2022

Future Needs of the Cybersecurity Workforce

Connie Justice
IUPUI

Char Sample
Boise State University

Sin Ming Loo
Boise State University

Alex Ball
Boise State University

Clay Hampton
IUPUI

Publication Information

Connie Justice; Char Sample; Sin Ming Loo; Alex Ball; and Clay Hampton. (2022). Future Needs of the Cybersecurity Workforce. In R.P. Griffin, U. Tatar, and B. Yankson (Eds.), *Proceedings of the 17th International Conference on Cyber Warfare and Security, 2022* (pp. 81-91). Academic Conferences International Limited. https://doi.org/10.34190/iccws.17.1.33

Future Needs of the Cybersecurity Workforce

Connie Justice[1], Char Sample[1,2,3,4], Sin Ming Loo[4], Alex Ball[4] and Clay Hampton[1]
[1]Purdue School of Engineering and Technology, IUPUI, Indianapolis, USA
[2]MTSI, Alexandria, USA
[3]SABSA Institute, UK
[4]Boise State University, Boise, USA
cjustice@iupui.edu
char.sample@mtsi-vai.com

Abstract: Expected growth of the job market for cyber security professionals in both the US and the UK remains strong for the foreseeable future. While there are many roles to be found in cyber security, that vary from penetration tester to chief information security officer (CISO). One job of particular interest is security architect. The rise in Zero Trust Architecture (ZTA) implementations, especially in the cloud environment, promises an increase in the demand for these security professionals. A security architect requires a set of knowledge, skills, and abilities covering the responsibility for integrating the various security components to successfully support an organization's goals. In order to achieve the goal of seamless integrated security, the architect must combine technical skills with business, and interpersonal skills. Many of these same skills are required of the CISO, suggesting that the role of security architect may be a professional stepping-stone to the role of CISO. We expected degreed programs to offer courses in security architecture. Accredited university cyber security programs in the United Kingdom (UK) and the United States of America (USA) were examined for course offerings in security architecture. Results found the majority of programs did not offer a course in security architecture. Considering the role of the universities in preparing C-suite executives, the absence of cyber security architecture offerings is both troubling and surprising.

Keywords: cyber security, security architect, CISO, education, workforce, Zero Trust Architecture (ZTA)

1. Introduction

Cyber Security education is facing an inflection point. Currently, there are 464,420 unfilled cybersecurity jobs (Cyberseek heatmaps) and the nature of the growth of these jobs suggests additional skills that are not being addressed in degreed cybersecurity programs. Cybersecurity is possibly in the strongest position to continue growing through proposed changes in course curricula, to accommodate changes in employers' needs. The research introduced in this manuscript compares curricula of UK and US universities to identify the percentage of universities with course offerings in cybersecurity architecture. A cyber security architect is a senior-level professional responsible for designing complex cyber security solutions synthesizing technology, management, and interpersonal skills within an organization (Cyber Degrees, n.d., Sherwood Applied Business Security Architecture, n.d.). Thus, the dearth of security architecture course offerings was not initially noticed. However, the growth of the cloud for site hosting along with the growing acceptance of Zero Trust Architecture (ZTA) implementation could exacerbate the skills gap.

Cyber Security programs continue development across universities creating their own academic silos in response to growing workforce demands for cyber security professionals (Cyberseek heatmaps, State of Cybersecurity, 2021, Cybersecurity Jobs Report, 2021). Strong industry growth justifies this increased pattern in cyber security programs. Current industry trends show millions of job openings by the year 2020/2021 (Cyberseek heatmaps). In ISACA's State of Cybersecurity Part 1. 61% of employers stated that they were significantly or somewhat understaffed (State of Cybersecurity, 2021). However, with the rise of artificial intelligence and machine learning (AI/ML), the distribution of jobs will likely change even if the number does not.

University cyber security educational programs continue turning out specialists supporting the market demand, creating entry-level penetration testers, assessors, auditors, and reverse engineers (Peltsverger 2015). Cybersecurity departments are common in most university curricula and will likely remain in place for some time. The field of cybersecurity has plenty of job openings providing university programs the opportunity to train students and enabling the achievement of high employment metrics.

However, cybersecurity professional demands continually change along with the virtual landscape. These changes require cybersecurity professionals to continually update their skillsets. Changes in both technologies and service offerings can outpace curricula development and deployment in many university programs. The time required to move from course envisioning to course delivery varies per institution but fails to keep pace with

industry's changing landscape. What is needed are course offerings in cybersecurity that teach students transferable skills (i.e.. critical thinking, systems thinking) that can be applied in any situation, while allowing students to remain current in technologies and services.

