Virginia Journal of Science / Volume 74, Issue 1 & 2 / Spring & Summer 2023
doi: 10.25778/jx3e-6785

A Targeted Study on the Match between Cybersecurity Higher Education Offerings and Workforce Needs[1]

Diane Murphy, Marymount University, dmurphy@marymount.edu
Nektaria Tryfona, Virginia Polytechnic Institute and State University, tryfona@vt.edu[2]
Andrew M. Marshall, University of Mary Washington, amarsha2@umw.edu

ABSTRACT

The Cybersecurity Workforce Gap is a call to action on a two-fold problem: the worldwide shortage of qualified cybersecurity workers and the need to develop a growing highly-knowledgeable, agile, well-trained cybersecurity workforce. This paper presents a methodological approach to achieve this goal in the Northern Virginia area. The area is characterized by an abundance of cyber-related industries, government agencies, and large businesses with high demand of skilled cybersecurity workers; at the same time, academic institutions offer cutting edge education and training access to highly capable students. Central to this methodology is the collaboration between local academia and industry and it includes: an examination of current literature to identify common practices in the development of cybersecurity talent; a Workforce Needs Survey answered by key local industry partners, followed by a thorough analysis of the results; and a review and analysis of the existing cybersecurity educational programs and experiential learning offered by Northern Virginia academic institutions. The outcome is to identify existing pathways to meet workforce needs as well as to reveal gaps in educational programs that need to be addressed. Finally, much needed recommendations for employers, academic institutions and students are presented.

Keywords: cybersecurity, workforce, experiential learning

[1] This work was supported by the Northern Virginia Node of the Cybersecurity Commonwealth Initiative (CCI) https://cyberinitiative.org/ through the "Building Capacity for Cyber-Capable Workforce" grant.

[2] Part of this work performed while the author was with George Mason University.

1. INTRODUCTION

As the digital economy continues on its accelerated growth path, the need for effective cybersecurity workforce development is critical to combat the increasing number of threats from cybercriminals, nation states, and even company employees (i.e., insider threats). For this, the cybersecurity industry has faced a talent shortage for many years, and despite an influx of cybersecurity talent, it is currently estimated that global demand for cybersecurity professionals continues to outpace supply — resulting in the Cybersecurity Workforce Gap ((ISC)^2 2021).

The issue is even more intense in places where "location matters." The Commonwealth of Virginia has the second largest cybersecurity workforce in the country; in January 2022 it was estimated to be about 93,000 cybersecurity workers (CyberSeek). Furthermore, it has a large contingent of government workers and government contractors in the areas close to Washington, DC as well as many large businesses such as Capital One and Amazon. It is also home to the most data centers in the country. Consequently, it has a major shortage of workers with some 49,000 open cybersecurity positions in January 2022 (CyberSeek).

To address this shortage, the Commonwealth Cyber Initiative (CCI), a multi-million-dollar investment from the Commonwealth of Virginia, was established, serving as an engine for research, innovation, talent development, and commercialization of technologies at the intersection of security, autonomy, and data. (cyberinitiative.org/). It has members from business, academia, and non-profits dedicated to ensuring the economic viability of the state in a changing digital world.

Additionally, as a response to the global demand for qualified cybersecurity workers, academic degree programs and certificates, training activities, camps, seminars, to name a few, are offered regularly. Despite all these efforts, there remains a gap between workforce needs and cybersecurity education offerings worldwide ((ISC)^2 2021). How do we fill the Cybersecurity Workforce Gap?

This paper presents a methodological approach to matching cybersecurity higher-education offerings and workforce needs based on research funded by CCI (Building Capacity for Cyber-capable Workforce 2021). Seven of the major four-year higher education institutions and community colleges in the Northern Virginia area worked together to (a) conduct a survey on over 100 Northern Virginia organizations to determine the current requirements (knowledge, skills, and abilities) for students as they transition from college to the cybersecurity workforce; (b) survey the cybersecurity education programs in our institutions in relation to these stated needs; (c) explore experiential learning modules in these institutions to examine how students can meet the "work experience" requirements of potential employers; and (d) make recommendations for employers, academic leaders, and students planning to enter the cybersecurity workforce.

