The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation

Daniel Hulatt, Eliana Stavrou

The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation

Daniel Hulatt[1][0000-0002-7105-3033] and Eliana Stavrou[2][0000-0003-4040-4942]

[1,2] Applied Cybersecurity Research Laboratory, University of Central Lancashire, Cyprus
[1] daniel.hulatt@gmail.com, [2] estavrou@uclan.ac.uk

Abstract. The unexpected digital transformation that was forced due to COVID-19 found many citizens and organizations unprepared to deal with the relevant technological advances and the cyber threat landscape. This outcome highlighted once more the cybersecurity skills shortage and the necessity to address this gap. A solution to this, is to consider a multidisciplinary cybersecurity workforce with professionals originating from different backgrounds, beyond the traditional ones such as computing and IT. To be able to engage people though, they need to be aware of the possibilities that exist in cybersecurity for those that originate from non-traditional disciplines. Moreover, cybersecurity professionals need to be aware of the added value when collaborating with these professionals. These are aspects that need to be extensively investigated to provide insights to academia and industry, to develop education and training curricula towards building a multidisciplinary cybersecurity workforce. This paper investigated these aspects in a Further Education and Higher Education College in the UK, where 88 students from 5 disciplines were surveyed, providing valuable observations as to the interest of students, and future professionals, to work in cybersecurity industry and their perception on the subject disciplines relevant to cybersecurity jobs.

Keywords: Cybersecurity education, Multidisciplinary Cybersecurity Workforce, Cybersecurity Skills Shortage

1 Introduction

COVID-19 has reformed how citizens and organizations communicate and do business. This new societal reality expanded the attack surface [1] and gave opportunities to attackers to get even more creative and attack every aspect of society. Unfortunately, not all organizations have been prepared to deal with the digital transformation that resulted due to COVID-19, in terms of security technologies, procedures, human resources and relevant expertise. This had impacted their operations severely, and on many occasions, putting them out of business.

Although demand for cybersecurity professionals is rising the last few years, there is a huge skills shortage that the industry is trying to address [2]. To do so, the industry needs to explore a diverse range of solutions to narrow the ever-increasing cybersecurity skills shortage. One approach is to consider a diverse workforce that will

completement the competencies of people that are developed in the context of different disciplines. Traditional disciplines that have a direct link with cybersecurity include Computing and IT. The challenge here is to be able to engage people originating from a range of disciplines, beyond the traditional ones, and build the necessary workforce faster. To be able to engage people though, they need to be aware of the possibilities that exist in cybersecurity for those that originate from non-traditional backgrounds. Also, it is essential for cyber professionals to be aware of complementary disciplines and how professionals from these disciplines can offer an added value when included in a cyber team. These are aspects that are not extensively investigated. However, at a time where cyber professionals are struggling to keep up with their responsibilities that expand due to the dynamic threat landscape, expanding the cyber teams with professionals from other disciplines to offer support, can assist in balancing the amount of responsibility with the cyber roles undertaken. In this way, cybersecurity talents will be retained and grow by expanding the cyber teams.

The objective of this work was twofold. First to identify potential cybersecurity roles that can benefit from the skills offered by people outside of the traditional routes such as computing and IT. These cybersecurity roles were extracted from the leading cybersecurity workforce framework proposed by NIST [10] [11]. Then, this work investigated the awareness level and the interest of students studying in non-computing disciplines in a vocational college in UK, to work within the cybersecurity industry. To this end, the perception of students studying towards Computing subjects was also investigated, providing an insight as to whether they identify that professionals from other disciplines have a fit in cybersecurity and can complement existing cybersecurity teams. The outcome of this work is expected to provide an insight to both education providers and the industry as to the efforts that need to be placed to engage people, from different disciplines, with cybersecurity and address the skills shortage. Section 2 discusses related work. Section 3 presents the cybersecurity roles that have a cross-over with different disciplines. Section 4 analyses the results from the investigations performed in a vocational college in UK. Finally, section 5 concludes the work and provides future directions.

