ESCALATE

Stirling, Scotland

"A digital Skills Escalator for Cyber Security in Stirling, Scotland"

Evidence Base for a Skills Escalator – Cyber Security (Work Package 4)

Author: Elaine Robinson, Ronald McQuaid, Aleksandra Webb, William Webster,

MWO, Stirling Management School University of Stirling UK

Date of Release: 30-08-2021

Contents

List of Abbreviations

ACE-CSR	Academic Centres of Excellence in Cyber Security Research
CSIIF	Cyber Skills Immediate Impact Fund
DCMS	The Department for Digital, Culture, Media & Sport
DESI	European Digital Economy and Society Index
ESCALATE	Coordinated Higher Institutions Responses to Digitalisation, Erasmus+ KA2 - Cooperation for innovation and the exchange of good practices, KA203 - Strategic Partnerships for higher education
EPSRC	Engineering and Physical Sciences Research Council
EU	European Union
GCHQ	Government Communications Headquarters
HEI	Higher Education Institution
HNC	Higher National Certificate
HND	Higher National Diploma
ICT	Information and Communications Technology
LM	Labour Market
NCSC	National Cyber Security Centre
NPA	National Progression Award
SICSA	Scottish Informatics and Computer Science Alliance
SME	Small and Medium-sized Enterprise
SQA	Scottish Qualifications Authority
STUC	Scottish Trades Union Congress
WP	Work Package

Useful Definitions[1]:

Digital Skills: Competences in and/or knowledge of IT tools including computer programs and programming languages.

Digitisation / Digitalisation of Jobs: increasing incorporation of artificial intelligence and automated systems into jobs, including resulting changes in skills and job automation by means of computer-controlled equipment.

Baseline Digital Skills: Digital literacy skills that employers ask for in the vast majority of jobs across all sectors in the UK labour market. Includes spreadsheet and word processing tools like Microsoft Excel and Microsoft Word, as well as enterprise management software like Oracle or SAP. These proficiencies are increasingly becoming a basic skill requirement for a majority of occupations.

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/807830/No_Longer_Optional_Employer_Demand_for_Digital_Skills.pdf

Executive Summary

The global cyber security workforce is a fast-growing area of well-paid jobs (salaries £22-90,000 in Scotland), with an estimated required growth of around 89% in the next few years ((ISC)2 Cybersecurity Workforce Study, 2020). In Europe alone the shortage is 168,000 with similar shortages and high growth requirements likely in the UK, Scotland. This is a fast changing sector with hackers and criminals constantly raising new and often innovative problems, suggesting a need for a flexible approach to staffing, education and a flexible skills development pipeline throughout the Cyber security sector.

The Stirling area in central Scotland is the main focus of this report, which is highly embedded and interconnected with the rest of Scotland. Hence what happens in the Stirling area is greatly influenced by the Scottish context and policies, as well as UK industry and organisations and Scottish and UK central governments. Stirling is well-suited to the development in cyber security training and employment, due to the large number of skilled graduates from HEIs in the area, as well as several employers in the field, both within Stirling itself, and the neighbouring cities of Glasgow and Edinburgh. It is not a complete census of related training or firms.

This report illustrates a 'Proof of Concept' of the potential use of a Digital Skills Escalator, particularly in relation to cyber security, focusing on the Stirling region in central Scotland. **The Digital Escalator is a concept that refers to a pipeline of skills (or more accurately a 'funnel of skills' from basic to highly specialised expert levels) linked to a specific smart specialisation sector, represented by a multi-level skills map where people can join or complete their skills journey at different stages.**

The Escalator Model is not intended to be a fixed journey from school to Higher Education and Continuing Professional Development (CPD) but instead is designed for people to enter and leave along its path when necessary. Its purpose is to promote discussion, engagement and coordinated partnership activity. While its focus is on formal training and education, it also incorporates work and other experience and informal learning.

The research included desk-based research and 8 interviews with public and private bodies and trades unions.

General recommendations for actions to help fill in the digital skills and cyber security skills gap include:

1. Increased investment in school staff and equipment, as well as focussing on helping more graduates go into computer science and cyber security teaching, and improving the curriculum were recommended by more than one of the interviewees. Providing a safe technological and educational environment for developing cyber security skills, for example shared specialist software and hardware in the area of training on ethical hacking, is essential for students at all levels of education.
2. Greater employer involvement with schools, including expanding the National Progression Award courses, and encouraging children and parents to see computing science and cyber security as a viable career choice, will help to cement the school as playing a foundational role for young people.
3. Increasing the employability of college and university graduates is important, particularly by addressing the digital skills gap, and especially for students with little previous exposure in this area and those from disadvantaged backgrounds. Training facilities such as dedicated tech centres and bootcamp courses for college and HE students to learn relevant coding languages could be co-funded or co-supplied by employers. Students could be offered

placements at local organisations which would strengthen the links between businesses, FEs and HEIs as well as provide a fresh talent pool for employers.

4. Investing in colleges through increasing the number of applied or practically-oriented courses, as well as apprenticeships and workplace-based learning models (similar to Graduate Apprenticeships co-delivered by colleges/universities and host organisations/ employers). In addition, better conversion pathways for continuing education in the cyber security specialism should be collectively developed by FE sand HEIs.
5. Increasing investment in the provision of workplace training, funded or co-funded by employers, unions, and the government, to ensure a basic level of cyber security and digital skills, as well as opportunities for specialist skills development and potential pathways for career changes for existing workforce. In particular, digital skills and cyber-security focused work-based training organised and championed by employers and unions needs further and continuous support to bridge the skill gaps across the workforce and offer new career opportunities for workers across economic sectors. For example, a union learning fund could include a cyber security skills element in relevant projects in Scotland.

This report provides an indicative summary of the potential pathways to digital skills development in the current skills system in Scotland, from the lowest to the highest qualification level courses. It focuses on formal education qualifications, but fully recognises the importance of actual on the job learning and professional courses, experiential learning, and mentoring.

This report now presents: a background to the ESCALATE Project; the concept of a Skills Escalator; the context of cyber security in Stirling and Scotland; *the digital Skills Escalator for cyber security in Stirling*; aligned Investments; and skills priorities and recommendations.

Methodology

Cyber security skills development provision in the Stirling region (municipal area) was mapped out through a combination of online desk research and interviews conducted with various stakeholders across Scotland. Stakeholder relationships were built through existing networks, snowballing, and desk research considering key policy initiatives and mapping the landscape of stakeholders. The research included 8 interviews with public and private bodies and trades unions. The cyber security Escalator was built by consolidating the information found from the desk research and the information gained through the stakeholder interviews.

The cyber security sector was chosen due to its growing importance and rapid changes for specialist firms and organisations across the region, its importance for Scotland's economy going forward, and its relevance to HEIs in particular due to their outward facing, collaborative nature. The choice was informed by previous experience and links to organisations among the team and following desk research, including the recent related strategies among Scottish organisations (including the Scottish Government and Skills Development Scotland).[2]

The work will be taken forward by liaising and sharing information with relationships built during the interview phase.

Escalator partners

The interviewees were:

- Trade union representatives (2)
- Cyber security analyst at a Scottish university
- Cyber security consultant, trainer, and mentor
- Computing Science assistant professor at a Scottish university
- Computing Science professor at a Scottish university
- Digital skills manager
- Senior researcher and project manager at a Scottish university

All of the individuals interviewed provided useful information directly contributing to the exercise of building this Skills Escalator. And a number were very willing to help with the work going forward, including providing more interview material, as well as sharing research of their own that had been conducted, and advice for the Report and the Escalator going forward. The project team appreciates these experts' knowledge and information sharing about initiatives across all aspects of digital and cyber security skills development that have happened in Scotland to date.

Acknowledgements: We gratefully acknowledge the time and commitment given by the interviewees and participants in this research. They have not been named for confidentiality reasons. We also thank Andrew Dean of Exeter University for his insights and comments.

