representative

The research for this study also suggests that the terminology and marketing material used to define cyber security courses and modules plays an important role in attracting – or deterring – potential cyber security students. In fact, other studies show that the 'militaristic/gendered' culture and language of cyber security alienates women who are considering entering the field.[121] As a result, women may struggle to imagine themselves working in this type of field and, therefore, fewer seek careers in it. A further factor is that due to cyber security being a predominantly male field, much of the vocabulary used to describe the industry tends to affect how these courses or activities are described (e.g. catch-the-flag or hackathon). There are interesting examples from outside the UK of hackathons being run exclusively for women, with appropriate branding. For example:

Box: 5.3: Examples of ways to brand hackathons

- **Hack the Patriarchy**: a hackathon for female programmers, developers, designers and other IT professional, held over two days in California. The event highlights the creative dimension rather than attacking cyber security systems.[122]
- **Athena Hacking**: taking the name of the Greek goddess, this event aims to support and nurture female professionals in California's technology sector. The emphasis is place on exploring technology, with the event described as a "gathering of curious minds to learn something new".[123]
- **The Girls in Tech Hackathon**: this event in Germany provides opportunities for girls aged 13-17 years to lean from female professionals in the IT industry.[124]
- **Anita's Moonshot Codeathon**: this event aims to "connect, inspire, and guide women in computing". It is open to females both with and without coding experience. Activities are focussed on solving real-life problems, such as building an application to help deaf people to communicate or directing citizens towards the nearest public transport stop and providing information about estimated waiting times. The event takes place online and is open to women across the world.[125]

As shown in the box, some FE and HE providers have attempted to change the branding of cyber security and related fields in their institutions by using different type of language to describe their cyber security course titles, descriptions and marketing materials. An example is Ada College, which is currently above the national level with 36% female starters in digital apprenticeships (according to the Tech Partnership, at the national level, 20% of digital apprenticeship starters are women). Careful use of language and images to highlight the creative and collaborative aspects of

[121] D'Hondt, K., e.t. al, 2016, Women in Cyber Security, Harvard Kennedy School
[122] Hack the Patriarchy
[123] Athena Hacking
[124] The Girls in Tech Hackathon
[125] Anita's Moonshot Codeathon

a career in the technology sector has had a positive effect in attracting more women into apprenticeships and courses.

At Ada College, students can opt for an apprenticeship in "Digital Innovation", which is a software developer apprenticeship standard at Levels 4 and 6 with some elements of cyber security. Instead of using the term 'software developer', the College labelled it differently because the title on its own is misleading and off-putting to women. The College wanted to go beyond the standard and bring out the innovative and creative aspects of software developers.

> *"There are many stereotypes that come with the term software development, so we decided to use the words 'digital innovation' because it appeals more to women."*
>
> Ada College representative

In order to decide what language to use on its marketing materials, the College conducted market tests to determine what type of language would appeal more to women. Reflecting results of the test, Ada College has developed a list of words it uses in its external communication and marketing material for its courses. Some examples of these words include: 'dynamic community', 'community', 'playfully challenging', 'digital thinker',' collective spirit', 'hands-on', 'power of collaboration', 'digital enlightenment', 'innovation', 'change-maker'.

Images are equally important to draw in female students and Ada College has sought to adopt a gender-sensitive approach. For example, it does not use images with a lone person sitting in front of a laptop to promote its apprenticeship and courses because it is seen as conveying the wrong message that a career in cyber security is a one-person job. Instead they show pictures of adults working in a team to bring out other types of skills. In order to appeal to girls, emphasising the collaborative, creative and active nature of cyber security has worked well for Ada College.

> *"We steer away from promoting activities that tend to appeal more to boys for our apprenticeship socials. We play up the collaborative side of the job because girls are interested in that – and it is also the reality of a job in the field."*
>
> Ada College representative

Another initiative to address the gender gap has been taken by the Open University, where each module undergoes a diversity and equality check. A module team is assigned to each module to check for equality and diversity issues. The team is supported by colleagues that are specialised in equality and diversity issues and provide them with advice and guidance to assess is a module has particular issues with equality and diversity. Equality and diversity issues are monitored on an annual basis by looking at the recruitment and performance of students. This includes comparing the performance of students from an equality and diversity perspective, including gender, ethnic origin and socio-economic status.

While the focus is on gender, other diversity indicators are also examined to understand if there are other underlying issues. Accessibility and support for students with disabilities is a major source of concern. When issues are identified, appropriate action is designed in consultation with the module team and specialised colleagues. In order to determine if a module has a positive or negative equality and diversity ratio, the University establishes norms in similar modules and agrees on improvement targets.

In addition to annual reviews, when modules are designed, they are reviewed by the University's Board of Studies. They are subject to further scrutiny by an academic member of staff charged with leading on equality and diversity issues across the school. This approach is used across the University's modules, including cyber security. As a result of the module teams' work, there have been changes to the design of module activities and language used to be more inclusive. This includes for example designing activities and using words that bring out confidence building in key skills, such as coding.