2 Related Work

In a 2020 study [3] conducted by the Department for Digital, Culture, Media & Sport (DCMS) in the UK, it was identified that 48% of UK organisations have a basic cybersecurity skills gap. Whilst over the last few years this has improved, a continued skills shortage has contributed to an ever-increasing number of successful cyberattacks on organisations. With the supply of suitable candidates for cybersecurity roles failing to meet industry demand, the cybersecurity industry needs to look at other recruitment strategies alongside its educational focus to meet its demand. Specifically, there is a need for the cybersecurity industry to consider the role of other disciplines. This is particularly important as they could contribute to the industry in ways that had not previously been considered, which in turn could have an impact when trying to manage and close the cybersecurity skills gap [4]. According to Hoffman et al. [5], by

focusing on the holistic development of a cybersecurity workforce, it is possible for an organisation to benefit from a much greater level of collaboration.

One of the problems with recruiting into a cybersecurity role is the perception that this is a technical area that is associated with computing-related studies and expertise. In a survey performed by ISC2 [4], it was discovered that amongst those questioned, 71% reported that their view of cybersecurity professionals working within the industry is that they are "smart, technically skilled individuals". The perception of cybersecurity being only for technically minded individuals will ultimately limit those interested in pursuing the subject from the outset. Currently, this stereotype has contributed to the narrow pipeline of new recruits, from different disciplines, into the subject of cybersecurity. It is for this reason that Javidi and Sheybani [6] explored in their project ways to encourage more students from a younger age to consider the role of cybersecurity in their daily life. They focused on providing cybersecurity educational training to teachers in all disciplines, to better prepare them to incorporate the subject, wherever possible, into the educational curriculums.

Even though studies, e.g. [4], indicate a strong perception regarding cybersecurity being a technically field, a shift to this mindset is required to address the cybersecurity skills shortage as indicated in a report published by Gartner [7], where it is concluded that we have passed the point in which a purely technical approach is needed. To this end, Blair et al. [8], have presented their vision on the multidisciplinary cybersecurity teams of the future, identifying a range of disciplines that have a role in the cybersecurity industry such as computing, operations research, artificial intelligence and data science, electrical and computing engineering, cognitive science and psychology, law, political science and international relations, and business. The work performed by Parrish et al. [9] also analyses a broad range of disciplines, e.g., computer science, information systems, information technology, computer engineering, software engineering, etc., that can be integrated into cybersecurity curricula and discusses how to build cybersecurity competencies for 2030 using an interdisciplinary approach. The value of building teams with complementary skills and experience, to allow organizations to manage risks effectively and holistically, is also highlighted in the latest version of the NIST Cybersecurity Workforce Framework (NICE) [11].

3 Cybersecurity roles, subject disciplines, and knowledge areas mapping

This work explored the links between the job roles defined in the NIST NICE Cybersecurity Workforce Framework [10] [11] and the vocational training offered by a Further Education (FE) and Higher Education (HE) College in the UK. The aim of NICE framework is to develop a common language for use in education and training, highlighting the interdisciplinary nature of working within the cybersecurity workspace as well as driving workforce structure and development planning [12]. The framework defines 32 areas of specialty which exist within the cybersecurity industry and are further broken down into 52 work roles.

Initially, the skills and knowledge attributes required by the job roles defined in the NIST NICE Cybersecurity Workforce Framework [10] have been analyzed. By comparing these attributes to the skills and knowledge developed in vocational training curriculums of a Further Education (FE) and Higher Education (HE) College in the UK, it was possible to identify cybersecurity roles where the skills and knowledge crossed into a range of different (non-traditional) disciplines. The identified NICE cybersecurity roles which could benefit from working alongside others with a greater variety of skills and knowledge across multiple subject domains included: Security Architect, Technical Support Specialist, Cyber Policy and Strategy Planner and Cyber Instructional Curriculum Developer. From the analysis, 8 non-traditional disciplines have been identified that present a crossover of knowledge and skills to perform the identified cybersecurity roles: Media, Art & Design, Teacher Education, Political Science, Psychology, Business, Law and Engineering.