[2] The Scotland country report from ESCALATE provides more information on the Scottish Economic Strategy, which considers digitalisations as one of the main are for economic growth: https://escalate.projects.uvt.ro/wp-content/uploads/2020/11/SOTA-Country-Report-SCOTLAND.pdf

Background to the ESCALATE Project

The ESCALATE project was the subject of a successful application to Key Action 2 – Cooperation for Innovation and the Exchange of Good Practices – of the Erasmus+ programme submitted by West University of Timisoara to the Romanian National Agency. The project has been developed by six partners from five EU countries, namely five universities and an independent company, which specializes on foresight and prospective - strategic studies for the public and private sector.

The ESCALATE project runs for 24 months from 01.11.2019 to 31.10.2021. Its aim is to assist universities in implementing activities designed to increase the levels of digital competences for employability, upskilling, according with a growing range of employment generated by the digital economy, aligned with the needs of and opportunities offered by the labour market and linked to professional profiles.

The primary focus is to understand digital education disruption and to enable open-source technology and innovative solutions for both educators and students, leading to increased learning-outcomes that meet the learning needs of students whilst also being relevant to the labour market and societal needs (creating a 'better' digital future).

Our target groups are higher education institutions (HEI), education providers, teachers, learners for existing and new digital skills provision. Indirect target group consists primarily of those citizens with low levels of digital skills at risk from digitalization facing a keen need to acquire the digital knowledge and use of digital technologies, but also labour market (LM) forecasters such as labour market observatories.

The project has two linked objectives:

- Firstly, to help universities understand the scale and depths of the challenges they face from digitalisation - to enable them to formulate effective policy and education system governance - by developing and making freely available new methods and techniques in digital skills acquiring, foresighting and forecasting. It has explored the state-of-the-art before developing and testing the new materials across 6 major themes.
- Secondly, it trialled a new innovative concept (a Digital Skills Escalator) across a selected region in each partner country to test its potential as a mechanism for both identifying where there is unmet demand and subsequent need for new digital skills provision and as a means of building a more holistic offer from education providers.

The work on the Digital Escalator was based on the University of Exeter's framework, which summarised existing practices and lessons learned from their work developing the Exeter Data Analytics Skills Escalator and was passed onto ESCALATE project partners who then built policy and stakeholder relationships to enable testing of the model in their own region and policy landscape.

This report is a 'Proof of Concept' of the potential use of a Digital Skills Escalator in the context of mapping out and developing digital skills for cyber security sector. It does not attempt to consider state of the art courses etc., related to cyber security, but rather provides an indicative summary of the potential development of related skills, in the current skills system, from the lowest levels to high level courses. It focuses on formal education qualifications but does fully recognised the importance of actual digital user behaviour and professional courses, experiential learning and mentoring.

This report will be distributed to interested organisations, policymakers and the wider public.

The concept of a Skills Escalator

Escalators are relatively new developments that seek to achieve the following two related, but not identical, aims.

1. To ensure a region has sufficient citizens skilled in a particular field/sector critical to economic success.
2. To ensure that the skills and training needed to enter or progress in this field/sector are available locally, at all levels.

The former can be understood as a driver of economic success and the latter is more concerned with inclusive growth. As a project we are looking specifically to develop Digital Escalators where the skills at the 'lower end' of the qualifications can be quite generic but will link into a very specific key sectoral need at the higher end. Linked to a Region's 'smart specialisation'.

A good example of this is the existing Exeter Escalator for Data Analytics Skills[3] is relatively broadly defined. It encompasses topics such as:

- Statistical understanding
- Digital and programming skills
- Use of AI and high-end algorithm development for the analysis of 'big data'
- The translation of environmental intelligence into new products and services and local growth.

The Digital Escalator is a concept that refers to a pipeline of skills (or more accurately a 'funnel of skills' from basic to highly specialised expert levels) linked to a specific smart specialisation sector, represented by a multi-level skills map where people can join or complete their skills journey at different stages.

The fact that a significant proportion of individuals may apply these skills usefully outside the prioritised smart specialisation sector is not problematic. Having a relatively broad, and some might say flexible focus (in which the 'environmental' focus can be picked up or dropped, as convenient) enables engagement across a wide range of educational and other partner organisations and access to a wider range of opportunities.

The Escalator Model is not a fixed journey from school to Higher Education and Continuing Professional Development (CPD) but instead is designed for people to enter and leave when necessary. Its purpose is to promote discussion, engagement and coordinated partnership activity.

The course and skills development opportunities on the Cyber Security Escalator are indicative of those that are related to cyber security at the time of our research but does not claim to be fully comprehensive. It is also not a complete census of related training or firms.

The Stirling area in central Scotland is the main focus of this report, which is highly embedded and interconnected with the rest of Scotland. Hence what happens in the Stirling area is greatly influenced by the Scottish context and policies, as well as UK industry and organisations and Scottish and UK central governments. Stirling is well-suited to the development in cyber security training and employment, due to the large number of skilled graduates from HEIs in the area, as well as several employers in the field, both within Stirling itself, and the neighbouring cities of Glasgow and Edinburgh.

[3] https://escalate.projects.uvt.ro/results/reports-and-results/

The context of cyber security in Stirling and Scotland

Employment in cyber security

Cyber security was chosen as the smart specialisation sector as it is a growing area of digital skills at both regional and national levels, as well as internationally. This is a fast changing sector with hackers and criminals constantly raising new and often innovative problems, suggesting a need for a flexible approach to staffing, education and a flexible skills development pipeline throughout the Cyber security sector. Estimates indicate that there is a cyber security shortage of over 3 million, almost as many as currently work in the field (3.5 million), including a shortage of 168,000 in Europe ((ISC)2 Cybersecurity Workforce Study, 2020)[4]. Our data suggests that "the global cybersecurity workforce needs to grow by 89% to effectively defend organizations critical assets" (p. 3).

Within the broad area of cyber security specific needs in the next two years were estimated to include: cloud computing security (40%); risk assessment, analysis and management (28%); security analysis (28%); and governance, risk management and compliance (26%)" (p. 35). These are near the top of the Skills Escalator, so how people can be assisted to develop skills in order to progress towards types of jobs forms the main parts of the Escalator. In addition to high level skills, basic general cyber security is needed by all staff using digital technology across the economy and society.

A survey conducted for MIT Technology Review's *Digital Acceleration in the Time of Coronavirus* found that technology decision-makers worldwide see cyber security as a main focus going forward for personnel going forward post-COVID-19.[5] For European organisations digital capabilities and application development were seen as key. As well as this, half of the European respondents stated educating their workers regarding cyber security threats was seen was a "principal challenge", with 60% reporting they will be focussing on securing employee devices as part of this.

The UK ranks fifth out of the (in 2020) 28 EU Member States in the 2020 European Digital Economy and Society Index (DESI)[6]. Despite this, there is still a sizable gap in digital skills, and with digital employment continuing to rise, this gap will continually increase if not addressed. In the UK, 74% of individuals have at least a basic level of digital skills. Areas of particular concern are ICT specialists, with only 1.8% of female employment being ICT specialists. Although there is a growing demand for ICT graduates, they only make up 3.8% of graduates overall. Though this is slightly above the EU average of 3.6%.

The Department for Digital, Culture, Media & Sport (DCMS) *UK Cyber Security Sectoral Analysis 2021*[7] notes that 1,483 active firms are providing cyber security products and services in the UK (an increase of 21% since DCMS Report in 2020). There 46,700 FTEs working in cyber security related role across identified firms (increase of 9%) The cyber security sector has grown 7% and has raised £821m raised in 2020 – twice as much as in 2019. The Gross Value Added (GVA) has reached around £4bn (increase of 6%).