The 2018 New Approaches to Cybersecurity Education (NACE) workshop in New Orleans, LA emphasized the need for diversity of thought with critical thinking skills regarding cybersecurity curricula (NACE, 2018, Cybersecurity Jobs Report, 2017). The workshop's papers recognized the need for cyber security programs to expand beyond the computer science departments, computer technology, computer engineering, and information science departments, and to even think beyond traditional science, technology, engineering, and math (STEM) disciplines. Hence, the recognition of the importance of both critical and adaptive thinking suggests cyber security programs, particularly those that offer an interdisciplinary approach, may be better positioned than others to adequately deal with the changing landscape and position students to become cyber security architects (Ramirez 2017).

A growing faction of cybersecurity scholars and academics have observed the need to break down silos and are also calling for interdisciplinary approaches to solving cyber security problems (Peltsverger 2015) that position students well in the areas that a well-rounded cyber security architect requires. Disciplines such as law, psychology, sociology, business management, resilience, reliability, statistics, data science, international studies, and others are becoming increasingly intertwined with cyber security (Ibid, 2015). Several initiatives exist to provide cyber security curricular guidance such as The Department of Homeland Security (DHS) and the National Security Agency (NSA) who jointly sponsored the National Centers of Academic Excellence (CAE) program and The Joint Task Force on Cybersecurity Education (CSEC2017), and the NIST National Initiative for Cybersecurity Education (NICE). These programs focus on curricula as an interdisciplinary path of study (Joint Task Force on Cybersecurity Education 2017, Cybersecurity Jobs Report 2017, National Initiative for Cybersecurity Education (NICE)). The response of the various university cyber security programs has been mixed. This response is understandable since agreement to break down the academic silos requires less effort than the act of integrating the disciplines.

One potential measure of a program's readiness to engage in updating curricula to reflect the impending new reality is the offering of security architecture courses. A Security Architect is defined for the purposes of this paper as a top-tier cybersecurity professional designing, directing, and overseeing cybersecurity and network security for the entire business entity (Cybersecurity Jobs Report 2017). Traditional architects combine knowledge from various disciplines in order to design structurally sound buildings (Savold et al. 2017). Similarly, security architects use skills learned in other disciplines to create robust network security solutions supporting organizational goals. Creating strong defensive networks in support of a mission requires a mix of breadth and depth in the skill set of the network architect (Triolo 2014). This research analysis of university cyber security programs in the US and UK provides the findings of one measure of preparedness, the offering of security architecture classes, for future requirements.

2. Background

2.1 Cybersecurity Workforce

Study international (2021) not only showed continued growth for all of cybersecurity but specifically mentioned skills that require building in security across all layers, "from the ground up" (Ibid 2021). This differs from the old approach where professionals were simply told to 'think like a hacker' (Sternstein 2012). The problem with the 'think like a hacker' approach is that in many cases students learned to think like a hacker at the expense of thinking like a defender, a good cybersecurity professional needs to do both.

In addressing this need, The National Initiative for Cybersecurity Education (NICE) led by the National Institute of Standards and Technology (NIST) formed a partnership of government, academia, and the private sector (National Initiative for Cybersecurity Education (NICE)). The partnership's mission is to increase the number of cybersecurity professionals to secure our national infrastructure by building on existing cybersecurity successful programs, highlighting innovation, and collaborating with all stakeholders to ensure current and future cybersecurity challenges are met. NICE has four communities of interest, Apprenticeships in Cybersecurity, Cybersecurity Skills Competitions, K12 Cybersecurity Education, and NICE Framework Users. The purpose of the NICE communities of practice is to provide a means for private and public sectors to come together and drive

change advancing cybersecurity education, training, and workforce development (National Initiative for Cybersecurity Education (NICE)).

2.2 The NiCE Framework

The NICE Framework perceives competencies as identified by employer or educator and assesses the students' ability to meet the competency (e.g. do the work) figure 1. Consequently, competencies are grouped by task, knowledge, and skill (TKS) statements. Therefore, competencies are employer-driven, focus on the student, and are observable and measurable.

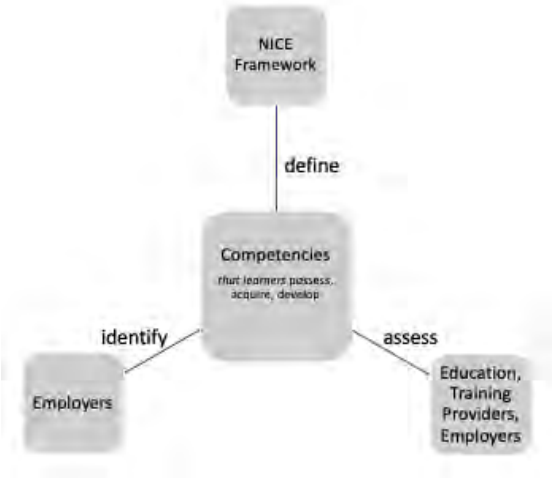

Figure 1: NICE Framework (NICE, n.d.)