6 Overall Conclusions and Recommendations

6.1 Cyber security courses and the educational building blocks

Students are able to choose from a wide variety of cyber security modules and courses offered at both HE and FE levels in England. Many courses or modules are labelled as cyber security, whilst others may be titled differently or may include cyber security as part of a broader curriculum.

Taken together, there are an estimated 110 cyber security courses and a further 2,209 courses in computer science at the undergraduate and graduate levels in England (and a further 639 courses elsewhere in the UK) according to UCAS. Courses in cyber security are offered by a variety of university departments, such as Computer Science, Engineering, Social Sciences, Business and Law Schools at undergraduate, postgraduate and PhD levels. While postgraduate studies make up the majority of the cyber security programmes offered in England, there is an increase in provision of undergraduate level degrees. In most cases, students who pursue a degree or course in cyber security come from a STEM background (i.e. A Levels in Maths or Science). STEM qualities are desirable for these degrees because they help students develop a logical, systematic approach to reasoning and thinking. However, the multi-disciplinary nature of cyber security means a STEM background is not always a requirement and a number of non-STEM subjects can be combined with cyber security (e.g. data protection, psychology, business or law). Indeed, the research underlines the importance of overcoming the perception that cyber security is a primarily technical area of study and work.

The FE sector mainly offers a number of computer science or STEM courses. In a few cases, FE institutions offer courses that include cyber security modules, which provide the building blocks for further studies in the cyber security field at the HE level. There are 120 FE institutions that provide computer science courses in England, the main subject in FE that prepares students for further studies in cyber security. In 2016-17 a total of 47,417 students were undertaking class-based courses at FE institutions for a qualification in subjects that include cyber security aspects or which could help students to pursue further studies or work in this field.[126] The majority of FE students were studying for either a Diploma or an A Level qualification (45.3% and 25.1% respectively).[127]

Few FE courses are specialised in cyber security at Levels 2 and 3 because institutions need to provide more general courses in computer science or digital skills. As such, there are relatively few FE institutions that provide courses purely in cyber security. However, FE students can take cyber security modules or specialise in cyber security at a later stage through a degree course or degree apprenticeship. Students who want to specialised in cyber security usually have to take a more general course in computer science with a cyber security module, unless they are enrolled in a technology college. Very few students go straight from an FE institution into a full-time entry-level cyber security-related job.

The FE sector offers apprenticeships with a cyber security element and degree apprenticeships in cyber security are now offered by several universities. There is currently a degree apprenticeship standard available at BSc level within the field of cyber security, whilst the BSc and MSc degree apprenticeships in Digital and Technology Solutions include modules in cyber security. Since degree apprenticeships were only introduced in September 2015, it is too early to assess their effectiveness in helping address the shortage of cyber security professionals. However, several major employers already offer degree apprenticeship positions, including GCHQ, BT, IBM and PwC,

[126] Source: Association of Colleges. The research did not look into online courses.

[127] Department for Education, 2016, Adult Further Education Outcome-based Success Measures

which suggests that they are an attractive option for employers and apprentices alike. However, it is still too early to see how attractive the apprenticeships are to employers after they conclude their studies.

At the HE level, courses are either labelled as cyber security or labelled as cyber security combined with a STEM or a non-STEM specialism. As such, students can choose a technical STEM route or a non-STEM route into cyber security. There currently are limited options for individuals who wish to learn about cyber security, but do not have the right background. In most cases, students that undertake cyber security courses have a STEM background. At MSc level, courses in cyber security are often, but not always, required to hold a first degree in computer science (or in a related field). This suggests a general inclination (at undergraduate and postgraduate levels) towards the more technical nature of cyber security (a conclusion also supported by the HESA data). The qualities that are desirable for technical degrees include knowledge of Science, Mathematics and/or Computing. It is important to note that due to the highly technical nature of cyber security, a degree in a STEM-related subject with cyber security is not enough to develop all the skills and knowledge required for a technical cyber security entry-level job.

According to an analysis of HESA data, a total of 15,356 students graduated from an HE institution with a degree in a cyber security-related field in England over the past three academic years.[128] Of these students, 10,384 were undergraduates and 4,914 were postgraduates. There has been a 22% increase in the number of postgraduates and a 31% increase in the number of undergraduates in the past three years. During this period, the percentage of UK students graduating from a HE institution with a degree in a cyber security related field in England amounted to 80% of the total, with 5% from the EU and 15% from outside the EU. The percentage of students from the UK has increased, the percentage from the EU has been stable and the percent from outside the EU has dropped in this period. The research also found that there is a strong preference by students for NCSC-certified courses.