Our goal is to encourage educational institutions, at all post-secondary levels, to include programs, courses and activities that result in cybersecurity workers equipped with the much-needed cybersecurity skills as defined in NIST's Workforce Framework for

Cybersecurity (Petersen et al. 2020). To cover the range of skills required by the cybersecurity field, courses from electrical and computer engineering (ECE), computer science (CS) and information technology (IT) departments, at community colleges and four-year institutions, public and private, were included in this study.

To the best of our knowledge, no other detailed methodology based on the collaboration of academia and employers exists. We are not just looking at job descriptions and university programs, we are surveying employer needs and components of our educational approach to training cybersecurity workers. We see this study as the first step of our work towards a targeted cybersecurity workforce while addressing the high academic standards needed to solve the current Cybersecurity Workforce Gap.

The rest of the paper builds on the methodology used to match cybersecurity higher-education offerings and workforce needs: Section 2 examines the current literature to identify common practices in the development of cybersecurity talent; Section 3 presents the Workforce Needs Survey along with its findings; Section 4 reviews and analyzes the existing cybersecurity educational programs while Section 5 focuses on reviewing and analyzing experiential learning offerings. Finally, Section 6 summarizes the study and discusses recommendations for employers, academic institutions, and students.

2. LITERATURE REVIEW AND COMMON PRACTICES IN CYBERSECURITY EDUCATION AND HIRING PRACTICES

2.1 The Cybersecurity Talent Shortage

The cybersecurity workforce talent gap is well-documented, both globally and nationally. For example ((ISC)^2 2021), in its latest annual cybersecurity workforce study, found that the global cybersecurity workforce needs to grow by 65% to effectively protect the world's growing digital assets which are increasingly critical to national economies and societies. This is a total of 2.71 million skilled workers needed in a global workforce estimated at 4.19 million, a year-over-year increase of more than 700,000 skilled cybersecurity professionals ((ISC)^2 2021).

At the national level, CyberSeek provides detailed, actionable data about supply and demand in the cybersecurity job market supporting local employers, educators, career counselor, students, current workers, policy makers and other stakeholders. It maintains a cybersecurity heat map (https://www.cyberseek.org/heatmap.html) that details the cybersecurity workforce talent gap across the United States. The data is maintained by a collaboration between the government (presented by the National Institute of Science and Technology, NIST), an industry association (CompTIA), and a job analysis organization (Burning Glass -now LightCast). As of January 30, 2021, the site listed 597,797 job openings in the U.S. and a total cybersecurity workforce of 1,053,468, demonstrating the wide cybersecurity talent gap. The heat map can also be broken down by state, metropolitan area, and public/private sector. The cybersecurity workforce is not evenly distributed

across the country, with three states having the largest talent gap (California, Virginia, and Texas). Virginia's workforce needs are largely in the Northern Virginia area because of its proximity to one of the major cybersecurity employers, the Federal government. The CyberSeek heat map shows the Washington, DC metro area as having the highest number of vacancies at 68,214, some 4,960 of these in the public sector in January 2022. However, many of the other positions in the DC metro area are also government focused as they are with contractors supporting the government, directly or indirectly.

A more general look at the workforce in Northern Virginia was recently released by the Northern Virginia Chamber of Commerce, in collaboration with the Northern Virginia Community College (Northern Virginia Community College 2021). The report found that the Northern Virginia region weathered the COVID-19 pandemic better than most other regions in the country, however, they are finding significant challenges in recruiting skilled workers as the economy begins to grow. Their survey showed that 42% of businesses indicated that the overall shortage of candidates with the right cybersecurity skills was seen as a major barrier to current growth.

The literature reinforces the widely publicized notion that the Cybersecurity Workforce Gap is global, national, and regional, with Northern Virginia one of the locations greatly affected.

2.2 Skill-based Hiring

There is currently an increased focus on skills and experience in the hiring process, particularly in technology, including cybersecurity. Skills-based hiring is defined generally as identifying the skills required for a position and searching for candidates who have these specific skills, instead of the traditional method of using a degree as a proxy (DeMark and Kozyrev 2021).