Table 1. Cybersecurity roles, subject disciplines, and knowledge areas mapping

	Media	Art & Design	Teacher Education	Political Science	Psychology	Business	Law	Engineering
Security Architect						K0002, K0008, K0026, K0052, K0214, K0287	K0003, K0004, K0260, K0261	K0010, K0011, K0030, K0035, K0055, K0057, K0093, K0102, K0170, K0322
Technical Support Specialist						K0002, K0114, K0287, K0292, K0317	K0003, K0004, K0260, K0261	K0109, K0114, K0294
Cyber Policy and Strategy Planner				K0127, K0248, K0313		K0002, K0006, K0146, K0311, K0313	K0003, K0004, K0168, K0313	
Cyber Instructional Curriculum Developer	K0239	K0239	K0204, K0208, K0213, K0216, K0217, K0220, K0243, K0245, K0250, K0252		K0124	K002, K006, K0146, K0287	K003, K004	

Table 1 highlights the knowledge areas required for specific cybersecurity roles which can be developed in the context of the identified disciplines. The listed work roles and knowledge areas are extracted from NICE Cybersecurity Workforce framework (version 2017). The NICE knowledge areas IDs (Kxxxx) are retained.

Professionals with a Media, Art & Design background can advise on alternative ways to promote information via written, oral, and visual media, assist in the devel-

opment of media-related cyber material for education and training purposes, and communicate complex information, concepts, or ideas to different audiences. Such knowledge can benefit the role of a Cyber Instructional Curriculum Developer. This role can also benefit from the knowledge of professionals with a Teacher Education background. Teacher Education studies develop knowledge on topics such as learning levels, learning modes and assessment techniques, education processes and educational technologies. All these topics are relevant to the Cyber Instructional Curriculum Developer role as it is expected to develop, plan, coordinate, and evaluate cyber training/education courses based on instructional needs. Political Science curriculums can build knowledge on aspects such as strategic theory, cyberspace policy and doctrine, political factors that can influence regulations and the nature and function of a National Information Infrastructure, etc. A professional with such knowledge can support a Cyber Policy and Strategy Planner. Moreover, Psychology studies build knowledge on cognitive domains and on methods applicable for learning in each domain. Professionals with a cognitive psychology background can advise a Cyber Instructional Curriculum Developer, creating effective training curricula by adapting appropriate learning methods for audiences with different abilities.

As it can be observed from Table 1, professionals originating from Business backgrounds have a wider cross coverage of knowledge with cyber roles. Specifically, all roles listed on Table 1 can benefit from this discipline as people build knowledge on key cyber aspects such as risk management, customer operations, business continuity and disaster recovery processes, operational impacts, etc. Another important aspect that is essential to all roles listed on Table 1 covers knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. These topics are covered in detail by relevant Law curriculums. Finally, a discipline that can be considered technically closer to cybersecurity aspects is engineering. This can also be justified from the knowledge coverage presented on Table 1 that concerns more technical roles (Security Architect, Technical Support Specialist). People with an engineering background have a good understanding of how systems work, they can configure, integrate and troubleshoot software and hardware and are aware of relevant security threats and vulnerabilities. An overall observation stemming from Table 1, is that a significant percentage of knowledge areas can be covered from the listed disciplines.

4 Investigations

In the context of this work, a questionnaire was prepared to investigate the interest and the perception of students in a FE and HE UK college regarding the disciplines which could complement and support the work carried out by specific cybersecurity jobs. Based on the college offered degrees, 4 non-traditional disciplines (Media, Art & Design, Business, Teacher Education) from the ones listed on Table 1 have been considered, plus a traditional discipline (Computing). Ethical approval was obtained prior delivering the questionnaire. Initially, 88 participants engaged with the investigations. Specifically, 8 participants were studying towards Media, 3 towards Art & Design studies, and 20 participants were studying towards Business and Teacher Edu-

cation subjects, respectively. Finally, 37 Computing students, were engaged to investigate if they can envision collaborating with people from other disciplines to fulfill cybersecurity tasks. Participation was on a volunteer basis. The low number of participants from specific subjects, provided an initial observation as to the interest in this topic. The following section presents results coupled with relevant discussion points.