There is anecdotal evidence that some FE and HE institutions face difficulties in attracting lecturers and researchers with expertise in cyber security. More evidence is needed to understand the scale of this problem and the extent to which it affects learning. There is a risk that skilled lecturers are poached by higher-ranked universities or industry. A lack of trained staff in cyber security exists more generally across many FE and HE institutions. This makes it difficult to keep up with new technological developments in the cyber security field. In addition, a large number of institutions work with outdated software and computer laboratories, which hinder the cyber security skills development of students and reduce their student recruitment potential. This is particularly the case at FE institutions.

[128] These include generalist computer science courses with a module or specialism in cyber security; cyber security generalist or specialist courses (e.g. cybernetics, digital forensics)); STEM subjects with a module or specialism in cyber security; or non-technical courses with a cyber security module or specialism, such as management, business studies or psychology.

Box: 6.1: Recommendations - Cyber Security Courses and the Educational Building Blocks

Recommendation 1: FE and HE institutions should expand the provision of cyber security modules within degree programmes other than cyber security or computer science. The research has shown that employers are willing to recruit graduates with a degree in other subjects into entry-level roles in cyber security provided that they have basic knowledge in cyber security. Increasing the provision of such modules would make such students more aware of and interested in the possibility of a career in cyber security and would help prepare them for an entry-level role (notwithstanding the need for employers to train most new recruits; see Section 6.2 below). This could include FE and HE pooling resources, for example sharing expertise and modules.

Recommendation 2: FE and HE institutions should increase the provision of non-technical modules and courses in cyber security. This would be both within cyber security, computer science or STEM degrees and within other subjects. The research has highlighted the growth in entry-level roles that are non-technical in nature and also the need for many cyber security professionals in technical roles to have knowledge of non-technical areas (e.g. ethics, law, psychology). Expanding the provision of modules and courses covering the non-technical aspects of cyber security would give those entering technical roles a more rounded knowledge. It would also make students more aware of, more interested in and better prepared for non-technical roles in cyber security (including those studying subjects other than cyber security or computer science).

Recommendation 3: Greater encouragement should be given to increasing the diversity of methods used to deliver cyber security courses for HE and FE to address. In particular, there is scope to increase the provision of courses that are delivered on-line, either for independent learners or for students supervised by a school, FE institution or HE institution. Such courses offer the potential to reach a larger number of students and thus lower the average cost per student. This is likely to be particularly beneficial for students or education providers in rural areas or outside the big cities, where provision might otherwise not be economically viable.

Recommendation 4: A review of the Cyber Security degree apprenticeship and the Digital and Technology Solution Specialist degree apprenticeship should be undertaken in 2-3 years' time. The research suggests that this way of developing cyber security skills has many potential attractions. However, experience is limited. Moreover, there are currently no standards in non-technical areas. A review of Degree Apprenticeships and data collected undertaken a year or two after the first cohorts of apprentices will have graduated could provide evidence regarding the extent to which degree apprenticeships provide a flow of skilled and experienced graduates who continue within cyber security roles. Such a review would build on the findings of the current review of the Digital & Technology Solutions Professional degree apprenticeship. Currently a statutory review is taking place of the Cyber Technologist and Cyber Analyst Level 4.[129]

6.2 Pathways to cyber security jobs

There are various pathways into an entry-level cyber security job. The study has focused on the main pathways via FE and HE.

There is a diversity of overlapping and inter-linked pathways through FE and HE into entry-level jobs in cyber security. Whilst this study has highlighted six main pathways, these should not be seen as discrete 'tracks' leading from specific courses to specific jobs. Instead, at least within the degree pathways, it is often the case that a degree with good grades, and a certain level of technical expertise, can open up many, perhaps most, entry-level jobs in cyber security. The majority of students from the FE sector go on to pursue a degree in cyber security or a related field, while a relatively small proportion of FE students undertake a higher apprenticeship after their A Levels (Pathway A). The apprenticeship route involves a range of technical apprenticeships which can lead to an entry-level job in cyber security. The most common pathway is to study for a

[129] Institute for Apprenticeships, 2018, Apprenticeship Standards Statutory Review

BSc in Computer Science with a cyber security module, a BSc specifically in cyber security or combining a BSc in another STEM degree with cyber security (Pathway B).

A number of entry-level jobs in the cyber security field are also taken by graduates who have non-STEM degrees (e.g. Criminology, History, Law, Psychology, International Relations) (Pathway C). Students going through Pathways B and C may study for a specialised Master's degree or PhD in cyber security if this was not their BSc speciality. Alternatively, they may choose to pursue a more specialised course/field of research (Pathway D). In all cases, further in-house training by the organisations that graduates join is likely to be needed to develop specialist cyber security knowledge and skills. Another possibility is that some people who have already entered the workforce decide on a change in direction in their career, which can involve an entry-level job in cyber security (Pathway E). Individuals across all pathways could also choose to set up their own business or to operate as freelance professionals; however, the need to have up-to-date knowledge would tend to limit the numbers doing so.