There appears to be a misalignment between higher education and employers regarding how skills are recognized (Weise et al. 2019). Traditional college transcripts do not fully record skills. The list of courses taken, together with course grades, provides little insight into subject mastery, let alone a person's capability of applying the knowledge learned to solve real-world problems. On the other hand, job postings on employment websites usually are packed with very specific skills that do not easily relate to the knowledge learned and courses documented on the college transcript. Increasingly one of our aims as educational institutions is for our students to be employable on graduation, particularly where there is a large talent gap such as in cybersecurity. This study takes a deeper dive at how our courses relate to the cybersecurity skills required by the workforce, and generally shown in the job postings.

Skills-based hiring has emerged as a most important technology talent acquisition strategy as IT jobs have remained unfilled (Global Knowledge 2021). In their 2020 global survey, Global Knowledge found that 60% of IT decision makers placed skills as their most important hiring qualification, while only 2% cited a relevant degree as their primary hiring criteria.

Efforts are underway to create a more skill-focused hiring and teaching ecosystem. The World Economic Forum has brought together several communities of influential leaders committed to the "Reskilling Revolution" (https://www.reskillingrevolution 2030.org/). This aims to create more efficient labor markets by more closely aligning the supply and demand of learning (World Economic Forum 2021).

Another notable example is the Open Skills Network (OSN) (https://www.openskillsnetwork.org/). The OSN alliance consists of innovators from education, industry, and government that are focused on creating and promoting a national network of skills libraries and skills data as well as a community of practice focused on widespread adoption of skills-based education and hiring practices (DeMark and Kozyrev 2021).

While there are broad skills mapping initiatives, the approach taken in this study is to limit the scope to cybersecurity programs in community college and four-year schools in Northern Virginia and to match the skills embedded in these cybersecurity courses to the skills most requested by Northern Virginia public and private organizations who were hiring entry-level talent for their cybersecurity teams. It is recognized that there are other approaches to educating the workforce, including certifications and apprenticeships (Bonvillian and Sarma 2021).

2.3 Community-college Programs in Cybersecurity

Two Northern Virginia based community colleges participated in the study. They are both part of the broader Virginia Community College System (VCSS) and their programs and courses were felt to be reflective of the other community colleges in the region. VCCS institutions generally offer the Associate of Applied Science (AAS) degree in Cybersecurity, designed to prepare students directly for the cybersecurity workforce as a technician or analyst. However, many of these students go on to four-year schools to obtain a bachelor's degree in cybersecurity or a related field.

2.4 Four-year School Programs in Cybersecurity

Five of the four-year schools in Northern Virginia participated in the study: three public universities and two private institutions. Each offered programs in cybersecurity, most often as a specialty or concentration in electrical and computer engineering, computer science, or information technology for both incoming freshmen and for transfer students from the local community colleges. Studying cybersecurity in a location where there are many public and private sector jobs available is attractive to many students from around the country.

2.5 Non-traditional Training Programs

While non-traditional training programs are not a part of this study, it should be noted that they are another source of cybersecurity talent, students often obtaining certifications as a result of their training. In the study we looked at certifications requested by employers in the region and the courses offered by our higher education institutions that covered the body of knowledge from certifications such as Security+ from CompTIA (CompTIA.org).

2.6 Experiential Learning

Employers seek students with work experience to demonstrate their skills and usually define this as an internship in the workplace. Students who participate in an internship show an increase in their employability (Nunley et al. 2016). While some employers look solely at a job or an internship in the field to qualify as work experience, we believe a broader perspective is necessary. The definition of experiential learning can be broadened to students acquiring "work-like" experiences designed to develop hands-on skills while applying learned fundamental knowledge. It reinforces experiences at the higher levels of the Blooms Taxonomy (including terms such as apply, analyze, evaluate, and create) (bloomstaxonomy.net/). We use the broader definition of experiential learning to survey the offerings from the higher education institutions to demonstrate their commitment to ensuring their students are workplace ready.

3. WORKFORCE NEEDS SURVEY

3.1 Survey Methodology

The academic partners were: two Community Colleges, namely Lord Fairfax Community College and Germanna Community College, and five four-year universities, namely George Mason University, Marymount University, University of Mary Washington, James Madison University, and Shenandoah University in the Northern Virginia region. The seven institutions worked together to develop an online survey to determine the current requirements from employers for our students as they transition from college to the workforce. The survey was anonymous and sent to organizations: (a) industries focusing on cybersecurity or working with cybersecurity partners, (b) government agencies, (c) academia. The targeted departments were Human Resources (HR), Development, Design, Management, and Training in addition to cybersecurity professionals who were hiring managers.