The Association for Computing Machinery (ACM) assembled a Joint Task Force on Cybersecurity Education (CSEC2017 2017) to address the need for education to aid in workforce development. CSEC2017 is based on several curricular frameworks and is designed in part using the U.S. National Research Council Next Generation Science Standards (CSEC2017 2017). The CSEC2017 views cybersecurity education grounded in scientific, computing, and cybersecurity principles that are continuously refined using evidence-based practice (CSEC2017 2017). Figure 2 shows the CSEC thought model. The knowledge areas depict the critical knowledge over a broad range of computing disciplines, and it is the basic structure of the model. The knowledge areas represent all knowledge within the cybersecurity discipline. The CSEC 2017 links to the NICE workforce framework as cybersecurity educational needs are unique due to the balancing of breath in overall cybersecurity knowledge, depth in a specific area, and aligning the educational needs with workforce demands (Raj et.al. 2018).

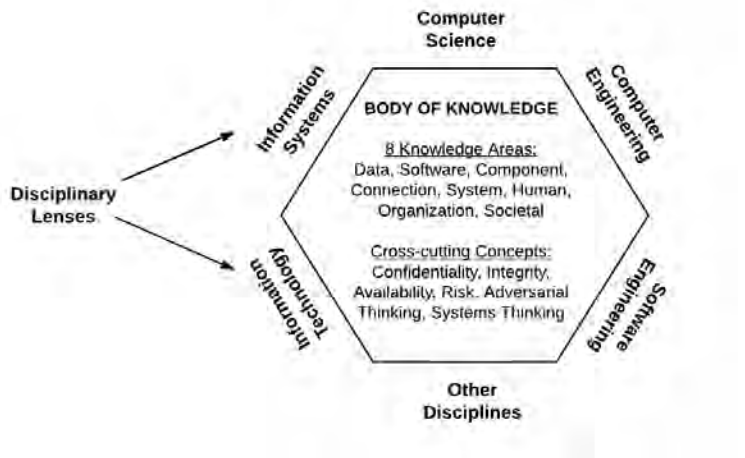

Figure 2: CSEC 2017 Thought Model (CSEC2017, 2017)

Another example of meeting the need for the cyber workforce is the National Security Agency (NSA), Department of Homeland Security's (DHS) partnership in the Centers of Academic Excellence (CAE). The CAE supports NICE in creating a pool of skilled workers able to protect the nation. Hiring skilled cybersecurity professionals to protect critical infrastructures, information systems, and networks is a top priority for

governments and businesses globally (Centers for Academic Excellence (CAE)). DHS provides tools, resources, and education aimed specifically at building the strength and sustainability of the cyber security workforce. DHS is working hard to retain current talent while filling the gaps by offering competitive bonuses and salaries in line with private businesses. Additionally, DHS provides a workforce tool for all companies to utilize identifying critical gaps in cyber security personnel (Centers for Academic Excellence (CAE)). The DHS Workforce development Lifecycle depicted in figure 2 is comprised of:

- Cybersecurity workforce identification and quantification
- Understanding workforce needs and skills gaps
- Hiring the right people for clearly defined roles
- Enhancing employee skills with training and professional development
- Creation of programs and experiences to retain top talent

Figure 3: DHS Workforce Development Lifecycle

More recently cloud migrations have resulted in a need for security architects. Organizational migration to the cloud is not new, Amazon, Microsoft, and Google have had offerings for years (Miller 2016; Harvey 2017; Foley 2018). Cybersecurity professionals were initially hired to identify risks in the cloud environment; however, more recently these same professionals have been asked to create solutions that enhance business workflows to allow for secure business processing. These solutions require the professional to go beyond thinking like a hacker, to thinking like a security architect, which requires an interdisciplinary skill set and mindset.

2.3 Academia's Response to Workforce Demand

One reason for the existence of academia silos can be explained through the research on the building of expertise that occurs by focusing on a specific discipline at the cost of exclusion of others. Studies are purposefully tightly restrained to allow the researcher to focus on a specific problem. Variables are limited, so results or findings can be generalized for applications where the same variables appear in different environments. Thus, cyber security, a discipline with underpinnings in computer science and mathematics, would naturally follow the same structural pattern. This ultimately leads to cyber security professionals who are conversant in technical speech but are less able to effectively comprehend or communicate with other disciplinary groups (i.e., management, marketing, etc.) found a typical work environment. In many cases, cybersecurity professionals are hackers who are quite skilled at breaking into systems and networks, but less skilled at building secure solutions (Bishop 2018).