Employers largely accept that they will need to train new recruits and therefore more often seek "rounded" candidates with a mix of technical expertise and, crucially, the ability to adapt and learn new skills. Many, perhaps most, employers are therefore open to holders of any degrees (albeit with a preference for STEM degrees) rather than cyber security degrees specifically. Indeed, some employers argue that graduates in very technical subjects are more likely to lack the wider skillset required for a job in cyber security. The adverts for some entry-level jobs do not specify a formal requirement to have a qualification, which creates the possibility for other pathways outside of FE and HE (e.g. those who have developed technical skills through cyber security as a hobby).

Another driver of the diversity of pathways is the fact that an increasing number of cyber security jobs are of a non-technical nature and/or require non-technical skills. Such jobs might relate to the managerial, legal, ethical, human or psychological dimensions of cyber security. For this reason, it is becoming increasingly common for graduates in non-STEM fields to take up cyber security jobs, which again means a diversification of the pathways.

Whilst the UK produces some 250,000 STEM graduates each year,[130] the proportion of such graduates entering cyber security is small. Indeed, the shortage of recruits into cyber security roles is aggravated by high competition from other sectors (e.g. financial services) for suitable graduates, including those with computer science or STEM degrees. The same phenomenon also affects other professions, such as engineering, with many engineering graduates entering non-engineering jobs. Of those studying on cyber security courses, only around two-thirds progressed into a role in cyber security or in IT in general between 2014 and 2017, with the rest going into management or other jobs (including 11% taking a non-graduate job).[131] This suggests a need to not only increase the number of students taking such courses, but also to increase the links to employers and the (perceived) attractiveness of cyber security roles.

The number of students taking Master's programmes in cyber security has been growing but a significant proportion of those students do not then enter cyber security jobs upon graduation.

[130] HESA, 2018, What do HE Students Study?

[131] Source: Higher Education Statistics Agency.

Box: 6.2: Recommendations - Pathways to Cyber Security Jobs

Recommendation 5: There is a need to define entry-level cyber security roles and pathways more clearly. Government, industry and other initiatives to promote cyber security (e.g. CyberFirst, Cyber Discovery, entry-level positions into an organisation, apprenticeships) should be encouraged or required to publicise more explicitly the various pathways through FE and/or HE into a career in cyber security, particularly for technical but also for non-technical careers. Such initiatives play an important role in promoting an interest in cyber security and in supporting the acquisition of skills and experience by students and school children, e.g. through competitions or the provision of accessible online material. Their role could be expanded to include providing advice to schools and school children regarding routes through FE or HE, and to FE or HE students regarding how best to enter particular careers.

Recommendation 6: There is a need to increase students' awareness of the possibilities for career progression and further pathways after taking up an entry-level job in cyber security. This can be done through careers advice and a joint effort of Government, academia and industry to help achieve this. Further to this, efforts are needed to de-mystify what a career in cyber security actually is and to emphasis the diversity of skills that are needed in the field. In part, this should also involve overcoming negative perceptions of roles in cyber security (e.g. about them being very narrow, technical roles). There is also a need to promote cyber security as being more like a "profession" in its own right which offers opportunities to progress in a structured way into a range of senior management roles. Government should continue efforts in this space.

Recommendation 7: There is a need for (new or existing) initiatives (whether sponsored by government, industry or other stakeholders) to promote the diversity of technical and non-technical careers in cyber security more widely. There is a widespread perception that it is necessary to study computer sciences or a STEM subject to have a career in cyber security and more should be done to raise awareness of non-technical careers to all graduates, including those from non-STEM subjects.

6.3 How cyber security courses are developed and industry's role

The study identifies many different ways in which industry is involved in helping to develop cyber security skills. It underlines the importance of such collaboration in ensuring that those graduating from FE and HE institutions have the skills needed by employers.

Cyber security courses have evolved in most cases from existing computer sciences (or similar) courses, initially as a module and then developing in some cases as a separate course in its own right. The decision by FE and HE providers to introduce a course or module (or not) is driven by a combination of factors – evidence of demand and the capacity to deliver courses being perhaps the most important considerations.

Collaboration between the public sector, industry and academia on cyber security is widely seen as crucial in designing high quality courses as well as promoting the transition of workers from other roles into cyber security. The nature of industry involvement ranges from being closely involved in delivering modules and certification, providing placements or participating in apprenticeship schemes, industry seminars, careers events to simply recruiting cyber security graduates. There are various factors that explain the nature of the relationship between industry and FE and HE providers. Cyber security courses and modules are developed by academic institutions with varying degrees of industry input. In that context, industry certification can be highly valued by students and employers alike.