The DCMS Report notes that Scotland has 86 registered cyber security businesses, with 283 offices (the majority are in Edinburgh/Glasgow, Aberdeen). Roughly in line with its UK share of population, Scotland is home to 8% of the UK's cyber security sector employment – big firms include Sopra

[4] https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

[5] Digital-acceleration-in-the-time-of-coronavirus-Europe_120820.pdf (technologyreview.com)

[6] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66933

[7] https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2021

Steria, Adarma, Fortinet, Quorum Cyber. According to ScotlandIS, digital technology is the 4th strongest export in Scotland, exporting more than £3.3 billion, and the digital technology sector grows at a rate that is 1.5 times faster than Scotland's overall economy.[8] The *Scotland Digital Technologies: Summary Report 2019*[9] notes that in 2018 the technology sector was responsible for 100,000 jobs across all sectors of employment in Scotland, with technology being an area both growing fast and continuing to expand. Those employed in technology roles covered sectors across all areas of the economy, including healthcare, finance, and energy: 60% of those employed in technology roles being in businesses other than technology itself. Data, cyber security, and artificial intelligence were cited as important specialist skills that were needed, with cyber security skills being required by 82% of the surveyed employers.

Although, as shown above, cyber security is a growing area of employment and business, yet according to the DCMS Cyber Security Skills in the UK Labour Market 2020 report, a high proportion of UK businesses lack staff with the technical, incident response and governance skills needed to manage their cyber security. Approximately 653,000 businesses (48%) have a basic skills gap, with the most common areas including setting up configured firewalls, storing or transferring personal data, and detecting and removing malware. Approximately 408,000 businesses (30%) have more advanced skills gaps, in areas such as penetration testing, forensic analysis and security architecture. A quarter (27%) have a skills gap when it comes to incident response.[10] The Cyber Resilience Strategy for Scotland 2018-20 states that the global cyber security workforce gap is expected to reach 1.8 million professionals by 2022.[11]

A particular area of concern is the lack of diversity in the Cyber Security workforce: the DCMS Report notes that 15% of the workforce are female (vs. 28% of the wider digital sector), the lack of personnel that come from ethnic minority backgrounds (16% in Cyber Security vs. 17% of the digital sector), and 9% are neurodivergent. The Report noted a lack of awareness in regard to these issues, scepticism in regard to the extent of the problem, and few measures being taken to encourage applicants from diverse groups, or to change or adapt the hiring process. The Digital Scotland *Tackling the Technology Gender Gap Together*[12] report notes the lack of female representation in digital technology roles in Scotland, with 82% of these being occupied by men.

According to ScotlandIS, 13,000 digital tech job opportunities are created every year in Scotland.[13] Despite the high demand for technology professionals, employers report skills gaps in areas such as data, cyber security, and artificial intelligence, with only one third of technology employers surveyed by the *Scotland Digital Technologies: Summary Report 2019*[14] reporting that they have the skills that they require. The Report also noted that employers see technical skills and experience being a challenge, with 28% reporting the issue as significant. As well as this, 48% of the business respondents reported digital skills shortages and gaps.

---

[8] https://www.scotlandis.com/about-us/
[9] https://www.skillsdevelopmentscotland.co.uk/media/46258/scotlands-digital-technologies-summary-report.pdf
[10] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020
[11] https://www.gov.scot/publications/learning-skills-action-plan-cyber-resilience-2018-20/
[12] https://www.skillsdevelopmentscotland.co.uk/media/42478/tackling-the-technology-gender-gap-together-2.pdf
[13] https://www.scotlandis.com/about-us/
[14] https://www.skillsdevelopmentscotland.co.uk/media/46258/scotlands-digital-technologies-summary-report.pdf

The Digital World Cyber Security careers map has salaries ranging from £22,000-£90,000 for Scotland.[15] As well as this, ScotlandIS state that the average salary of digital tech workers: £36,900, which is 26% higher than the average salary of all workers in Scotland.

The increasing demand, along with the gaps in both specialist cyber security skills, as well as basic and more complex IT skills generally, at both the regional and national level, points to a need for more targeted skills provision.

Some of Scotland's education and skills strategic priorities related to cyber security

Cyber security awareness is also something that HEIs in particular are concerned with and need to be confident in. Previous research for the ESCALATE project[16] found that as institutions are generally very open in terms of collaboration and research, with department, research units, and individuals being tied to various other research organisations, government departments, and professional bodies means that HEIs are especially vulnerable to cyber-attacks. This was borne out in the interviews conducted, as the university cyber security consultant interviewee noted the vulnerability of universities to cyber-attacks, and the increase of certain types of attacks, such as ransomware, since the onset of the COVID-19 pandemic and with the necessity of employees working from home.

The Scottish Government's vision: The Strategic Framework for a Cyber Resilient Scotland[17] is for Scotland to thrive by being a digitally secure and resilient nation, with four outcomes to achieve this vision:

- People recognise the cyber risks and are well prepared to manage them
- Businesses and organisations recognise the cyber risks and are well prepared to
- manage them
- Digital public services are secure and cyber resilient
- National cyber incident response arrangements are effective

The Framework notes the importance of public bodies being cyber resilience, with 88% of Scottish public sector organisations achieving the Cyber Essentials accreditation provided by the National Cyber Security Centre.

In addition, there are many industry bodies and training providers that encompass cyber security in Stirling and Scotland (see below).

In Scotland, Skills Development Scotland have created Digital Foundation Apprenticeships, aimed at bridging the digital skills gap.[18] It partners technology companies with pupils to support digital career pathways. The digital Foundation Apprenticeships will cover Hardware, Software, and Creative & Digital skills, so that pupils can gain experience of digital skills whilst at school.

---

[15] https://www.digitalworld.net/cyber-security-careers

[16] Webb, A., McQuaid, R. and Webster, C.W. (2021) 'Moving learning online and the COVID-19 pandemic: a university response', *World Journal of Science, Technology and Sustainable Development* https://doi.org/10.1108/WJSTSD-11-2020-0090 ; Robinson, E., McQuaid, R., Webb, A. and C.W.R. Webster (2021) 'Unintended Consequences of E-Learning: Reflections on the Digital Transformation of Learning in Higher Education', in Larsen, C. et al. (eds) *Transformations of Local and Regional Labour Markets across Europe in Pandemic and Post-Pandemic Times* (Rainer Hampp Verlag, Muenchen). http://hdl.handle.net/1893/32909

[17] The Strategic Framework for a Cyber Resilient Scotland (www.gov.scot)

[18] https://www.skillsdevelopmentscotland.co.uk/news-events/2017/march/digital-foundation-apprenticeships-can-help-bridge-digital-skills-gap/

Funding for training has increased such as the launch of the Digital Start Fund[19] – a £1million fund provided by the Scottish Government and managed by Skills Development Scotland – designed to aid those who are out of work and those on low incomes and bridge the gap for businesses who are in need of workers with digital skills by helping to develop skills in software development and cyber security. Training providers include HEIs, Glasgow Life, CodeClan, and ScotlandIS:

- CodeClan is a digital skills academy, accredited by the SQA, designed to bridge the digital skills gap for Scotland's technology industry.[20] It was founded and funded in part by Skills Development Scotland.
- ScotlandIS is a membership and Cluster Management Organisation for the digital technology industry in Scotland. It is for "building, supporting and enabling the digital technology ecosystem."[21] 85% of its membership are SMEs.
- ScotlandIS Cyber is designed to help support business and organisations in creating and delivering cyber driven digital products and services. ScotlandIS Cyber has a directory to link companies looking to collaborate and for individuals looking for cyber products and services. This specialist directory lists "every company in the country that provide these products and services."[22]

There is a range of issues related to basic-level cyber security teaching in schools. There appears to be limited related investment in school staff and equipment, and learning about the subject in the curriculum. There is also a need for a safe technological and educational environment to develop cyber security skills for students at all levels of education.

National priorities

Cyber security in Scotland is closely related to the rest of the UK and so UK government-led initiatives are important in shaping the cyber security landscape in Stirling as are Scottish government-led initiatives. From a UK context, there is an initiative sponsored by the UK's National Cyber Security Centre, part of GCHQ (Government Communications Headquarters), delivering a new Cyber Security Body of Knowledge[23] which is intended as a guide to help enable and develop the cyber security profession. It is designed to help address the skills gap in the cyber security sector, and to consolidate and map relevant knowledge in the field through both analysis of the relevant literature available on cyber security, as well as discussions via workshop, interviews, and online surveys with professionals in the field. The initiative is funded by the National Cyber Security Programme with support from The Department for Digital, Culture, Media & Sport.