The selected organizations had the following characteristics:

1) They were CCI Northern Virginia (NoVa) Node industry partners.
2) They had cybersecurity alumni from one of the four-year schools.
3) The industry partners were from both community colleges and four-year schools.
4) Local businesses and organizations were in the community colleges' target areas.
5) The organizations were in cybersecurity professional organizations, such as ISACA and ISSA.

The initial questions on the survey focused on the type of organization and the role that the survey respondent held in the company, as well as their role in the hiring of college graduates. The next set of questions focused on the job titles used to recruit entry-level cybersecurity professionals, including those that were not classified as cybersecurity work.

The next set of questions were designed to obtain more specific details about the knowledge, skills and abilities (KSAs) expected of recent college graduates. Questions

were asked about the types of cybersecurity knowledge (general and specific), soft skills, cybersecurity tools, and certifications.

Another set of questions focused on the activities of the organizations themselves to support the talent gap. One question was asked about the internships they offered, if any, the training they gave on hiring, and whether they reimbursed their employees for taking certifications after hire.

A final set of questions focused on the hiring process, including the average time it took to hire a qualified person, the number of new entry-level hires, the salary on hire, and the retention rate once hired.

In total 120 survey responses were collected. Seventy-five percent of the survey respondents were from industry, 17% from government agencies, and 8% from academia.

3.2 Results and Analysis

Below are the results and implications of the responses for some of the most important questions in the survey.

3.2.1 Job Title and Level.

Analysis of the titles selected by the employers' representatives are summarized in Table 1.

Table 1: Cybersecurity Job Titles and Levels

Job Level	Job Titles	Percent per job	Percent per job level
Entry Level	Specialist	21%	21%
Mid-Level	Analyst Consultant	27% 3%	30%
Senior Level	Engineer Manager Architect	24% 12% 5%	41%
Not specified	Data Scientist Other	5% 3%	8%
TOTAL			100%

Implication: Employers are mainly recruiting for higher level cybersecurity positions other than those which the NIST Framework (Petersen et al. 2020) considers entry level. Only 21% of the titles given fell into the entry level category, with nearly twice as many jobs at the senior level (41%). This is a major pipeline challenge for educational institutions. Community college programs and four-year undergraduate programs are focused on preparing students for entry level jobs.

3.2.2 Cybersecurity Internships.

Only 71 (60%) of the respondents answered this question with only 37% saying they had an existing internship, and 8% saying they were planning one for the future.

Implication: These numbers are worrisome as the internship is still the major vehicle for students to get experience prior to graduation. Most employers are looking for students with at least some experience. The survey showed a low number of organizations reporting offering internships.

3.2.3 Important Knowledge and Skills.

The five highest knowledge areas selected were:

i. Network security
ii. Authorization and authentication
iii. Access controls
iv. Known vulnerabilities and attack vectors
v. Programming/coding

The top specific technical skills included:

i. Malware analysis
ii. Penetration testing
iii. Intrusion detection/prevention
iv. Encryption
v. Cloud computing authorization and authentication

Implication: The general cybersecurity knowledge areas should be covered in academic cybersecurity programs. General subjects such as network security, in its broader meaning, seem to be more in demand than some more specific sub-areas such as encryption, protocol standards, and confidentiality. This might indicate that organizations are mainly looking for students with a broad understanding of cybersecurity rather than specific components.

Programming/coding is becoming a major employer requirement as automation of cybersecurity processes increases. All of our graduates need to meet these knowledge requirements. Cloud computing, however, is a relatively new topic and may not yet be included in some cybersecurity programs because of the time it takes some organizations to authorize curriculum changes.

3.2.4 Soft Skills.

The most common soft skills included:

i. Critical thinking
ii. Integrity
iii. Problem solving
iv. Communications
v. Teamwork

Implication: Soft skills are becoming a major requirement in many cybersecurity positions. Four-year academic institutions and community colleges should be building these skills along with the technical skills.