4.1 Results

Familiarity with cybersecurity and interest to work in this area.

The study began by acquiring an initial view of participants' familiarity with cybersecurity. Approximately 50% of responders reported hearing about cybersecurity from their school/college, 46% listed social media, while other sources of information included news articles (39%), family (19%), and friends (22%).

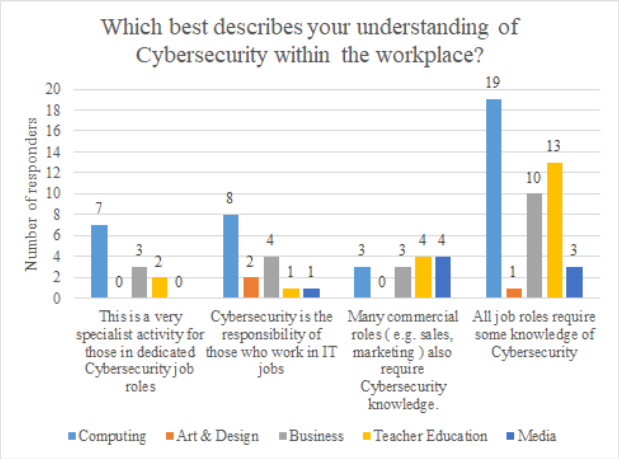

Fig. 1. Perceptions on relation of cybersecurity with workplace within each discipline

The increase in cybersecurity awareness is supported by the results shown in Fig. 1, which indicate that only 14% believe that "Cybersecurity is a specialist activity limited to dedicated Cybersecurity job roles". A high percentage (52%) of responders listed that "All job roles require some knowledge of Cybersecurity". This perception indicates that there is a growing acceptance that cybersecurity aspects touch upon job roles across industries. It is therefore critical for everyone to be involved in the topic as the current cyber threat landscape can impact people's ability to conduct their day-to-day role to a great extent. An interesting observation though is the higher percentage of students (approx. 31%) engaged with non-Computing curriculums that have this perception compared to the percentage (21%) of students following Computing studies. Investigating this observation further, one can derive from Fig. 1 more insight. There is a high percentage (approx. 40%) within people currently following a Computing curriculum who believe that cybersecurity is limited to specialist roles or it is the responsibility of those who work in IT jobs. The same perception is reported

by approximately 27% of responders from non-computing disciplines. This could indicate that the way the topic is taught outside of Computing leads to a much more rounded and generalised understanding of the subject, whereas the teaching in the Computing programs focuses more on the specialist skills and knowledge that it neglects to highlight the role of other disciplines. These initial findings would indicate that cybersecurity programs within Computing curricula need to highlight the need to work with professionals having different backgrounds.

Students were also asked to "Rate on a scale of 1 (extremely unlikely) to 10 (extremely likely), how likely are you to consider a job in Cybersecurity?". Computing students indicated that they would be 'Somewhat likely' to consider a job in this industry (Mean=7.49). Students from the Media (Mean=3.13), Art & Design (Mean=3) and Teacher Education (Mean=3.7) disciplines reported that they would be 'Very unlikely' to consider a job in this industry. Business students appeared to have a 'neutral' feeling towards the idea of working in this industry (Mean=5.05), further investigations though indicated that there were 2 clusters, one interested and one not that interested in working in cybersecurity. Also, a few students from Teacher Education reported their strong interest in working in this area, which was an encouraging observation even though the majority reported otherwise. Overall, the interest of non-computing disciplines was low, highlighting the need to make more efforts to engage these disciplines with cybersecurity. Note that this aspect was measured before any clarity was provided to students as to how their skills can be utilized in cybersecurity.

Perceptions on subject disciplines relevant to cybersecurity jobs.