The Cyber Skills Immediate Impact Fund (CSIIF) by the UK Government "aims to quickly increase the diversity and numbers of those working in the UK's booming cyber security sector. This is one of a range of initiatives designed in support of the National Cyber Security Strategy aim of developing a sustainable supply of home-grown cyber security talent in the UK. The Fund is open to organisations such as training providers and charities, who can demonstrate their initiatives are not designed to fill internal vacancies, but rather service a range of employers."[24]

[19] https://www.digitalworld.net/study/digital-start-fund
[20] https://codeclan.com/
[21] https://www.scotlandis.com/
[22] https://www.scotlandis.com/scotlandis-cyber/
[23] https://www.cybok.org/
[24] https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund

The 2017 UK Digital Strategy[25] outlines how the UK will be resilient towards a changing digital future, ensuring individuals have the necessary skills for the digital economy, and tackling the digital skills gap. It highlights the importance of supporting individuals with digital up-skilling and re-skilling – a process that will last throughout an individual's working life. The strategy has seven strands: building digital infrastructure; increasing access to digital skills; establishing and growing digital business; helping businesses go digital; ensuring cyber security; maintaining quality in digital governance; growing the data-driven economy.

The digital skills strand of the UK's Digital Strategy aims to tackle digital exclusion, promote collaboration between the public, private, and third sector to tackle the digital skills gap, and support up-skilling and re-skilling for workers through their working lives. This includes helping to enable a diverse workforce, with programmes such as the CyberFirst Girls competition, run by GCHQ to promote cyber career pathways for young girls, the TechFuture Girls programme, an 'after school club' for girl to support engagement in IT, and courses for mothers to learn digital skills such as Techmums and Mums in technology.

The UK Government's Digital Skills Innovation Fund was set up to address local or regional digital challenges and support those from under-represented groups and or disadvantaged backgrounds gain access to digital roles. It also aims to encourage partnerships between employers and training providers to share good practice and identify gaps in provision.

Within `Scotland, the Cyber Resilience Strategy for Scotland: Learning & Skills Action Plan for Cyber Resilience[26] also helps set the context for cyber security skills in Stirling. It has an action plan consisting of four key aims:

- Increase people's cyber resilience through awareness raising and engagement
- Explicitly embed cyber resilience throughout our education and lifelong learning system
- Increase people's cyber resilience at work
- Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland.

The European Union, and various international agencies such as the United Nations, can also be important in setting the wider context, but are not set out here.

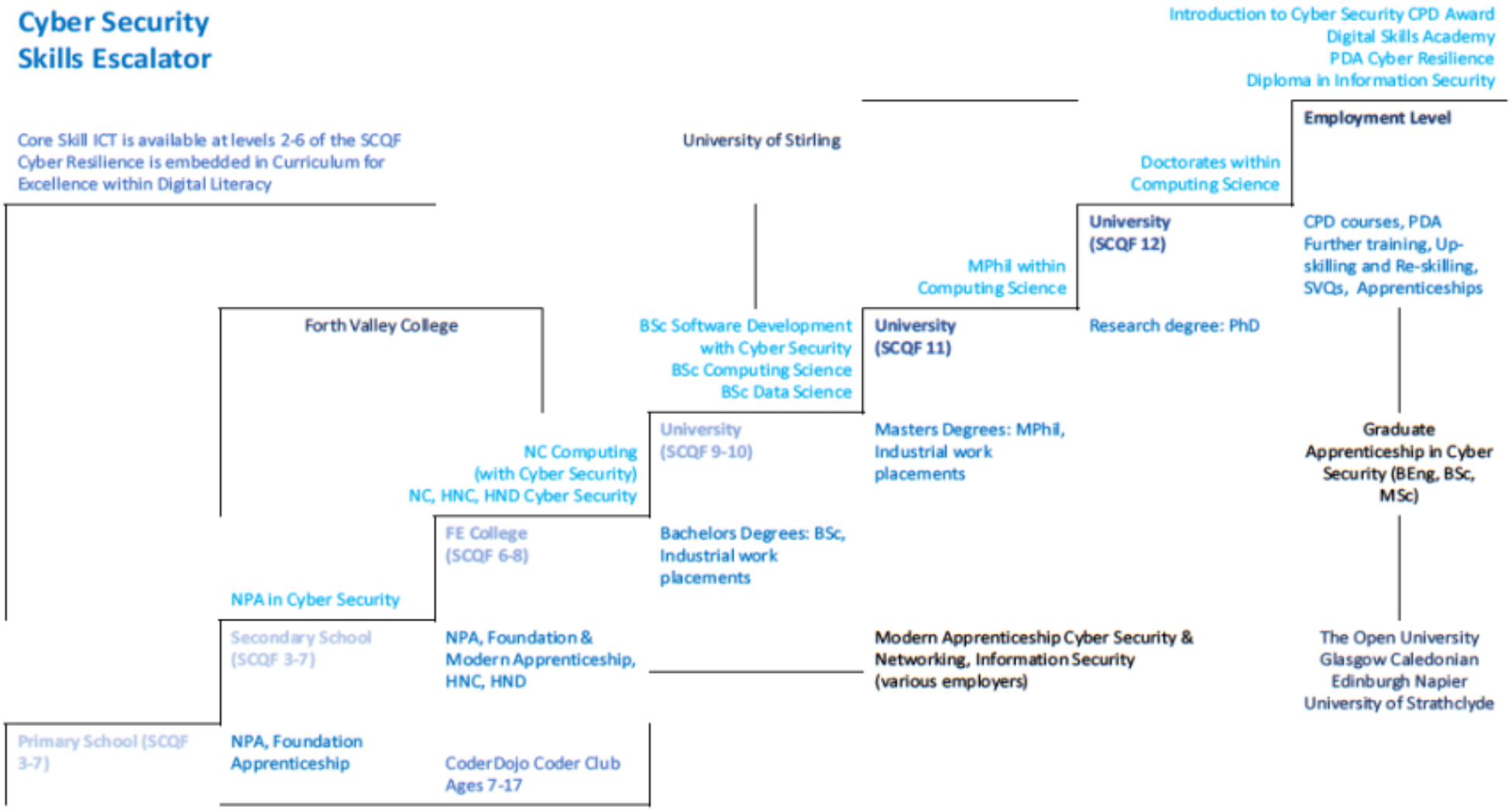
[25] https://www.gov.uk/government/publications/uk-digital-strategy
[26] https://www.gov.scot/publications/learning-skills-action-plan-cyber-resilience-2018-20/

The Digital Skills Escalator for cyber security in Stirling

Although some practical digital skills, and more specifically cyber security skills, are developed through practice at home at an early stage, formal digital skills generally start to be developed in schools and progress through further and higher education and professional training (see Figure 1).

However, much cyber security skills development is also strongly linked to practical experience. The Escalator should therefore be seen as a merging of education, training, mentoring and other skills development as well as formalised and informal practical experience.

Figure 1: Indicative Escalator Model for Cyber Security Skills in Stirling



Digital Skills taught at schools

Cyber resilience is currently embedded in the (national school) Curriculum for Excellence within Digital Literacy. The Scottish Qualifications Authority (SQA) has *ICT as one of the five core skills* along with communication, numeracy, working with others, and problem solving.[27] The SQA is reviewing the ICT Core Skill framework, in which cyber resilience will likely be highlighted as a core aspect[28]. Cyber resilience is currently embedded in the Curriculum for Excellence within Digital Literacy.

A number of schools offer the *National Progression Award (NPA) in Cyber Security*.[29] This is co-delivered by employers and teachers and helps to establish cyber security as a viable career path for young people. Allowing for this award to be made available at more schools would reinforce this, and cement schools as playing a foundational role in getting people interested in computing science and cyber security.