Cyber security programs responded to the industry's demand for specific technical skillsets, and this approach showed initial successes resulting in the global growth of new programs. However, like nursing where professionals initially took care of the patient's immediate needs, programs evolved to include increasing numbers of courses and disciplines (psychology, chemistry, sociology, kinesiology, etc.) in order to better prepare nurses for their jobs. So too, cybersecurity curricula must evolve to include additional disciplines with the goal of improving students' overall performance for the future workplace, through understanding the various viewpoints necessary to architect strong security solutions.

Teaching students how to architect strong security solutions expands the training boundaries beyond technology to understand business processes, organizational and individual behaviors. The security architect must be able to put forth the various views of the solution system, that covers how each user understands their interaction

with the designed security solution while executing their role in the business process workflow (SABSA, DoDAF, TOGAF.). The interdisciplinary requirements associated with security architecture demands more than traditional technology knowledge from the cybersecurity professional. University programs are tasked with creating agile thinkers, yet many of the exercises focus more on tactics, tools, and procedures which are more consistent with training rather than reflective thought.

Security architecture work continues to change in support of growing security requirements that reflect the cloud-based architectures. The interdisciplinary nature of security architecture work is well-suited for course development and delivery that blend technical and behavioral disciplines. This mix of skills is compounded in the virtual environment which offers flexible capabilities, but these capabilities also introduce additional security challenges (Rose, Borchert et al., 2020). One way of creating security solutions in this cloud is the adoption of Zero Trust Architecture (ZTA) concepts. ZTA's assumption of a compromised hostile environment presents additional challenges to designing and integrating new secure architectures (Ibid). Thus, students and course developers have an opportunity to use and refine interdisciplinary skills (law, finance, psychology, sociology, data science, computer science, information science, etc.). However, students need coursework that teaches the inner workings of technologies, business processes, and other disciplines in order to design ZTA compliant solutions.

This failure to adequately support other disciplines further isolates cyber security professionals and may limit students to becoming industry commodities. Commodities are quickly acquired and discarded, making for career-limited growth options. AI enabled tools promise to exacerbate the commodity problem. Robots powered by AI to perform hacking are a cheaper option than humans. To ensure cybersecurity students are educated and trained to meet the needs of the cybersecurity workforce it is crucial to structure cybersecurity programs for future interdisciplinary growth.

3. Problem Statement

The interdisciplinary nature of cybersecurity increasingly suggests the need to restructure cyber security programs away from the silo approach and into the interdisciplinary approach. The general problem facing educational institutions, and students is accredited programs may not adequately prepare students for cybersecurity workforce challenges where diverse skill sets are becoming increasingly important. Specifically, the universities are focusing on technical rather than the holistic education of the cybersecurity learner when the workforce has a growing need for the holistic cybersecurity professional-the cyber security architect (Cyber Degrees). Universities need to develop a holistic cyber security architect program to meet the future cybersecurity demands in the job force.

The interdisciplinary nature of security architecture provides an attractive means to fuse together the traditional technology programs with other disciplines. In order to determine the best technical solution to a problem, the problem must first be well understood. Security architects are tasked with bringing together the various stakeholders to gain a greater understanding of their views and risk tolerances, *before* making technical recommendations (Sherwood Applied Business Security Architecture, n.d., DoDAF Architecture Framework Version 2.02, n.d.). This experience in practical application of solutions learned through various courses in both the undergraduate and graduate programs exists in some universities but not all programs. This led the researchers to ask the question, how many programs offer security architecture courses?

4. Research Method

This study with the resultant analysis is exploratory in nature. The goal is to determine the rate of programs offering security architecture courses. Thus, this study is a preliminary data collection effort over 2 two countries (US & UK) that seeks to answer a simple question, what percentage of university-based cybersecurity programs offer a course in security architecture? The researchers hope to use this initial study as a launching point for additional studies in education course curricula. The study is limited to university programs that are accredited by their respective country's accreditation agencies. Certificate programs, junior colleges, and community colleges were exempted from this study.

One reason why this study was limited to university programs is the knowledge requirement of a security architect (CSEC2017, Peltsverger 2015). As previously mentioned, security architecture requires knowledge of both security technology, information technology in general, and business processes required to support the

organization's mission (CSEC2017, Peltsverger 2015); therefore, the professional engaged in this line of work will possess professional experience. The experience associated with security architecture should not serve as a deterrent to the various cyber security programs since all programs surveyed offered courses in security policy and management of security professionals, both areas with strong experience requirements. Data collection relied on querying the individual institutionally owned websites discovered through the countries' accrediting agencies. Furthermore, training courses while offering good technology experiences lack the much-needed context that provides the experiential component that students desperately need.