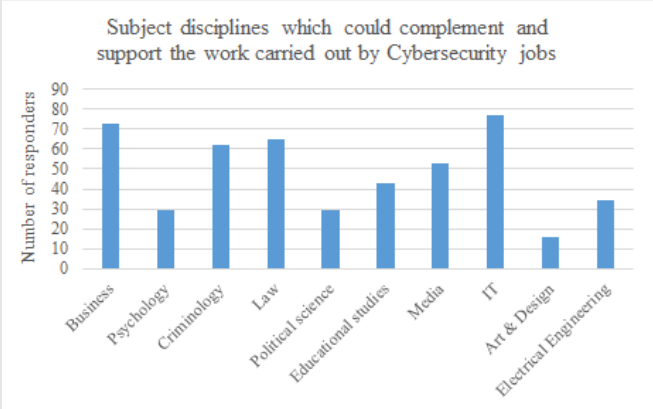

Fig. 2. Subject disciplines relevant to Cybersecurity jobs

An important aspect of this work was to investigate whether students can identify potential aspects of collaboration between people originating from different disciplines. The study required the students to read the brief job descriptions of the 4 NICE cybersecurity job roles listed on Table 1, and select all the disciplines (Fig. 2) they believed would have some crossover with the cybersecurity jobs described. Fig. 2

demonstrates that most participants saw an important role for IT and Business professionals in supporting the job functions described, with a significant number of participants also suggesting a role for those who have studied Criminology, Law and Media. However, it is noted that participants saw less of a role for Art & Design, Psychology, Political Science and Electrical Engineering within the Cybersecurity industry. This may be due to a lack of insight into the value that these disciplines may bring in cybersecurity. The role of other disciplines should be addressed as part of cyber awareness programs, highlighting how they could support cybersecurity, and addressing issues such as human error, message delivery and systems design and installation.

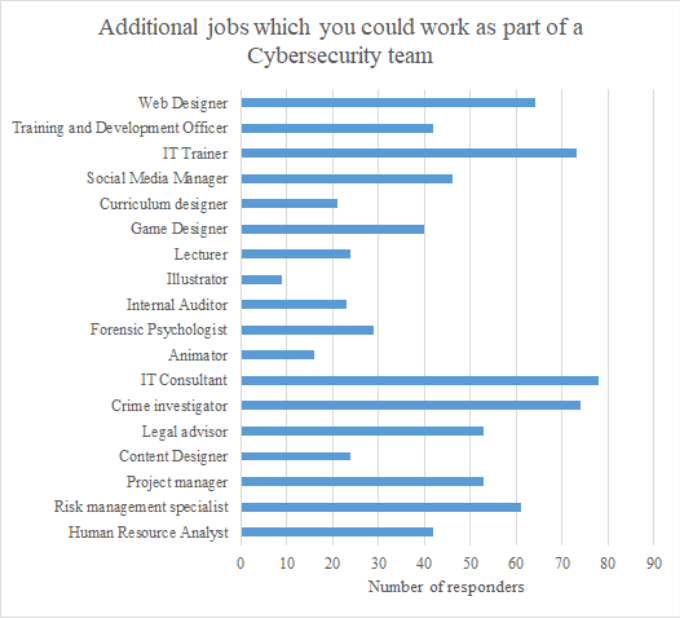

Fig. 3. Other jobs that can complement a cybersecurity team

Fig. 3 shows a breakdown of job titles related to the disciplines listed in Fig. 2. Students had to select the jobs which could work as part of a cybersecurity team. Interestingly, the results show a similar response to the results in Fig. 2, in that the highest rated jobs relate to IT, Business, Criminology and Law. However, it was surprising to observe that Media roles, e.g., social media manager, game designer, etc., received less attention compared to the higher number of responses reported in Fig. 2 and acknowledging this discipline. Moreover, participants provided low responses related to Curriculum Designer and Lecturer roles, even though more participants listed Educational Studies as a discipline that can complement cybersecurity. This could indicate a general misunderstanding about the type of roles different programs of study could lead to. Another surprising observation is that the Training and Development Officer received more responses compared to relevant roles such as a Curriculum Designer

and Lecturer. This could also indicate lack of knowledge as to how these roles are related and how they can completement cybersecurity teams.

Current competencies in cybersecurity.

Moving on, participants were asked about their competencies developed in their programme of study and whether they can help them work in cybersecurity (Fig. 4).