3.2.5 Specific Cybersecurity Tools.

The tools that were the highest requested were:

i. Open source: Wireshark and Nmap
ii. Proprietary: Splunk and Nessus

Implication: The specific coverage of tools varies with institutions although most make use of open-source tools such as Wireshark, Kali Linux, and Nmap. These are important parts of the "hands-on" component of community college and four-year programs and are reinforced by engagement in competitions. Students are also encouraged to learn and practice on their own, during their school life and after graduation.

3.2.6 Certifications.

The top 3 certifications were Security+, CISSP, and CEH. Two related certifications were AWS and ITIL.

Implication: Security+ is the most common certification required for entry-level positions in industry or government. Community colleges often tailor their associate degrees to include this certification, and others, to help position the students for better entry into the cybersecurity workforce after completing their associate degree. Universities may cover one or more certifications such as Security+ at the undergraduate level. CISSP and CEH are largely covered in graduate programs because of the experience requirements associated with them. Institutions should take note of the increasing need for the newer certifications such as AWS and ITIL -- while not directly cybersecurity, they are becoming common in job announcements as adjacent (preferred) requirements.

3.2.7 Requirements for Security Clearances.

Requirements for clearances were high in our survey. Only 25% said they had no clearance requirements, and another 27% required applicants to be "clearable." Nearly 50% of the respondents, however, requested a clearance, and many of them (25% of total) were at the top secret level and above.

Implication: Students need to understand the concept of "clearability" and getting a position with a clearance since 75% of the companies responding indicated that they were working in the cleared space. They also need to understand the time it takes to obtain such a clearance -- the higher the level, the more time will be required. This also affects internships and job opportunity for non-citizens and non-permanent residents (e.g., international students), which are a growing part of the student population in Northern Virginia.

3.2.8 Entry Level Salary.

More than 50% of the respondents listed a starting salary between $55,000 and $70,000 while only one (1) respondent cited more than $90,000 per year.

Implication: As there is a lot of hype on salaries in cybersecurity many students are motivated to enter the field. For example, although CyberSeek lists the average cybersecurity professional salary as nearly $100,000, this study should help students understand they need to be realistic for their expectations for an entry-level position.

3.2 Summary

The survey registered the important technical skills for the cybersecurity workforce. It also showed that beyond the much-needed technical knowledge, soft skills such as teamwork, communication skills, and continued learning skills were listed as important additional topics. Entry-level jobs were not as widespread as assumed, as many employers are looking for a higher level of experience and skills. Clearances and "clearability" were significant employment factors in the Northern Virginia region. Finally, the availability of internships in the region was disappointing as academic institutions try to meet the employers' expectations for "work experiences."

4. REVIEW OF CYBERSECURITY EDUCATION PROGRAMS

4.1 Survey Methodology

The next step in our project was to review the partner academic institution's programs to ensure they are meeting the employer expectations for new hires and are keeping current with advances in the field (e.g., cloud computing). Based on the initial survey of workforce needs, a survey was developed to evaluate how university and community college programs are serving workforce needs. The survey identified four core categories of skills which were sought after by employers. These areas were:

1) *Technical Knowledge/Skills*
   Including network security, authentication, malware analysis, intrusion detection/prevention, cloud computing, and risk management
2) *Soft Skills*
   Including critical thinking, oral and written communications, and teamwork
3) *Tools*
   Including Wireshark, Nmap, Splunk, and Nessus.
4) *Certifications*
   Including, Security+, CISSP, CEH, AWS, and ITIL.

The survey was not anonymous, and academic institutions were asked how many, if any, of their courses covered each of the above sub-areas. For example, if an institution had two courses that included the area of authentication, two courses would be listed. As is typical, broader knowledge areas such as teamwork were often covered across multiple courses.

The seven higher education institutions were sent the survey and asked to complete the survey by analyzing their course offerings against the most important knowledge, skills, tools, and certification areas listed in the workplace survey.

4.2 Results and Analysis

All seven institutions responded to the online survey. All quantitative responses were totaled. The open-ended responses were reviewed by the working group participants to identify common themes.

The analysis was broken down into the four main categories covered in the survey.