However, there are a number of issues with both computing science and cyber security in schools in Scotland. As noted in a report for The Centre for Research in Digital Education[30], there is a lack of adequate *teaching availability* in computing science at Scottish schools.

Greater priority for computing teaching in schools is needed with the *Scottish Technology Ecosystem Review* of 2020 suggesting that "a transformation of Computing Science education at school level, with the principle that the subject must be treated, from 1st year at secondary school level with the same focus as Mathematics or Physics"[31] is needed, alongside more support outside of education. There may be scope for pilots in school where this is trialled in different ways as part of the curriculum and perhaps greater 'Training the Trainers' where teachers are provided with online or other courses and new easy to use resources that could emerge from the pilots.

There is insufficient *female representation* in digital technology occupational roles in Scotland that can be traced back to early and higher education. For instance, the *Tackling the Technology Gender Gap Together*[32] report notes that the dearth of female representation in digital technology roles (just 18%), which was seen by survey respondents as stemming from the lack of women in ICT courses at university. The Report noted that women make up 16% of students in Computing Science courses at Scottish Universities, and 20% of those studying Computing Science at the National 5 level at school. Initiatives such as the Tech Talent Charter[33] help to encourage organisations to become more inclusive. It is run as an industry collective, and helps organisations of varying size, and in diverse fields. Encouraging companies and organisations to sign-up for the Charter could help to drive greater diversity and inclusion in the workforce and promote a wider variety of candidates at the educational level.

Unlike medicine or law, cyber security and other technology jobs such as data analyst or software developer are not always seen as viable career options due to being more newly established. It was suggested in stakeholder interviews that more work needs to be done to ensure greater children and parents' *awareness of the potential careers* and salaries available to those who opt to pursue cyber security (and computing science more generally) as a career path. Allowing for employers to

[27] https://www.sqa.org.uk/sqa/83655.html
[28] https://www.gov.scot/publications/learning-skills-action-plan-cyber-resilience-2018-20/
[29] https://www.gov.scot/publications/learning-skills-action-plan-cyber-resilience-2018-20/
[30] https://www.research.ed.ac.uk/files/118843174/CS_Teacher_Shortage_Report_UoE_SDS_Nov_2019.pdf
[31] https://www.gov.scot/publications/scottish-technology-ecosystem-review/
[32] https://www.skillsdevelopmentscotland.co.uk/media/42478/tackling-the-technology-gender-gap-together-2.pdf
[33] https://www.techtalentcharter.co.uk/about-the-tech-talent-charter

provide demonstrations at schools would also help, due to the swift changing nature of technology. Skills Development Scotland is helping to launch new cyber security lessons which are being developed by industry specialists and teachers in Scotland. The pilot programme of 2020 ran across six secondary schools across Scotland, with 120 pupils taking part[34]. The lesson centres around penetration testing (ethical hacking) and aims to take students through the process of ethically hacking a fictional airline in a virtual environment. Training will include penetration testing, social engineering, and collecting intelligence of digital footprints. Skills Development Scotland also developed the Cyber Skills Initiative, which teaches school children about ethical hacking and digital forensics[35].

The National Parent Forum of Scotland and Skills Development Scotland created a "Cyber security careers IN A NUTSHELL", as part of the information series In a Nutshell, to encourage young people to consider a cyber security career pathway. The Nutshell series is designed to work as a *starter pack* to help discuss possible career options with children[36].

The UK's National Cyber Security Centre (NCSC) promotes cyber and *cyber security career pathways for girls*, with initiatives including the CyberFirst Girls Competition with pupils at nine Scottish schools getting to the semi-finals in the 2021 competition[37]. The competition is part of the NCSC's general CyberFirst programme, designed to help encourage 11-17 year olds to consider a cyber security career pathway though student bursaries, courses, and competitions[38].

Outside of school, there are a number of initiatives, although many are relatively small, and sometimes run on a volunteer basis. Initiatives such as the Young Scot's Digital Academy[39], Lead Scotland's Getting Digital programme[40], and the Digitally Agile Community Learning and Development project[41] help in *developing cyber resilience* in young people.

Within Stirling, the *CoderDojo Stirling club*[42] is a free, volunteer-run, monthly coding club for children ages 7-17. The club is based at the Stirling CodeBase site. It is part of CoderDojo Scotland[43], part of an international collaboration providing educational coding experiences for young people.

Digital Skills taught at colleges

There are various qualifications available at further education colleges in Scotland, such as Higher National Diplomas (HNDs)(SCQF level 8), Higher National Certificates (HNCs)(level 7), and National Progression Awards (NPAs)(levels 4, 5 and 6), a snapshot of these can be found in Scotland's Cyber Resilience Strategy[44] and courses can also be located on the SQA website[45].

[34] https://www.skillsdevelopmentscotland.co.uk/news-events/2020/february/cyber-experts-join-teachers-to-launch-pilot-school-programme/
[35] https://www.skillsdevelopmentscotland.co.uk/news-events/2019/september/scottish-schools-love-cyber-security-sessions/
[36] https://www.npfs.org.uk/downloads/cyber-security-careers-in-a-nutshell/
[37] https://www.gov.uk/government/news/scottish-schoolgirls-succeed-in-uk-cyber-security-competition
[38] https://www.ncsc.gov.uk/cyberfirst/overview
[39] https://www.youngscot.net/what-we-do/digital-academy/
[40] http://www.lead.org.uk/getting-digital/
[41] https://www.digitallyagilecld.org/
[42] http://coderdojostirling.com/
[43] https://coderdojoscotland.com/
[44] https://www.gov.scot/publications/learning-skills-action-plan-cyber-resilience-2018-20/
[45] https://www.sqa.org.uk/sqa/74739.html

Courses Provided by Colleges Across Scotland		
College	**Type**	**Course Name**
Dundee and Angus College	HNC	Cyber Security
Fife College	HND	Cyber Security
City of Glasgow College	HNC	Cyber Security
Glasgow Clyde College	HND	Computing Cyber Security
New College Lanarkshire	HNC	Cyber Security
North East Scotland College	HND	Cyber Security
University of the Highlands and Islands (various Colleges)	NPA	Cyber Security

Within Stirling, Forth Valley College provides Cyber Security courses at the NC, HNC, and HND level, along with NPA courses for schools.

Courses Provided by Forth Valley College	
Course Type	**Course Name**
NC	Computing (with Cyber Security)
HNC	Cyber Security
HND	Cyber Security
NPA	Cyber Security

It was noted in stakeholder interviews that a large number of college graduates go on to study cyber security at university, rather than going directly into employment. There appears to be missed potential here, as many of these graduates may be suited to joining the workforce at this stage, rather than going onto further education, and employers regularly request experience in cyber security as well as formal qualifications. One of the interviewees noted that both employers and college graduates seek university level qualifications when this may not be necessary. It was noted by a number of interviewees that the college sector is underserved, with inadequate support in terms of resources and sometimes a sense of misalignment between the employers' expectations and educational skills gained at colleges or universities.