5. Results

All data presented was based on data obtained from the UK and US accredited cybersecurity programs with data extracted in October 2021. What was discovered was that many universities did not call the courses cyber security architecture, nor did they call the course security architecture. Few universities offered cyber security architecture or security architecture courses. If we noticed any of those courses in the data, we noted the name. The overall rate for US accredited universities was 215 and the overall rate of UK universities was 75. The sample set for the US was N=215 and UK N=75. 13 universities in the US offered a security architecture course and 202 universities had no security architecture course. Conversely, four universities in the UK offered security architecture courses and 69 did not offer a security architecture course.

2021

Country	Architectural courses offered				Course not offered	Unable to discern	Total
	General	Enterprise	Computer	Security			
UK	0	1	0	4	69	1	75
UK (%)	0%	1.33%	0%	5.33%	92%	1.33%	
US	41	22	98	13	40	1	215
US%	19.10%	10.20%	45.60%	6.00%	18.60%	0.47%	

Other interesting discoveries were made through the course of this research. There were accredited programs in cybersecurity that did not possess a degree in cybersecurity or courses in security architecture. Some of the architecture courses that were not counted did not fit the definition of security architecture course such as skills learned in other disciplines to create robust network security solutions supporting organizational and a mix of breadth and depth in the skill set of the network architect (Triolo 2014). The courses were more hardware architecture oriented or software architecture oriented. There were courses such as systems architecture, network architecture, PC architecture, and software architecture. These courses did not have anything in common with the security architect course that is recommended by the authors. Additionally, some programs showed research only security focus and no focus on the interdisciplinary security required of the security architect (Ramirez 2017).

5.1 Proposed Solutions

There are several potential solutions to the cyber security architect problem and each one warrants discussion. The proposed solutions are not limited to those discussed here and are likely highly situational. In some cases, some institutions may find some programs unworkable, for this reason, these are suggestions, not requirements.

- Create a liaison position in the departments that interacts with other disciplines. This approach would entail hiring a liaison who reaches out to different departments and works to define the necessary courses to make cyber security a joint major with the available disciplines.
- Embed departments together to work on a common goal. An example of this approach occurs at Cardiff University in Wales where criminal justice, cyber security, data science, psychology, computer science exists in teams that work together in solving common research problems. Another example can be seen at Bournemouth University where the psychology department is co-located with the cyber security department where research into decision science in cyber security explores and answers questions in risk and trust related behaviors (www.bournemouth.ac.uk).
- Require cyber security to be a dual major or joint major at the undergraduate level. This would force cyber security students to understand how cyber supports other disciplines and communicate with personnel in a manner demonstrating an understanding of the discipline.
- Create distinct curriculum for cybersecurity majors including, but not limited to; cybersecurity risk assessment, creating policies, third party risk, and network security architecture.
- Create a cybersecurity department for all disciplines and require students to take the common core cybersecurity curriculum before taking curricula in specific disciplines. See figure 3. Additionally, create

common cybersecurity core curriculum before discipline specific curriculum and midway or end of discipline specific curriculum, see figure 4.