Despite a generally positive situation, there are some mismatches and conflicting perceptions between industry and FE and HE sectors. Some employers argue that academic courses do not reflect what the latest developments in cyber security and that students do not leave courses with the sorts of skills that companies need. Equally, FE and HE providers sometimes argue that employers have unrealistic expectations of what students can learn on a course. The development

of part-time MScs and of Degree Apprenticeships in cyber security are strengthening the links between industry and universities by making it possible for students to combine study with work experience.

Box: 6.3: Recommendations - How cyber security courses are developed and industry's role

Recommendation 8: Although the research did not explore the quality of FE and HE cyber security courses linked to employer engagement, a number of benefits were identified that can arise from such involvement, including skills needs mapping and career engagement. Therefore, action could look to be taken both locally and at national level to ensure employers are involved in the design and delivery of cyber security courses. As the study highlights, there are various factors including geography and proximity to industry that determine the relationship with FE and HE institutions. At a national level, the further development of Degree Apprenticeships should help to strengthen this relationship. There is scope in this regard to replicate some of the sectoral initiatives across the wider economy. A stronger framework at a national level to promote links between industry and academia would also be helpful (possibly based on an expansion of the CyberInvest initiative).[132] Within this overall framework, particular attention should be paid to encouraging smaller firms to become engaged in developing cyber security skills. This would be helpful in creating employment links for industry with FE and HE.

Recommendation 9: Cyber security should be promoted as a distinct profession in its own right. This will require the Government, the FE and HE sector, and industry to work together to reach agreement on the definition of standardised roles and skills clusters, certification criteria, professional development routes and other aspects. Businesses should help to ensure there is a shared vocabulary to describe the skills they need that are recognised by potential job applicants. New entrants should be clearer on the skills they need and the importance of professional development. At present there is a rather confusing array of industrial certification systems and there is scope for these to be rationalised.

Recommendation 10: Government policies and programmes in the cyber security skills area should be made more visible, particularly amongst HE and FE students and other potential recruits into entry-level roles. Developing a complete roadmap of which projects are being funded by different parts of government could help to improve the connections between and visibility of such initiatives.

6.4 Gender balance in cyber security

The study confirms that the gender imbalance continues to be a significant problem in the cyber security educational building blocks.

The research confirms that the gender gap remains significant in cyber security courses and modules. According to an analysis of AoC and HESA data, in 2016-17, only 16% of students undertaking FE and HE cyber security courses or courses with a cyber security module were female. This is very similar to the situation across STEM subjects more generally.

Despite national efforts to encourage more female students into cyber security, preconceived notions and ideas continue to affect the number of female students applying for cyber security courses or modules. The field of cyber security is still dominated by stereotypes and is widely perceived as a male-dominant field. As a result, female students do not perceive cyber security as a viable career path and see the field as being too 'geeky' and/or oriented to males. The lack of role female models in this predominantly male field also affects the number of prospective female students. The research established that many FE and HE providers have taken steps to tackle this gender imbalance problem. This includes: holding conferences or talks to emphasise the role of

[132] CyberInvest is a community of industry, Government and academia, which seeks to enhance collaboration and coherence in cyber security research within UK universities.

women in cyber security, the provision of outreach to local schools to attract more female applicants, and networking events.

More generally, female students or potential students are often not aware of the opportunities in the cyber security field. One HE representative who contributed to the study claimed that 'cyber security is an easy sell' but the issue is in the way in which this information is delivered to young women. Women have opportunities to enter the cyber security field, particularly since there are increasing numbers of jobs openings. They are, however, not well informed on what cyber security is really about and the skills that are needed to enter the field.

The challenge is to attract the interest of young women who are not naturally drawn to cyber security. The key is to raise awareness amongst girls of the attractions of a career in technology and cyber security while they are still at school. The same can be said across most STEM subjects. It is well known that the interest of women to pursue a STEM subject drops after they complete their A Level. This suggests more needs to be done to retain female interest in the field before and beyond their A Levels across all STEM subjects. Recruiters need to be sensitive to gender issues in the way they spread the image of cyber security in their recruitment policies and materials. The same argument applies to the way in which FE and HE providers promote cyber security courses. A more inclusive or neutral way of branding cyber security will appeal not only to more women, but to a wider pool of students in other subject areas as well.

The findings from the interview and survey programmes suggest that the terminology used to define cyber security courses and modules plays an important role in attracting (or deterring) cyber security students. In fact, other studies show that what is sometimes seen as the 'militaristic/gendered' culture and language of cyber security alienates women considering a career in field. A small number of establishments have adjusted the way in which they brand and advertise cyber security courses or apprenticeships to attract more female candidates.

The relatively small number of females studying cyber security of course adversely affects the flow of female graduates into entry-level jobs in the cyber security field. In general, employers receive few job applications from female candidates which means that they struggle to have gender diverse teams working within their cyber security departments. Some of the gender-related issues in cyber security can also be applied more generally to STEM subjects and have their origins in the attitudes and perceptions female pupils develop at an early age.