Digital Skills taught at universities

Particularly for high level skills, university education is often required (along with relevant on-the-job experience). Cyber Security has been a growing university discipline across the whole of the UK. The National Cyber Security Centre (NCSC) and the Engineering and Physical Sciences Research Council (EPSRC) each year recognise university institutions across the UK that have excellence in Cyber Security research. The Academic Centres of Excellence in Cyber Security Research (ACE-CSR) list has grown from 8 universities in 2012, to 19 in 2020, and Cyber Security research is covered across a range of disciplines, including computer science, engineering, psychology, sociology, mathematics, law and humanities. These 19 universities must show:

- "commitment from the university's leadership team to support and invest in the university's cyber security research capacity and capability
- a critical mass of academic staff engaged in leading-edge cyber security research
- a proven track record of publishing high impact cyber security research in leading journals and conferences

- sustained funding from a variety of sources to ensure the continuing financial viability of the research team's activities." [46]

University Courses Across Scotland		
University	**Type**	**Course Name**
Abertay University	Undergraduate	BSc (Hons) Cybersecurity
		BSc (Hons) Ethical Hacking
	Postgraduate	MSc/PGDip Ethical Hacking and Cyber Security
University of Aberdeen	Postgraduate	MSc Cybersecurity
University of Dundee	Undergraduate	Information Security (module)
University of Edinburgh	Postgraduate	MSc Cyber Security, Privacy and Trust
Edinburgh Napier University	Undergraduate	BEng (Hons) Cyber Security and Forensics
	Postgraduate	MSc Advanced Security and Digital Forensics
Glasgow Caledonian University	Undergraduate	BSc (Hons) Cyber Security and Networks
		BSc (Hons) Digital Security and Forensics
		BSc (Hons) Graduate Apprenticeship Cyber Security
		BSc (Hons) Cyber Security and Networks Pathway
	Postgraduate	MSc Cyber Security
		MSc Graduate Apprenticeship Cyber Security
Heriot Watt University	Undergraduate	BSc (Hons) Computer Science (Cyber Security)
Robert Gordon University Aberdeen	Undergraduate	BSc (Hons) Cyber Security
	Postgraduate	PGCert/PGDip/MSc Cyber Security
		PGCert/PGDip/MSc Information Technology with Cyber Security
University of Strathclyde	Postgraduate	MSc Cyber Security
University of the West of Scotland	Undergraduate	BEng (Hons) Cyber Security
	Postgraduate	MSc Cyber Security

Residents of Stirling have relatively easy access to most of these universities and all of the central Scotland universities. The University of Edinburgh is recognised by the NCSC and the EPSRC as an Academic Centres of Excellence in Cyber Security Research (ACE-CSR).

Edinburgh Napier University's undergraduate course in Cyber Security and Forensics (BEng) was the first undergraduate course in the UK to achieve full accreditation from the NCSC.

Within Stirling, the University of Stirling provides an undergraduate BSc (Hons) course in Software Development with Cyber Security. The course is provided in collaboration with Forth Valley College. The first two years are located in Forth Valley College's campus in Falkirk, and the last two years are delivered within the University of Stirling's campus in Stirling.

Undergraduate courses at the University of Stirling such as the BSc (Hons) Computing Science and BSc (Hons) Data Science also contain elements of Cyber Security in the course content.

Courses Provided by the University of Stirling	
Course Type	**Course Name**
Undergraduate	BSc (Hons) Software Development with Cyber Security
Undergraduate	BSc (Hons) Computing Science
Undergraduate	BSc (Hons) Data Science

[46] https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research

Research on Cyber Security can take place as part of the Global Security and Resilience theme[47] , which is one of the key research priority area at the University of Stirling. The Global Security and Resilience theme covers a wide range of disciplines.

Postgraduate options at the University of Stirling include research degree MPhil and PhD within Computing Science.

Other Higher Education Research Groups, Societies and Research Networks in Scotland

The University of Edinburgh has the Security, Privacy and Trust group in the School of Informatics which is the largest grouping in the field in the UK, with 18 academic staff and 15 affiliated staff from around the University. There is a monthly security seminar series held by the group, featuring world experts in the field.[48]

Other networks within the University of Edinburgh include the Blockchain Lab which aims at studying all aspects of distributed ledger technology.[49] The University of Edinburgh is also home to the Bayes Centre innovation hub for Data Science and Artificial Intelligence. The Bayes Centre occupies a building neighbouring Informatics Forum and has numerous links with the School.[50]

The CompSoc (Computer Science Society) is the largest tech student society in Scotland. The society includes several Special Interest Groups. The Cyber Security Interest Group SigInt is the most active of these.[51]

At the University of the West of Scotland, the Artificial Intelligence, Visual Communications and Networks (AVCN) research centre is a strong research centre within the university. AVCN has "its own cloud infrastructure, 5G network, and a complete mid-size data centre designed to carry out computational experimentation in the field of Big Data, Cloud Computing, Data Security and Privacy."[52]

Abertay University's Division of Cyber Security is one of three Divisions in the School of Design and Informatics. It has strong links with government, Police, and industry. Projects include improving the security of SMEs, training in cybercrime response using games technologies, and cyber security into the Software Development Lifecycle. The Division's research a key part of the university's Security Research Theme along with Forensic Psychology, Forensic Science, and Law. The research of the Division is structured into four overlapping areas: responding to prevailing challenges of system security; vulnerability detection and the threats introduced by Internet-connected devices; the usability of security prevention measures; and using visualisation techniques to improve security.[53]

Across Scotland, there is the Scottish Informatics and Computer Science Alliance: SICSA. This collaboration of 14 Scottish universities aims to develop Scotland's place as a world leader in

[47] https://www.stir.ac.uk/research/research-themes/global-security-resilience/
[48] https://web.inf.ed.ac.uk/security-privacy
[49] https://www.ed.ac.uk/informatics/blockchain
[50] https://www.ed.ac.uk/bayes
[51] https://sigint.mx/
[52] https://www.uws.ac.uk/research/research-areas/computing/artificial-intelligence-visual-communication-networks-avcn-research-centre/
[53] https://www.abertay.ac.uk/research-overview/research-strategy-and-structure/division-of-cyber-security/

Informatics and Computer Science research and education[54]. One of the Research Themes of SICSA is Cyber Security.[55] This theme is closely aligned with the SICSA Cyber Nexus, in which SISCA engages with businesses, government, public, and third sector parties to "ensure Scottish higher education institutions are playing their part in making Scotland more cyber resilient and in creating a vibrant innovation community."[56] The SICSA Cyber Nexus is funded by the UK Government via the Scottish Government's Cyber Resilience Unit.[57]

At the University of Stirling, individuals can join the Computer Club. The Computer Club supports projects and activities for those interested in Computer Sciences, and events include a Hackathon.

The Data Science and Intelligent Systems[58] research group is one of a number of various research centres and groups based at the University of Stirling. The group is multidisciplinary, with academics based across various subjects including engineering, computing science, biological and environmental sciences, and mathematics. The leader for the Cyber Security research theme of SICSA is based at the University of Stirling within the Data Science and Intelligence Systems research group.

Employee Training/CPD Opportunities

Skills for Security, a UK Skills Sector Body, is the UK's largest fire and security apprenticeship provider for employers. Upskilling CPD courses are provided online, including Principles of Internet Safety. Apprenticeships are courses lasting a minimum of 12 months and combines hands-on work with the opportunity to train and obtain qualifications. Apprenticeships include Fire and Security Systems.[59]

The UK Government's Cyber Essentials scheme, provided by the NCSC, helps organisations guard against cyber-attacks. The scheme shows organisations how to address and prevent common cyber-attacks as well as a more in-depth Cyber Essentials Plus course that includes hands-on technical verification.[60] Certification is provided by the IASME consortium.[61]

Glasgow Caledonian University has a Digital Skills Academy 7-week introductory course Introduction to Cyber Security designed for beginners to learn foundational theoretical knowledge and gain practical experience of network and system security. It is aimed towards companies wishing to train staff in aspects of Internet security.[62]

Glasgow Caledonian University also has the GCU Digital Skills Academy, an accredited training centre providing flexible evening and part-time courses, specialising in Cisco and Oracle.[63]

The University of the Highlands and Islands provides the Introduction to Cyber Security CPD Award for primary and secondary school teachers. The course is designed to help teachers "develop the knowledge, understanding and problem-solving skills related to teaching basic cyber security, and

[54] https://www.sicsa.ac.uk/
[55] https://www.sicsa.ac.uk/research/cyber-security/
[56] https://www.sicsa.ac.uk/research/sicsa-cyber-nexus/
[57] https://cybernexus.org/
[58] https://www.stir.ac.uk/research/hub/tag/606462
[59] https://www.skills4security.com/
[60] https://www.ncsc.gov.uk/cyberessentials/overview
[61] https://iasme.co.uk/cyber-essentials/
[62] https://www.gcu.ac.uk/digitalskillsacademy/cybersecurity/
[63] https://www.gcu.ac.uk/digitalskillsacademy/

are configuring an environment suitable for cyber security education." The course is delivered online so that it may fit around the teacher's work schedule.[64]

A number of apprenticeships are also offered, to allow individuals in school and employment to obtain a qualification and industry experience whilst studying or working in employment:

The Foundation Apprenticeship in IT: Software Development, [65] developed by Skills Development Scotland with employers, colleges, and Sector Skills Councils, allows for school students to gain an apprenticeship qualification whilst studying at school. The course allows students to work on college and industry led projects, and attend a work placement. The Foundation Apprenticeship provides a National Progression Award (NPA) at SCQF level 6.