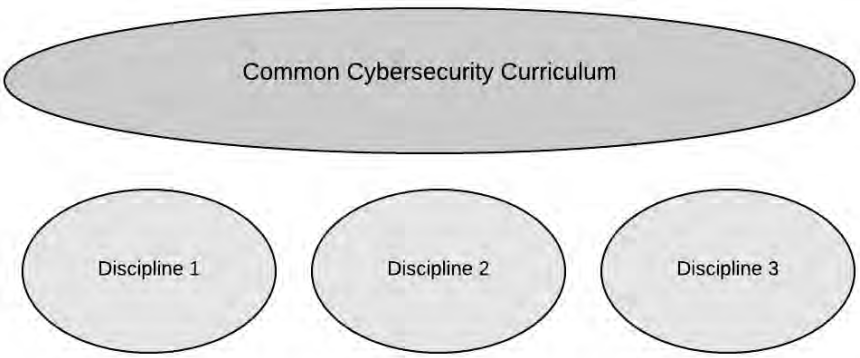

Figure 4: Common cybersecurity curriculum before specific discipline curriculum

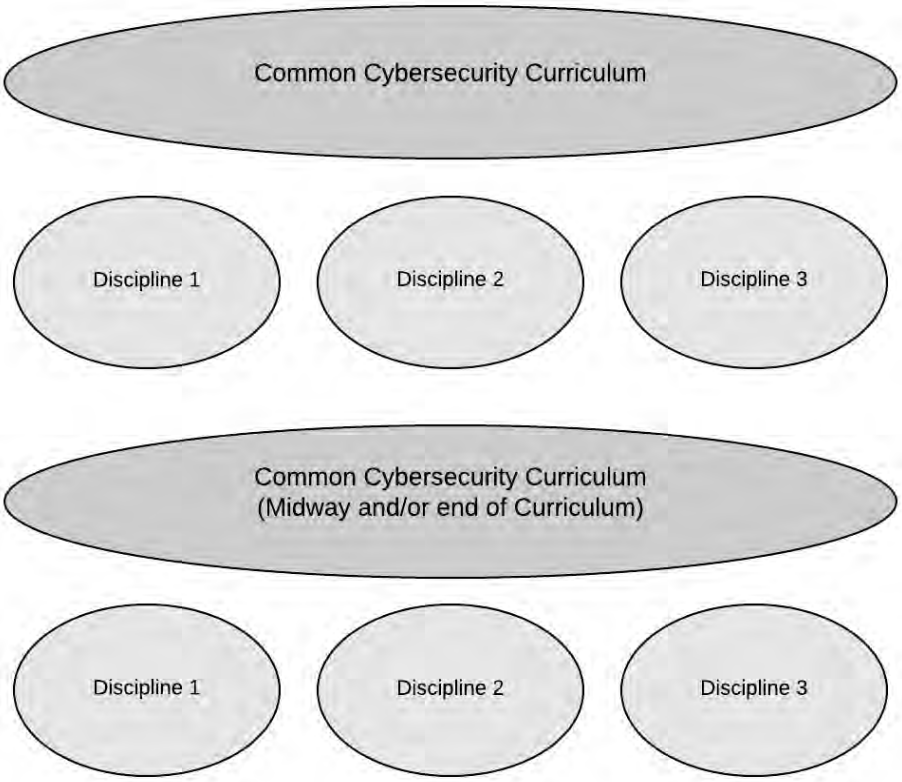

Figure 5: Common cybersecurity curriculum before and midway and/or end of specific discipline curriculum

5.2 Cybersecurity Bachelor's Degree (BS)

A new cybersecurity Bachelor of Science degree was created as a result of the research conducted in this manuscript. The degree was approved in the spring of 2021 and was available to students in the fall of 2021. The degree was based on figure 4 above with a common cybersecurity curriculum and disciplines/concentrations. The degree was initially built with courses that exist in the program, with the intent to build out concentrations in the coming semesters.

The plan of study is clustered as follows: primary cybersecurity courses, foundational cybersecurity courses, elective cybersecurity courses, and general undergraduate courses. The BS in cybersecurity is a 120 undergraduate credit requirement. The breakdown of the 120 credits is as follows:

Students must complete:

- 27 credits of Primary Cybersecurity courses (Concentration Courses)
- 36 credits Foundational cybersecurity courses
- 9 credits from the combined lists of primary cybersecurity, elective cybersecurity, and foundation cybersecurity courses
- 38 credits from general undergraduate courses and electives
- 10 credits of Leadership courses

Currently, there is only one concentration, the technical cybersecurity concentration. During the fall of 2021, two to three concentrations will be planned for the fall of 2022 semester. Ideas for concentrations to be considered are policy, education, psychology, ethics, communication, and linguistics. Along with the concentration, courses that will be added to the cybersecurity BS. are cyber security architecture and zero trust architecture.

5.3 Security Architecture Design

Security professionals are frequently reminded to "bake in" security, not "bolt it on" (Applegate, 2013). The IT industry still has many challenges in designing security from the start. Oftentimes, security is addressed after the fact and the system is heading towards production. Also, there ought to be better guidance for individuals creating requests for proposals (RFP), where the government sends out RFPs with security being addressed at later times in the design process. This security by design must be engineered to the environment, and the security solution supports processes from the very start. Typical cyber security architects in the field gain knowledge and experience from on-the-job experiences and this takes several years to attain. Designing security into the project requires other disciplinary knowledge outside of the traditional technical areas.

5.4 Robust Offensive and Defense Skills

Specialized roles such as penetration testers and reverse software engineers provide an entry point into an organization, but not professional growth opportunities. Triolo (2014) noted attackers need to be correct once and defenders need to be correct every time. A certain set of skills must bridge the gap between attacker skills and defender skills, these skills are often found in integrators who may have obtained the skills through experience or coursework.