1) *Technical Knowledge/Skills*: Overall the technical knowledge and skills surveyed were well incorporated into the various cybersecurity programs. For all knowledge areas and skills, excluding cloud computing, each institution had at least one course, and often several, which included material on that skill. The outlier of the most in-demand skills was cloud computing which was not included in every program.

2) *Soft Skills*: The soft skills surveyed are almost as well integrated into the various cybersecurity programs as the technical skills. However, we do see a few more small gaps in this data set. Here there exist several schools for which there is at least one soft skill not included in any courses. Oral communication skills have the least coverage. Here the data seems to point to the continued inclusion and further incorporation of soft skills into the region's cybersecurity programs.

3) *Tools*: Broadly the data seems to indicate that the cybersecurity programs surveyed are including industry recognized tools into their programs. This is not surprising given that it aligns with the data from the technical skills sections. There are gaps in specific tool coverage. However, this does not necessarily indicate gaps in skills areas for which the tools are applicable. For example, an institution could be teaching vulnerability scanning using an open-source tool such as OpenVAS instead of Nessus, and thus teaching the skill of vulnerability scanning just with another tool.

4) *Certifications*: Here the data points to a large gap in courses preparing students for a number of the industry-recognized certifications. Several institutions include no certificate preparation or teach just a single course. Here progress could be made by including broader coverage of certifications, especially those recognized and in demand by employers.

4.3 Summary

The broad take-away from the data was that the higher education institutions in the area were generally doing well covering technical knowledge and skills in their cybersecurity programs. However, small gaps appear, and work could be done to ensure uniform coverage of a basic set of skills across the region and the inclusion of newer topics, for example, cloud computing.

5. REVIEW OF EXPERIENTIAL LEARNING ACTIVITIES

5.1 Survey Methodology

The employer survey demonstrated the lack of internships in the current workplace and led the group to look at how we could demonstrate that our students are ready to work in the cybersecurity field. We began to examine how we could demonstrate all forms of "experiential learning" as an alternative strategy. First, we looked at what went on in our institutions to find examples of experiential learning inside and outside an academic program and these are shown in Table 2.

Table 2: Examples of Experiential Learning

Inside the Program	Outside the Program
Significant hands-on activities using common tools (e.g., GitHub, Wireshark, Python).	University work study requiring technical skills (e.g., web development) and campus-based It projects (Conrad 2020).
Courses teaching the knowledge for a specific industry certification (e.g., A+).	Participation in technology and innovation competitions.
Project-based learning: teaching technology through hands-on projects alone.	Undergraduate research programs in a program or through NSF's Research Experience for Undergraduates (REUs).
Courses with significant projects focusing on soft skills such as teamwork, presentations, ethics.	Leadership in student organizations such as ACM, IEEE, and ISACA.
Capstone projects: term-length assignments completing a major technology project. Technology internship.	Service-learning projects: students volunteer technology expertise to a not-for-profit or small business. Apprenticeship: working students who learn while employed in industry.
Cooperative education (co-op): balancing knowledge with practical, hands-on in the workplace.	Self-learning: hands-on courses leading to certificates or formal certifications.

To better understand experiential learning in Northern Virginia, we also surveyed the same seven institutions on how experiential learning is incorporated into their cybersecurity programs. The survey asked about the number of courses that included significant hands-on labs, the courses including team-based learning, and the number of courses incorporating the knowledge base of specific industry certifications. The survey also asked about the number of courses including internships and capstone projects. In addition, the survey asked about activities that were outside the required courses of the

program. This includes activities such as participation in cybersecurity competitions, undergraduate research, participation in student lead clubs, service-learning, and apprenticeship programs. In this portion of the survey the higher-education institutions were not asked to respond with the number of courses covering such material, but more broadly if their institution has the listed opportunity, encourages it, and/or are working on such opportunities.

The survey was not anonymous, and all seven institutions responded to the survey, although not all responded to every question.

5.2 Results and Analysis

Experiential learning, such as significant hands-on labs, group projects, and exposure to industry tools, is well integrated into all of the cybersecurity programs surveyed. All institutions included hands-on labs and coverage of common industry tools. Only the subcategory of co-op education was poorly offered. Indeed, co-ops, at the time of the survey, were not included in any of the responding institutions.