The Modern Apprenticeship in Information Security[66] and Information Security Technical[67] takes 12-24 months to complete and allows candidates to gain an SVQ in Information Security at SCQF levels 5-8 whilst completing a work placement.

The Graduate Apprenticeship in Cyber Security,[68] is a course where students can learn while working in paid employment. This course is provided at undergraduate and postgraduate level, in universities such as Glasgow Caledonian University, Edinburgh Napier University, the Open University, and the University of Strathclyde. Postgraduate courses, such as the MSc in Cyber Security provided at the University of Strathclyde, are aimed at working professionals already employed in an IT role, and is designed to help workers develop and enhance their digital skills. Courses are attended online, and on-campus, and features a mixture of group projects, exams, lectures, work-based learning, and practical assignments. Graduate Apprenticeships are funded by the Scottish Government through Skills Development Scotland.

Accreditation

There are well established career development paths and certification schemes including CISSP (Certified Information Systems Security Professional) run by ISC2 (International Information System Security Certification Consortium).[69]

UK societies for Cyber Security and accreditation schemes include:

British Computer Society

Chartered Institute of Information Security

Information Systems Security Association (ISSA)

EC-Council

The National Cyber Security Centre Certified Training scheme

[64] https://www.uhi.ac.uk/en/courses/cpd-award-introduction-to-cyber-security/index.php
[65] https://www.apprenticeships.scot/browse-frameworks/foundation-apprenticeships/it-software-development/individual-it-software-development/
[66] https://www.apprenticeships.scot/browse-frameworks/modern-apprenticeships/information-security/individual-information-security/
[67] https://www.apprenticeships.scot/browse-frameworks/modern-apprenticeships/information-security-technical/individual-information-security-technical/
[68] https://www.apprenticeships.scot/browse-frameworks/graduate-apprenticeships/cyber-security/individual-cyber-security/
[69] https://www.isc2.org/Certifications/CISSP

The National Cyber Security Centre Certified Professional Scheme (CCP)

CCNA Cisco Certified Network Associate and CCNP Cisco Certified Network.

Awareness Raising

Raising awareness generally of careers in cyber security is needed. Some courses help to do this, albeit in a limited way. Glasgow Caledonian University has a Cyber Security Clinic which aims to "raise awareness of good cyber behaviours in the everyday lives of individuals within the Greater Glasgow community."[70] Services and advice are provided online and face-to-face via pop-up clinics in Glasgow City Centre. The clinic gives advice on various cyber security issues and has specialities in gaming, encryption, password management, spam emails and home network security.

Cyber Scotland Week aims to improve awareness; showcase innovation; and promote skills. It is designed to "draws together events across Scotland designed to make businesses, organisations and individuals more cyber aware and resilient."[71]

The Scottish Cyber Awards "are for anyone working in the cyber field who feels they or they know of someone who is going above and beyond their day job to make a difference to the cyber security of Scotland."[72] Awards include Best Cyber Education Programme, Cyber Security Teacher of the Year.

Digital Skills in the Workplace

There is a distinction between developing cyber security skills through work experience (which we mainly consider in this section) and cyber-security as a professional career.

Prospects, a UK graduate careers website run by Jisc, outlines various job profiles, including what the job entails, typical salary ranges, skills and qualifications needed, as well as potential employers, work experience, and career prospects. The Cyber Security analyst job profile includes potential employers such as security consultancies, information technology companies and network providers, financial services institutions, and governmental organisations.[73]. It also links to specialist job vacancy websites: CWJobs, Cyber Security Jobs, CyberSecurityJobsite, ITJobsWatch, and Technojobs. As well as the various professional development and accreditation schemes.

Digital World was developed by Skills Development Scotland and the Digital Skills Group to help people explore digital careers. The very useful website maps out careers, as well as locating training courses that are available across Scotland. Its careers map for Cyber Security lays out different jobs, the typical job titles used for these, the typical duties done in the job, the qualifications that are required, the typical salary range, and the necessary skills needed for the job. As well as this, the website lists IT roles that commonly are associated or feed into Cyber Security careers.[74]

Scottish Union Learning, part of the Scottish Trades Union Congress (STUC), helps to support trade unions in accessing skills and lifelong learning opportunities for their members. To address the digital skills gap in Scotland, Scottish Union Learning provides the Everyday Skills Group, which looks to promote learning in areas including literacy, numeracy, and basic IT and digital skills. It works with other partners including the Scottish Government, Education Scotland, Learning Link Scotland, and the Scottish Book Trust to raise awareness of needs and appropriate venues of support. This includes

[70] https://www.gcu.ac.uk/cebe/cybersecurityclinic/
[71] https://cyberscotlandweek.com/
[72] https://scottishcyberawards.co.uk/
[73] https://www.prospects.ac.uk/job-profiles/cyber-security-analyst
[74] https://www.digitalworld.net/cyber-security-careers

engaging with Governmental strategies and national initiatives and events.[75] As well as this, a project between Scottish Union Learning and Digital Skills Education Ltd provides cyber skills training to unions, union representatives, members and workers in Scotland through interactive workshops. The project stems from Digital Unions and Cyber Resilience 'Seedcorn' projects and aims to increase cyber resilience in workplaces. It was awarded funding from the Scottish Government.[76] Courses for union members include micro credentials provided through the Open University and the Future Learn platform. These courses, provided at SCQF 11, allow for upskilling of digital skills. The Cyber Security Operations course is endorsed by Cisco and last for 12 weeks. At the end of the course, graduates receive 15 postgraduate credits.[77]

In response to the significant skills gap in Scotland in regard to cyber security, in 2020 a project by Skills Development Scotland, social enterprise SaluteMyJob, Abertay University, IBM and tech start up Skillzminer was launched aimed at helping reskill Scottish Veterans to fills the 13,000 digital jobs in Scotland. The project sees participants attend a preparatory course at Abertay University, along with online study and job shadowing.[78]

Role of experience

An issue consistently raised is the importance of on-the-job experience as well as formal qualifications. This raises issues of increasing and improving mentoring and in-work support so that this is an attractive option in addition to seeking additional qualifications, and to support more women into the sector. Perhaps digital badging (e.g., accrediting what people can do or how long they have worked in the sector)[79] may also assist in making experience more attractive to those with only formal qualifications but little or no industry experience, to those limited formal qualifications and to employers.

It seems essential that a Skills Escalator, or indeed, cyber security skills development generally should try to systematically integrate actual work experience into more formal training at all levels.

[75] https://www.scottishunionlearning.com/work-everyday-skills/
[76] https://www.scottishunionlearning.com/cyber-resilience/
[77] https://www.futurelearn.com/microcredentials/cybersecurity-operations
[78] https://www.skillsdevelopmentscotland.co.uk/news-events/2020/february/scottish-veterans-reskilled-to-fill-growing-cyber-security-workforce-gap/
[79] A suggestion by Andrew Dean, Exeter University.

Aligned Investments

There are a number of initiatives that are complementary of to specific skills development in cyber security. Related new investments in cyber security include the Abertay University cyberQuarter, an £18m cyber security research and development centre, due to be open Summer 2022.