5.5 Capture the Flag Training and Exercises

Many universities and colleges participate in capture the flag cyber challenges requiring participants to act as both attackers and defenders (Manson & Pike 2014; Murphy & Murphy 2013). These exercises are primarily focused on vulnerability exploitation, with prevention being covered as a reaction to attack signatures (Manson & Pike 2014; Murphy & Murphy 2013). In some cases, the cyber challenges require teams to build resilient solutions, but once again these solutions are designed to withstand known attacks in general. Creating and building defenses, in this arrangement, becomes an ad-hoc process that lacks rigor.

As an example, in the NACE workshop Bishop (2018) proposed creating "build the flag", a new twist on capture the flag competitions as a way to broaden and strengthen the knowledge, skills, and abilities of participants. The idea of build the flag would enhance the cyber security architect curriculum by building entire systems from the ground up to meet specific requirements given. The focus is to design and build systems with security in mind bringing together all learning acquired (New Approaches to Cybersecurity Education (NACE) Workshop, 2018). The build the flag exercise that incorporates ZTA principles could serve as a competition or even a capstone project for students that would offer an alternative capable of appealing to non-traditional cyber students.

5.6 Management Skills

In Henry's, "Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements" paper, he discusses the Cyberspace Education Framework in which broad high-level educational objectives were narrowed to show key outcomes for specific cybersecurity activities (Henry, 2017). Such activities were then applied to cybersecurity knowledge, skills, and abilities (KSAs) in management. The important takeaway from this approach is that cybersecurity is multi-faceted, multi-dimensional, and purpose specific. The topics of study

included high-level and mid-level management as well as project management. According to Trilling 2018, cybersecurity professionals are usually excellent in technical skills, and then as they progress in their occupation, they are moved into managing without any training or education in the discipline. Businesses require skilled and prepared managers.

5.7 People Skills

The ability to communicate with people and articulate cybersecurity problems and issues; educate the workforce in cybersecurity dangers to protect company assets; and communicate and work with other employees and customers to improve the security posture of the company. Soft skills, specifically communication, was described as a critical skill that a cybersecurity professional needed to possess (Hartley et. al. 2017; Jones et. al. 2018; Yuan et. al. 2017). Jones et. al's paper asked the specific question concerning what soft skill is important to your job and communication was number one. Under communication was written communication, public speaking, presenting, and collaboration (Jones et.al 2018).

6. Recommended topics for the Cyber Security Architect

"Security architects design, build, and oversee the implementation of network security for an organization" (Cyber Degrees). The security architect is entrusted to create a solution reflecting a deep technical knowledge of security products, applications, and operating systems, and how to integrate those products in support of organizational goals. Solutions are complex and must work (Ibid). The mix of technical skills, management skills, and people skills are unique. Introducing this mix of skills in cyber security programs as a foundational course would provide a foundation for a wider path of experiences for students. This section introduces some concepts and/or ideas for content relevant for cyber security architects such as security architecture design; robust offensive and defensive skills; and capture the flag training and exercises. This is just a representation and is not inclusive of all that is available.

7. Conclusions

The changing nature of problems requiring interdisciplinary approaches to cyber problems will force change in educational institutions' programs. Higher education is in danger of falling behind in the race to educate future cybersecurity professionals (Knapp et.al. 2017). These changes will need to recognize the importance of other academic disciplines in creating the next generation of cyber security professionals. This paper identified and measured a gap in cyber security education and put forth suggestions to offer potential ways forward by educating students on cyber security architecture.

A potential side benefit to adding coursework in security architecture for students is that they are better prepared to speak in terms that potential employers understand while still maintaining their technical terms. These skills would, in turn, make students more valuable to employers. Institutions that succeed in this endeavor will also distinguish themselves with employers

8. Future Work

Future work would include extending the to all universities in the UK and in the US, not just the programs that are accredited by their respective country's accreditation agencies. Additionally, it would benefit the research if it were to include certificate programs, junior colleges, and community colleges as part of the study. Further future work on this topic will include defining curriculum across multiple disciplines for the cyber architect. Universities and colleges will need to develop programs from the undergrad to the doctorate level to meet the cyber architect degree requirements. Cyber architect work should be reviewed for the role across multiple industries including the DOD space.

Another item for consideration is reviewing the role of the system engineer and morphing this role into a cyber architect position. A review of current system engineer degrees and curriculum should be performed to determine the path to a cyber architect. System engineers typically move to a cyber position, so it would be beneficial to universities and colleges to review this path as well.