Opportunities outside the program, such as student clubs and undergraduate research, varied more than the experiential learning incorporated into each program. Three institutions did not offer responses to this section of the survey. Of those that responded at-least some types of opportunities outside the program were either offered, recommended, or in the works for the future.

5.3 Summary

Overall experiential learning is a part of all the cybersecurity programs surveyed. However, the data points to differences in the types of experiential learning. For example, many courses include lab and team-based projects, but no courses include co-op-based learning. This could point to the difficulty in setting up such co-op programs and how they may be effectively used.

Outside the classroom results varied and it is difficult to draw many conclusions given the sparse data.

6. RECOMMENDATIONS AND CONCLUSIONS

6.1 Recommendations for Employers

Employers did not report to be currently looking to hire a large number of entry-level cybersecurity staff, focusing primarily on more experienced personnel. However, employers must recognize that recent college graduates are an important component to fill the large Cybersecurity Workforce Gap. There are also a wide variety of job titles which can be confusing for students as they look through job postings, finding it difficult to determine which are entry-level. Some consistency in job titles would be helpful and NIST NICE (National Institute of Standards and Technology's National Initiative for Cybersecurity Education) might be used as the framework for this. In addition, the salary

structure for college graduates might need to be looked at given the hype about cybersecurity being a highly-paid profession.

Skills and work experience are major parts of the current skills-based hiring approach. If our students are to get more experience while in our academic institutions, employers need to offer more internships and students must be notified about them so they can effectively compete for them. A centralized internship database for those that are being offered is needed, for example as a collaboration between the Northern Virginia educational institutions and industry and government partners. The CCI NOVA node has begun this initiative with its website at https://cci-novanode.org/. The employment opportunities are listed here (https://www.cci-novanode.org/jobs.html) and internships and apprenticeships are listed here (https://cci-novanode.org/cciapprenticeships.html). A survey of this site by faculty, employers, and job seekers might be a next step. The CCI NOVA database could be extended to allow students/alumni to post their resumes. This would help connect our candidates with CCI NOVA node partners to keep these applicants in Virginia and maybe reduce the lead time for the hiring process.

6.2 Recommendations for Academic Institutions

Our survey demonstrates that the Northern Virginia academic institutions are largely in compliance with the knowledge and skills required by employers in the region. They need to keep abreast of new focus areas (e.g., cloud computing) and develop more timely processes to add new topics to their curriculum.

The technical knowledge and skill and soft skills acquisition, however, are not clearly evidenced on college transcripts. Soft skills such as teamwork, communication skills, continued learning skills were listed as important additional topics by employers but are generally not listed on the transcript. The need to display skills should be part of career preparation and demonstrated on student's resumes. A review of how specific knowledge and skills are integrated into academic programs might reveal gaps and best practices.

Employers recognized the role of certifications as a demonstration of technical skills, particularly Security+ for entry-level jobs. Coverage of the body of knowledge of certifications by our academic institutions should be studied. Taking certifications such as Security+ for credit may also be worth exploring.

The institutions all recognized that experiential learning such as hands-on labs, based on real world scenarios and out of the classroom learning, such as internships, are important to developing knowledgeable cybersecurity professionals and meeting workforce requirements. Experiential learning opportunities should be further developed on college campuses to show work experience outside an internship.

6.3 Recommendations for Students

Students must prepare themselves for the cybersecurity workplace. It is not just about gaining the knowledge and skills in class; the cybersecurity field is so dynamic that students should be constantly engaged inside and outside the classroom. There are many opportunities to learn new topics outside the classroom with a variety of free and low-cost

training options. Students should also take advantage of opportunities to demonstrate their skills through participation in Capture the Flag (CTF) and other cybersecurity and programming competitions.

Students should also consider taking industry-recognized certifications such as Security+ as well as adjacent technology certifications such as those from ITIL and AWS.

Students must recognize that getting a job or an internship requires work on their part. Their resumes and cover letters must reflect all their knowledge and skills as well as projects that demonstrate experiential learning. Today, a good LinkedIn profile is also important in the hiring process.

Clearances are significant in our area and students must understand what it means to be "clearable" particularly in social media. Students must also have realistic salary expectations for their first job.