The centre aims to be:

- "A physical space for collaboration and experimentation using digital tools and technologies.
- A secure cloud-computing infrastructure enabling online teaching and learning, and a digital provision of R&D and knowledge-exchange activities.
- A Pump Priming Fund to help develop new cyber products, services and education programmes."[80]

EIT Digital is an organisation which aims to further digital innovation and entrepreneurial education in Europe.[81] Its ecosystem consists of corporations, SMEs, start-ups, universities and research institutes. EIT Digital has a satellite based in Edinburgh, at the University of Edinburgh's Bayes Centre. The satellite office is supported by Scottish Enterprise, Scottish Funding Council, Edinburgh Innovations, Borders Enterprise and Highlands and Islands Enterprise. It currently hosts three Doctoral Training Centres across two universities focussed on Cyber Security, Fintech and Digital Identity.[82]

In response to the significant skills gap in Scotland with regards to cyber security, in 2020 a project by Skills Development Scotland, social enterprise SaluteMyJob, Abertay University, IBM and tech start up Skillzminer was launched aimed at helping reskill Scottish Veterans to fills the 13,000 digital jobs in Scotland. The project sees participants attend a preparatory course at Abertay University, along with online study and job shadowing.[83]

CodeBase Stirling[84] is a hub that supports the tech community by providing a space for start-ups, hotdesking, workshops, events and helps to development digital skills through a Level:Up Programme. Events include coffee mornings to connect with various individuals in the technology, creative, and business industries, educational webinars, and monthly meet-ups with members of the other CodeBase hubs throughout Scotland.

In addition, it is worth noting that the Scottish Government, and its agencies, help provide a framework for some national co-ordination of cyber security skills development.

[80] https://www.abertay.ac.uk/business/cyberquarter/
[81] https://www.eitdigital.eu/about-us/
[82] https://www.eitdigital.eu/about-us/locations/london-clc/edinburgh-satellite/
[83] https://www.skillsdevelopmentscotland.co.uk/news-events/2020/february/scottish-veterans-reskilled-to-fill-growing-cyber-security-workforce-gap/
[84] https://www.thisiscodebase.com/stirling

Skills priorities and recommendations

Digital skills gaps and shortages in Stirling

The high level of future demand for cyber security specialists is expected (see above) means that skills shortages (a lack of potential job candidates with the required skills) and skills gaps (a lack of needed skills within the existing workforce) need to be tackled. It was noted in more than one of the interviews conducted, that teaching both cyber security and computing science in general in schools needs to be improved. As discussed above, 'Train the ~Trainers' programmes may be useful.

Several the interviewees highlighted the lack of computing science teachers in Scotland – something that is also noted in the joint report *Towards a Sustainable Solution to the Shortage of Computing Teachers in Scotland*[85], which notes that target numbers by the Scottish Government for computing science teaching students have not been met. Teaching cyber security is a challenge at schools, as it requires students to conduct exercises that, if outside the training exercise, would be considered illegal (such as hacking into a website). Such practices may not be carried out on systems connected to the school network. These systems, and the constant training that is required for cyber security teachers to keep up-to-date with their subject area, is not always provided for fully by the school. To be successful at the specialisation level of cyber security, there also must be a good foundation in general digital skills from school level up. Providing a safe environment for training students in various cyber security skills, such as how to prevent increasingly more common and sophisticated hacking attempts, would be recommended at all levels of education.

Alongside this, an interviewee also noted that the progression route once students gain the NPA certification is unclear, leading to questions such as: should students go into employment afterwards, or should they go on to do a specialist degree in cyber security? If the pathway was laid out more clearly this would also help. Hence there needs to be clarity on the career progression alternatives (both in terms of qualifications and experience) following each qualification, or each step of the Skills Escalator.

As well as this, digital skills in general, including cyber security, should be introduced to non-technology courses in school.

Higher level smart specialisation sector skills gaps needing to be addressed

In some interviews it was mentioned that there was a problem with the hiring process for cyber security careers. In Scotland, many businesses will hire cyber security workers from other businesses, rather than newly graduated students. Potential new cyber security professionals may find themselves working low-level jobs for low wages, with difficulty in career advancement, and suffer burnout.

Instead of going into employment, it was noted that a lot of college graduates will go into university instead. Alongside this, employers tend to look for university graduates, rather than seeking those who have graduated from college. This leaves a large untapped pool of talent, who may have the necessary skills, and could be recruited into positions straight from college into employment.

Some interviewees spoken to mentioned colleges as being an underserved sector.

It was also noted by a professional in security training, mentoring, and consultancy, that cyber security training does not follow the same pathway of other careers and this is something of a

[85] https://www.research.ed.ac.uk/en/publications/towards-a-sustainable-solution-for-the-shortage-of-computing-teac-2

detriment. Neurosurgeons, for example, require training in general medicine, prior to their specialisation. Cyber security, on the other hand, often starts training very specialised. Again, a strong foundation of computing science at school would go some way to help this. There is a need for greater integration between formal education and workplace training, with 'buy-in' from employees and employers, and helping to ensure that learning on the job is of a level sufficient for potential career change into, and career success in cyber security.

Finally, in terms of the future development of related industries and employment in Stirling region, it is worth noting that: existing and new local businesses need access to cyber security expertise, that there needs to be greater development of cyber security skills in Stirling schools as well as awareness raising more generally; and that any aspiration for high tech employment in the region is likely to be linked to availability of cyber security expertise.

Recommendations to tackle the above skills gaps and shortages

To help fill in the digital skills and cyber security skills gap, a number of actions may be useful according to our interviewees.

General recommendations for actions to help fill in the digital skills and cyber security skills gap include:

1. Increased investment in school staff and equipment, as well as focussing on helping more graduates go into computer science and cyber security teaching, and improving the curriculum were recommended by more than one of the interviewees. Providing a safe technological and educational environment for developing cyber security skills, for example shared specialist software and hardware in training on ethical hacking, is essential for students at all levels of education.
2. Greater employer involvement with schools, including expanding the National Progression Award courses, and encouraging children and parents to see computing science and cyber security as a viable career choice, will help to cement the school as playing a foundational role for young people.
3. Increasing the employability of college and university graduates is important, particularly by addressing the digital skills gap, and especially for students with little previous exposure in this area and those from disadvantaged backgrounds. Training facilities such as dedicated tech centres and bootcamp courses for college and HE students to learn relevant coding languages could be co-funded or co-supplied by employers. Students could be offered placements at local organisations which would strengthen the links between businesses, FEs and HEIs as well as provide a fresh talent pool for employers.
4. Investing in colleges through increasing the number of applied or practically-oriented courses, as well as apprenticeships and workplace-based learning models (similar to Graduate Apprenticeships co-delivered by colleges/universities and host organisations/ employers). In addition, better conversion pathways for continuing education in the cyber security specialism should be collectively developed by FE sand HEIs.
5. Increasing investment in the provision of workplace training, funded or co-funded by employers, unions, and the government, to ensure a basic level of cyber security and digital skills, as well as opportunities for specialist skills development and potential pathways for career changes for existing workforce. In particular, digital skills and cyber-security focused work-based training organized and championed by employers and unions needs further and continuous support to bridge the skill gaps across the workforce and offer new career

opportunities for workers across economic sectors. For example, a union learning fund could include a cyber security skills element in relevant projects in Scotland.

Recommendations for how the Skills Escalator model can be improved

This report has been a short review of cyber security skills in Stirling and the potential for creating a more comprehensive Skills Escalator in Stirling with implications for other parts of Scotland. This report has illustrated a 'Proof of Concept' of the potential use of a Digital Skills Escalator.

A larger study and a greater number and range of employers, employees, students, potential students, educationalists, trainers, and policy makers would probably raise more issues and help the unpacking of issues raised. In addition, the geographic focus could be expanded to Central Scotland, and indeed all of Scotland, especially given the inter-connectedness of so many areas. The main conclusion is that an Escalator model is useful for considering cyber security skills development in Stirling and Scotland and important issues need rapid action in order for local people to take the opportunities offered by the sector.