Another aspect that will create new AI related jobs in the cybersecurity field and for cyber architects is the concept of the Fourth Industrial Revolution where quantum computing, AI, precision medicine, 3-D printing, AI, autonomous vehicles, Nanotechnology, Neurotechnology; LIFI, high-speed bi-directional network/mobile communications using light, energy capture, storage, and transmission; geoengineering; blockchain;

development of advanced materials; additive manufacturing (3D Printing) and multidimensional printing; virtual and augmented realities; and space technologies will create new technical jobs (Schwab 2018). These new technological endeavors singular or combined will create new jobs and expand technological responsibilities for old ones. All of which will create new cybersecurity functions and applications.

References

Become a security architect, Cyber Degrees, Retrieved from https://www.cyberdegrees.org/jobs/security-architect/

Cybersecurity Jobs Report: 3.5 Million Openings In 2025. (n.d.). Retrieved November 14, 2021, from https://cybersecurityventures.com/jobs/

Cybersecurity Skills Gap, 2016. Centers for Academic Excellence (CAE) https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

Cyberseek Heat Maps https://www.cyberseek.org/heatmap.html

DoDAF Architecture Framework Version 2.02. https://dodcio.defense.gov/library/dod-architecture-framework/

Hartley, R., Medlin, D., and Houlik, Z., 2017. Ethical Hacking: Educating Future Cybersecurity Professionals. In Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 3857).

Harvey, C. 2017, May 25. "Google cloud platform: History features & pricing" website: https://www.datamation.com/cloud/google-cloud-platform/

Henry, A., 2017. "Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements" ACCS discussion, Australian Centre for Cyber Security, UNSW, paper no. 4, August 2017.

Joint Task Force on Cybersecurity Education, Cybersecurity Curricula 2017 (CSEC2017). Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Jones, K.S., Namin, A.S. and Armstrong, M.E., 2018. The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals. ACM Transactions on Computing Education (TOCE), 18(3), p.11.

Knapp, K. Maurer, C. and Plachkinova, M., 2017. "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance." Journal of Information Systems Education 28(2): 101-113, 2017.

Manson, D., and Pike, R., 2014. "The case for depth in cybersecurity education." ACM Inroads 5(1): 47-52, 2014.

Murphy, D., and Murphy, R., 2013. "Teaching cybersecurity: Protecting the business environment," Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference. Kennesaw GA, USA, ACM: 88-93, 2013.

Miller, R., (2016, July 2). "How AWS came to be" website: https://techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/

National Initiative for Cybersecurity Education (NICE) https://www.nist.gov/itl/applied-cybersecurity/nice/about

New Approaches to Cybersecurity Education (NACE) Workshop, 2018, https://www.cerias.purdue.edu/site/nace/

National Initiative for Cybersecurity Careers and Studies (NICCS), Workforce Development, https://niccs.us-cert.gov/workforce-development

Peltsverger, S., 2015. "A survey of university system of Georgia cyber security programs". Proceedings of the 2015 Information Security Curriculum, 2015.

Raj, R.K., Blair, J.R., Sobiesk, E. and Parrish, A., 2018, December. Enhancing Cybersecurity Content in Undergraduate Information Systems Programs: A Way Forward. In Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy (Vol. 1)

Ramirez, R., Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization, Massachusetts Institute of Technology, 2017, unpublished.

Rose, S., Borchert, O., Mitchell, S., and Connelly, S., (2020 August). "SP 800-207 Zero Trust Architecture" website: https://csrc.nist.gov/publications/detail/sp/800-207/final

Sherwood Applied Business Security Architecture (SABSA) 2021 website: https://sabsa.org

Savold, R., Dagher, N., Frazier, P., and McCallam, D.," Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks," In Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on (pp. 127-138). IEEE, 2017.

Schwab, K. 2018. Shaping the fourth industrial revolution. Geneva, Switzerland: World Economic Forum.

State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets. (2021).

Sternstein, A., 2012, January 30. "Feds need to start thinking like hackers" website: https://www.nextgov.com/cybersecurity/2012/01/feds-need-to-start-thinking-like-hackers/50540/

Study International Staff, 2021, May 6. "Cybersecurity: A career that will stay in-demand for decades to come" website: https://www.studyinternational.com/news/cybersecurity-career-in-demand/

Trilling, R., 2018, September. Creating a New Academic Discipline: Cybersecurity Management Education. In Proceedings of the 19th Annual SIG Conference on Information Technology Education (pp. 78-83). International World Wide Web Conferences Steering Committee.

Triolo, C., "Hackers only need to get it right once, we need to get it right every time," SC Media, 2014.

United States Department of Defense https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_viewpoints/

Yuan, X., Yang, L., He, W., Ellis, J.T., Xu, J. and Waters, C.K., 2017, March. Enhancing Cybersecurity Education Using POGIL. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (pp. 719-719). ACM.