Box: 6.4: Recommendations – Gender balance in cyber security

Recommendation 11: Initiatives to promote cyber security (whether sponsored by government, industry or other stakeholders) should provide more programmes and competitions specifically targeted at female school pupils. This should specifically include a focus on pupils that have not yet made their GCSE choices, i.e. Year 9 or below. In that respect, the activities of CyberFirst provide a positive example from which other initiatives can learn. Many studies highlight that the origins of the gender imbalance in cyber security lie at school when pupils form their attitudes towards different subjects. The difficulty of attracting female students into STEM generally has similar origins. More should be done therefore to draw in female students that do not have a natural inclination to computing by introducing the subject while they are still at school. Taking a lead from the CyberFirst Girls Competition, other organisations could look to organise activities specifically to encourage female students.

Recommendation 12: Good practices in addressing the gender imbalance across FE and HE should be better publicised so that measures can be replicated more widely. As the report highlights, there are a number of examples of initiatives to encourage female students to study cyber security. But there seems to be less emphasis on sharing good practice and experience**.** There are different ways this can be done: for example, developing online guides sharing good practice and case studies; mentor programmes and guest speakers; female role models; or setting up fora and organising workshops so that FE and HE representatives can meet and share experiences on how best to address gender imbalance issues in their respective institutions.

Recommendation 13: Greater publicity should be given to successful female leaders and professionals in the cyber security field in order to inspire more women to undertake HE and FE courses relevant to cyber security and to consider careers in cyber security. A career in cyber security should be further promoted so young female students can explore the wide range of opportunities (i.e. mentor programmes and guest speakers). This should be considered by industry (e.g. when advertising jobs), HE and FE institutions and Government.

Recommendation 14: FE and HE institutions should do more to ensure that appropriate language is used to describe cyber security courses and modules so that they appeal to women and to a more diverse audience in general. Adapting course titles and module descriptions to attract potential female students and students from diverse backgrounds is a key to broadening the supply of skilled graduates into the field. Extra-curricular activities organised by companies, the government or education institutions should use inclusive language to draw in a diverse pool of candidates. Language for these events or activities should emphases group work and problem solving, as opposed to using military or masculine connotations.

Overall, this study suggests that although the provision of Further and Higher Education courses and modules in cyber security is increasing in England, there is still insufficient provision to meet demand. With the cyber security threat growing, action by Government, industry and academia is needed to address this problem and this report has set out a number of priorities in this regard.

Appendix A: Examples of Professional Accreditation by Institution and/or Organisation

University / Level	Professional Accreditation
Greenwich University (MSc)	Upon completion of the programme, students can achieve an additional qualification after taking the Systems Security Certifies Practitioner exam within six months of graduating.
University of Derby (MSc)	Students can prepare for the BSI ISO 27001 lead auditor certifications
University of Bradford (MSc)	There is the opportunity to gain additional qualifications in Certified ISO/IEC 27001 Lead Implementer and CEH v8 Ethical Hacking.
London Metropolitan University (MSc)	Students can gain CISCO accreditation
University of Suffolk (BSc)	Course includes preparation for the certification exams for (ISC)²'s Certified Secure Software Lifecycle Professional (CSSLP) and Certified Information Systems Security Professional (CISSP) qualifications
University of Central Lancashire (BSc)	Completion of the course leads to partial CEng accreditation from the British Computing Society

Appendix B: List of References

Anita's Moonshot Codeathon

Association of Colleges

Athena Hacking

Cabinet Office, 2016, National Cyber Security Strategy 2016 to 2021

Cambridge Assessment, 2007, AS and A Level Choice – Gender Makes a Difference

Centre for Cyber Safety and Education, ISC^2, 2017, Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk, A Frost & Sullivan Executive Briefing

Centre for Cyber Safety and Education, ISC^2, 2018, Innovation Through Inclusion: The Multicultural Cyber Security Workforce, A Frost & Sullivan White Paper

Centre for Cyber Safety and Education, ISC^2, Executive Women's Forum, 2017, The 2017 Global Information Security Workforce Study: Women in Cyber Security – A Frost & Sullivan White Paper

Centre for Strategic and International Studies, 2016, Hacking the Skills Shortage, McAfee.