Closing the Cybersecurity Workforce Gap is not going to be solved overnight and needs close collaboration between employers and academic institutions. While this study was conducted in Northern Virginia, we believe our findings can inform other researchers across the country, bearing in mind that the number of open cybersecurity jobs varies in different areas of the country (CyberSeek) -- variations in the local cost-of-living will have an impact on salaries, and the programs taught at regional academic institutions vary across the country. This study provides a deep dive into the gap between employers and academic institutions in Northern Virginia and provides some important recommendations in closing the gap through a close collaboration between academia and industry.

ACKNOWLEDGMENTS

This work was supported by the Cybersecurity Commonwealth Initiative (CCI) https://cyberinitiative.org/ through the "Building Capacity for Cyber-Capable Workforce" grant.

The Following individuals participated in the initial study:

- Diane Murphy, Marymount University
- Nektaria Tryfona, Virginia Polytechnic Institute and State University
- Andrew M. Marshall, University of Mary Washington
- Henry J. Coffman, Lord Fairfax Community College
- Samy El-Tawab, James Madison University,
- Bryant Payden, Germanna Community College
- Ahmad Salman, James Madison University
- David Scibelli, Shenandoah University

STATEMENT OF RESPONSIBILITY

Diane Murphy: Participated in designing and analyzing the result from the industry survey and the survey to the universities and community colleges in response to industry requirements. She coordinated the survey responses for Marymount University. She was also a major part for the analysis and writing of the report that was submitted to the Commonwealth of Virginia.

Nektaria Tryfona: Participated in the initial survey development and dissemination to industry partners. She was responsible for the coordination of the project. She helped in building the survey, in the analysis of survey results, in aggregating results from all partners. She was responsible for reporting results and recommendations to the Commonwealth.

Andrew M. Marshall: participated in the initial survey development and dissemination to industry partners. He helped in the analysis of survey results and was responsible for reporting on the University of Mary Washington's cybersecurity course offerings and programs.

REFERENCES

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

Bloom's Taxonomy, https://bloomstaxonomy.net/

Bonvillian, W. B. and S. E. Sarma. 2021. Workforce Education: A New Roadmap. The MIT Press.

Commonwealth Cyber Initiative, https://cyberinitiative.org/

Conrad, S. S. 2020. Experiential learning: Preparing students for the workforce through faculty mentorship and feedback in campus-based IT projects. Journal of Computing Sciences in Colleges, 36(3): 142–150.

CyberSeek, https://www.cyberseek.org/

DeMark, S. and J. Kozyrev. 2021. Enabling pathways to opportunity through a skills-based architecture. The Journal of Competency-Based Education, 6(1): e1241.

Global Knowledge. 2021. 2020 IT Skills and Salary Report. https://images.globalknowledge.com/wwwimages/web/salary-report/current/it-skills-salary-report-2020-global-knowledge-en-ww.pdf

Northern Virginia Community College. 2021. 2021 Northern Virginia Workforce Index, retrieved from https://www.nvcc.edu/oiess/oir/labor-market/_docs/NOVA-IndexReport-2021_FINAL.pdf

Nunley, J. M., A. Pugh, N. Romero, and R. A. Seals. 2016. College major, internship experience, and employment opportunities: Estimates from a résumé audit. Labour Economics, 38: 37-46.

Petersen, R., D. Santos, K. Wetzel, M. Smith, and G. Witte. 2020. Workforce framework for cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1, November 2020

Tryfona, N., D. Murphy, A. M. Marshall, S. El-Tawab, A. Salman, D. Scibelli, H. J. Coffman, and B. Payden. 2021. Building capacity for cyber-capable workforce, Project Report, Northern Virginia Node Cybersecurity Commonwealth Initiative (CCI) https://cyberinitiative.org/

Weise, M. R., A. R. Hanson, R. Sentz, and Y. Saleh. 2019. Human+ Skills for the Future of Work. https://www.economicmodeling.com/robot-ready-reports/

World Economic Forum. 2021. Building a Common Language for Skills at Work: A Global Taxonomy. https://www.weforum.org/reports/e47fb10b-de89-4092-98c6-198fd2328556