Fig. 4. Students' perception on current skill set and relevance to cybersecurity

Fig. 4 demonstrates that most of the Computing and Business students feel that the skills and knowledge developed would help them to gain employment in the Cybersecurity industry. To some level, this was expected due to relevant cybersecurity topics that are typically taught in these curriculums. The surprise result came from the other discipline students, especially those in the Teacher Education that did not feel that the skills and knowledge developed in their studies complement Cybersecurity roles. This observation contrasts the strong indication from Fig. 2 that Educational Studies would complement Cybersecurity roles. A positive note, when students were asked whether they are interested in learning more about cybersecurity and relevant roles within their current studies, the majority (approx. 86%) of students answered positively.

5 Conclusions & Future Directions

With the cybersecurity industry continuing to grow at a pace faster than the skills gap can be addressed, developing multidisciplinary teams can assist in addressing this issue and empower organizations to better defend and keep up with a dynamic cyber threat landscape. The initial investigations from this work, indicated that there seems to be very little interest from students outside of those currently studying a Computing course, to work in cybersecurity. In addition, this work established that there was a lack of clarity on how the skills and knowledge developed in vocational courses across a range of disciplines can be translated into a career in the cybersecurity industry. To address these findings, it is recommended that educational facilities start to

explore projects between the departments identified in this report to foster a better understanding of the relationship between the different disciplines and cybersecurity. An example of this could be the creation of a cybersecurity awareness campaign, with the cybersecurity content being co-authored by students from Business and Computing and the key content being converted into graphics by students in Media and Art and Design for use on social media. By exploring the topic together in this way, it would have the benefit of providing practical demonstrations about how the disciplines could work together. By building cybersecurity synergies between different disciplines, this approach will assist over time in identifying opportunities for those studying in alternative disciplines to enter an industry where there is a significant skills shortage, with fantastic career opportunities.

References

1. Hakak, S., Khan, W. Z., Imran, M., Choo, K. R., and Shoaib, M.: Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies, *IEEE Access*, vol. 8, pp. 124134-124144, 2020.
2. Muncaster, P., Two-Thirds of CISOs Struggling with Skills Shortages, 2020, https://www.infosecurity-magazine.com/news/twothirds-of-cisos-struggling/
3. Department for Digital, Culture, Media & Sport. Cyber security skills in the UK labour market 2020, https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020
4. ISC2: How Views on Cybersecurity Professionals Are Changing and What Hiring Organizations Need to Know, 2020, https://www.isc2.org/-/media/ISC2/Research/2020/Perception-Study/2020ISC2CybersecurityPerceptionStudy.ashx, last accessed 25/04/2021
5. Hoffman, L., Burley, D., Toregas, C.: Holistically building the cybersecurity workforce. *IEEE Security and Privacy*. 10(2), 33–39, 2012.
6. Javidi, G., Sheybani, E.: K-12 Cybersecurity Education, Research, and Outreach. *IEEE Frontiers in Education Conference (FIE)*, pp. 1-5, 2018.
7. Gartner: The Urgency to Treat Cybersecurity as a Business Decision, 2020.
8. Blair, J.R.S., Hall, A.O., Sobiesk, E.: Educating Future Multidisciplinary Cybersecurity Teams. *Computer*. 52(3), 58–66, 2019.
9. Parrish, A., Impagliazzo, J., Raj, J. K., Santos, H., Asghar, M. R., Jøsang, A., Pereira, T., Stavrou, E.: Global perspectives on cybersecurity education for 2030: A case for a meta-discipline, In: Proc. 23rd Annual ACM conference on Innovation and Technology in Computer Science Education, Larnaca, Cyprus, 2018.
10. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework. *NIST Special publication* 800-181, 2017.
11. Petersen R., Santos, D., Wetzel, K., Smith, M., Witte, G.: Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181, Rev. 1, 2020.
12. Paulsen, C., McDuffie, E., Newhouse, W., Toth, P.: NICE: Creating a cybersecurity workforce and aware public. *IEEE Security and Privacy*. 10(3), 76–79, 2012.