CISCO, 2014, Annual Security Report

CISCO, 2018, Annual Security Report

CREST, 2017, Closing the Gender Gap in Cyber Security

CV Library

Cyber Security Challenge UK, 2018, Women in Cyber Security

Cyber Security Curricular Guidelines – CSEC 2017

CyberDiscovery

CyberFirst

CyberFirst – Girls Competition

CyBOK (The Cyber Security Body of Knowledge)

D'Hondt, K., e.t. al, 2016, Women in Cyber Security, Harvard Kennedy School

Department for Business Innovation & Skills, 2014, Understanding the Link Between Employers and Schools and the Role of the National Careers Service

Department for Business, Innovation and Skills, 2015, Government Rolls-Out Flagship Degree Apprenticeship

Department for Digital, Culture, Media and Sport, 2017, Policy Paper, A Safe and Secure Cyberspace – Making the UK the Safest Place in the World to Live and Work Online

Department for Digital, Culture, Media and Sport, 2018, Cyber Security Breaches Survey

Department for Education, 2016, Adult Further Education Outcome-based Success Measures

Department for Education, 2017, Number of applications to apprenticeship vacancies

Department for Education, 2018, Apprenticeship and levy statistics

Department for Education, 2018, New T Levels Mark a Revolution in Technical Education

e-skills.uk, 2013, Careers Analysis Into Cyber Security: New & Evolving Occupations

e-Skills.uk, 2014, The Women in IT Scoreboard, British Computer Society

Education & Skills Funding Agency, 2018, Providers Selected to Deliver T Levels in Academic Year 2020 to 2021

European Union Agency for Network and Information Security, 2014, Roadmap for NIS Education Programmes in Europe

Facebook Newsroom, 2018, Training 1 Million People and Small Businesses in Europe by 2020

Federation for Small Businesses, 2016, Cyber Resilience: How to Protect Small Firms in the Digital Economy

Forbes, 2018, Why so Few Women Work in Cyber Security (and how we can change it)

Fullfact, 2017, How many international students leave after studying in the UK?
Get In Go Far, 2018, About Apprenticeships
Glassdoor
Gov.uk, 2018, Further Education Courses and Funding
Gov.uk, 2018, General Work Visa (Tier 2)
Gov.uk, 2018, What Qualification Levels Mean
Hack the Patriarchy
HESA, 2018, What do HE Students Study?
Higher Education Statistics Agency
HM Government, 2014, Cyber Security Skills: A Guide for Business
Home Office, 2018, Register of Sponsors Licensed Under the Points-based system
Hotcourses, 2018, IT (Networking and Cyber Security) – Level 3 Extended Diploma (Full-Time)
House of Commons, 2016, Digital Skills Crisis – Second Report of Session 2016-17
IAAC, 2017, The Profession - Understanding Careers and Professionalism in Cyber Security
IISP, 2018, The Cyber and Information Security Profession in 2017/2018
Indeed
Indeed Blog, 2017, Indeed Spotlight: The Global Cyber Security Skills Gap
Institute for Apprenticeships, 2018, Apprenticeship Standards Statutory Review
Institute of Coding
ISACA, 2015, Global Cyber Security Status Report – UK data
ISC^2, 2018, Cyber Security Professionals Focus on Developing New Skills as Workforce Gap Widens
ISC^2, 2018, Exam Pricing
ISC^2, 2018, Our vision
IT Governance, 2018, What is Cyber Security?
Janeja, V., e.t. al, 2018, Enhancing Interest in Cyber Security Careers: A Peer Mentoring Perspective
Jethwani, M., e.t. al, 2016, "I Can Actually be a Super Sleuth" – Promising Practices for Engaging Adolescent Girls in Cyber Security Education
Kaspersky Lab, 2017, Beyond 11% - A Study into Why Women Are Not Entering Cyber Security
Konfer
National Cyber Security Centre, 2018, 4,500 Young Women Race to Complete CyberFirst Girls Online Challenge
National Cyber Security Centre, 2018, NCSC-certified degrees
National Institute of Standards and Technology, U.S Department of Commerce, 2017, National Initiative for Cyber Security Education (NICE) – Cyber Security Workforce Framework
Prospects, 2018, Cyber Security and Management, the University of Warwick
Pearson, 2018, BTEC Level 2 Technicals – Digital Technology
Pedley, D., McHenry, D., Motha, H., Shah, J., 2018, Understanding the UK Cyber Security Skills Labour Market, Ipsos MORI
Qufaro, 2018, Bletchley Park Qufaro and GK Apprenticeships Work in Partnership to Deliver Cyber Security Apprenticeships
Qufaro, 2018, Extended Project Qualification in Cyber Security
Shadbolt, 2016, Shadbolt Review of Computer Sciences Degree Accreditation and Graduate Employability
South & City College Birmingham, 2018, Computing and Cyber Security Level 3
STEM Ambassadors
Symantec, 2018, Internet Security Threat Report

Target Jobs, 2018, Cyber Security Specialist: Job Description

Tech Partnership, 2018, Tech Partnership Legacy

The Careers and Enterprise Company

The Girls in Tech Hackathon

UCAS, 2018, A Levels

UCAS, 2018, Degree Apprenticeships

UCAS, 2018, Thinking About Uni?

University of Plymouth, 2018, Employer Engagement Opportunities

Women in Science, Technology, Engineering and Maths, 2014, The talent pipeline from classroom to boardroom

Women in Science, Technology, Engineering and Maths, 2018, Industry-Led Ten Steps

Women in the Security Domain (and) Or Mathematics – Royal Holloway, University of London

Zahout, M., 2017, Women in Cyber Security, McCloy Fellowship on Global Trends

Appendix C: Survey questions

1. Please confirm that you have read and understood the statement on how your personal data will be processed in accordance with the rights of data subjects under Data Protection Act (2018).
2. Please state the name of your institution:
3. Please tick the box that best describes your institution: Higher Education; Further Education; Other.
4. If you are a Further Education institution, do you provide: Level 3 courses, Level 4 courses or Level 5 courses in cyber security?
5. Please state your role within your institution:
6. Do you offer cyber security courses?
The following questions were for those who answered "yes" to Q.6[133]:
7. Are all available places for the current academic year filled in your cyber security course(s)?
8. Do you think that since 2014 demand for places to study cyber security has increased, decreased, or remained about the same?
9. Please provide an estimate of the number of students; the percentage of female students; the percentage of overseas students at Level 3, Level 4 or Level 5/ BSc or MSc level.
10. What percentage of your cyber security course is purely technical at BSc level?
11. What percentage of your cyber security course is purely technical at MSc level?
12. Are students enrolled in cyber security courses required to develop other transferable skills, such as teamwork; problem solving skills; communication skills; other.
13. Are there any courses available to students that have a cyber security module/component in other Departments, such as Computer Science; Engineering; Psychology; Law; Business studies; none?
14. Do your cyber security courses offer any form of accreditation?
15. In your view, have these accreditations had an impact on employability?
The following questions were for those who answered "no" to Q.6[134]:
16. If you do not offer a cyber security course, what is the reason for this?
17. Do you plan to add a cyber security course in the next 3 years?
18. What courses are currently available to students that have a cyber security module/component (options: Computer Science; Engineering; Psychology; Law; Business studies; none)
19. Are students enrolled in these courses (with a cyber security module/component) required to develop other transferable skills, such as teamwork; problem solving skills; communication skills; other.
20. At which level of qualification do you offer courses with a cyber security module?
Gender balance
21. How many students on your cyber security course(s) identify as women?
22. If there are fewer than 50% that identify as women in cyber security courses, what is the reason for this gender imbalance in your view?
23. What do you estimate is the gender balance amongst students on courses that have a cyber security module/component?
24. If there are fewer than 50% women on the courses with a cyber security component/module, what is the reason for this gender imbalance?
25. What steps (if any) have you taken to promote the participation of women in cyber security

[133] Questions were tailored depending on if respondent was from FE/HE institutions.

[134] Questions were tailored depending on if respondent was from FE/HE institutions.

or other courses with a cyber security component/module?
26. What steps have proved effective in promoting the participation of women in cyber security or courses that have a cyber security module/component?
27. Please comment on any other reasons for low female participation in cyber security courses and/or steps that might be taken to rectify this situation.
Career pathways
28. What do you estimate is the percentage of UK nationals studying cyber security within your institution?
29. Among your graduates in cyber security remaining in the UK, approximately what percentage of your students went into jobs in this field last year?
30. Among students that completed a cyber security course, what do they go on to do? (If you have any destination data, could you please share - e.g. percentages going into further study, percentage that get a job, or those unemployed)
31. How well aware are student of cyber security pathways that are open to them?
32. How easy is it for a student to obtain an entry-level job in cyber security?
33. Do you offer support to your students to help them enter cyber security occupations?
34. In your view, what are the three most important skills that employers are looking for in applicants for entry-level cyber security jobs? On what basis do you make this judgement?
35. What methods have proved most effective in facilitating students' entry into cyber security occupations?
36. To what extent do the following constitute barriers to students obtaining cyber security job: Students' own perceptions and attitudes; Influence of parental/guardians' perceptions and attitudes; Peer network/friend perceptions and attitudes; Employers' attitudes and requirements; Limited soft skills (i.e. people skills, social skills, communication skills); other/don't know.
37. In your view, do employers do enough to attract students to apply for jobs in cyber security?
38. To what extent is there a difference between the public and private sectors with regard to cyber security career pathways?
39. Please use the space below to comment on any other barriers to entry into cyber security jobs that your students face.
Development of cyber security modules
40. In what ways are employers or industry bodies involved in developing your cyber security courses and modules?
41. Are your cyber security courses/modules certified by: cyber security employer; industry bodies; other.
42. Could employers or industry bodies do more to help develop or deliver cyber security courses (in general across the FE/HE sector)?
43. Do you have any thoughts on what more can be done by the FE and HE sector to develop the provision of cyber security training?
44. Is there anything more that government or industry could do to support the development of cyber security skills?
45. Would you be willing to provide further inputs to the study? (e.g. a telephone interview to help clarify answers to the survey)