NICE community coordinating council

Help Wanted: Cybersecurity Educators

How NCAE institutions are responding.

December 2024

A research paper for discussion from the NICE Community Coordinating Council, Transform Learning Process Working Group, Cybersecurity Educators Workforce Gap Project Team.

Mike Morris, Western Governors University, Co-Chair of Transform Learning Process Working Group
Jason Hammon, Western Governors University, Project Lead

Literature Review & Research:
Keith Anderson, Marymount University
Kampanart Vikayanon, Marymount University
Lori Coombs, Marymount University
Andrew Spragg, Marymount University

Quantitative and Qualitative Analysis:
Oluwatomisin Giwamogorewa, Marymount University
Sapol Jirapanjavat, Marymount University
Clinton L. Ilges III, Marymount University

The Transform Learning Process Working Group focuses on the NICE Strategic Plan's objective to Champion the Development and Recognition of Teachers, Faculty, and Instructors as Part of the In-demand Workforce (2.6). The group conducts an ongoing environmental scan of programs, projects, and initiatives related to this strategic plan's goals and objectives to assess the scope and sufficiency of efforts. The group also identifies gaps where more attention and effort are needed. The group identifies strategies and tactics necessary to meet its objective.

Our project team consists of contributors in various stages of their academic career and seeks to provide opportunities for collaboration, research, and publication. As such, this paper will highlight substantive contributions from each team member as we try to improve our craft.

Authored September 2024
Published December 2024

Table of Contents

Executive Summary

The **Cybersecurity Educators Workforce Gap Project Team** has prepared this report to meet Objective 2.6: *Champion the Development and Recognition of Teachers, Faculty, and Instructors as Part of the In-demand Workforce*. We have compiled and prepared a review of available research to provide the history, context, and particular issues facing schools designated by the National Security Agency and Department of Homeland Security as Centers of Academic Excellence (NCAE). We have connected our research to an established vein of inquiry regarding Computer Science and validated similar concerns of institutions with Cybersecurity programs. Through our research and survey of NCAE schools, we find pressing issues currently affecting our nation's ability to educate students.

Much like the Cybersecurity profession generally, Cybersecurity educators are in demand. However, their supply is constrained by unique factors. In fact, the more the talent pipeline expands to increase the available supply of professionals, the demand for educators increases. These trends follow the long-standing issue of meeting the undergraduate demand for Computer Science, as Cybersecurity has historically been placed within related departments. The ability to develop and train new instructors faces a unique moment because the maturation of the Cybersecurity discipline has only recently accelerated. Government, Industry, and the Academy are defining curriculum standards and job roles, but building programs for students has a long lag time. Building capacity and staffing for those programs typically follow Ph.D. models and similarly lag.

Through a survey of NCAE schools in 2024, we find that institutions are struggling to meet the demand for cybersecurity educators. The survey analysis broadly concludes the following:

- Student demand is rising for cybersecurity education programs.
- NCAE-C institutional leadership views cybersecurity education as a strategic priority.
- Universities are hiring with the intent to expand the number of educators at their institution, but most efforts are small and local.
- Hiring efforts are affected by the limited supply of candidates and the budget and funding limitations of the institutions.

These schools respond only a local level—there is no broad strategy to address the talent gap, although opportunities for coordination exist within the NCAE network. The schools recognize that the demand is high, the supply is low, and there are funding limits to bridge the difference. The shortage is real and keenly felt. Our objective is to share this research broadly and advocate for an increase in planning and funding to meet the need.

Introduction

Cybersecurity is in demand! In the past decade, the demand for cybersecurity professionals has increased at a rate much higher than other occupations and continues to do so (U.S. Department of Labor, 2024b). Similarly, there is a surge in interest in undergraduate cybersecurity education by incoming student populations. Institutions of Higher Learning (IHLs) are having trouble filling vacant positions with qualified educators to meet increasing student demand. This phenomenon is known as the cybersecurity educator workforce gap (the gap).

The **Cybersecurity Educators Workforce Gap Project Team,** as part of the NICE Strategic Plan, convened to implement Objective 2.6 *Champion the Development and Recognition of Teachers, Faculty, and Instructors as Part of the In-demand Workforce*. Our primary purpose is to provide a broad overview of "Cybersecurity Educators" within the context of IHLs designated as National Security Agency Centers of Academic Excellence (NCAE). This includes their historical context, their supply and demand, their qualifications, the unique context of the Academy, and where they fit in the overall cybersecurity talent pipeline. What can institutions do to fill their staffing gaps?

Our objective is to "champion" for cybersecurity educators. This paper focuses on the narrow slice of "Teachers, Faculty, and Instructors" within NCAE IHLs. However, we acknowledge that much cybersecurity education happens outside of the university. There are excellent services provided by training organizations, bootcamps, certification providers, government initiatives, technology solutions, and in the K12 space that fall outside of our scope.

The primary audiences for this publication include the NICE community and their public and private sector partners. Secondary audiences include NCAE IHL faculty and administrators, future cybersecurity doctoral candidates and instructors. This project may also benefit stakeholders that find interest in the current challenges that institutions face regarding the cybersecurity educator workforce gap. We provide additional resources for further reading and investigation, along with a curated set of recommendations that have informed our research. Please see Appendix A for key resources that inform this discussion space.

Literature Review

A Cybersecurity workforce gap combines multiple historical lines of inquiry that we will examine in this literature review. We begin by examining the relatively recent high demand for cybersecurity professionals due to technological advances. Demand for professionals point toward the current pipeline for filling the gap generally. Our study focuses on Institutions of Higher Learning who are primary players in meeting the gap, within a wider context of the demand for computer science education. As the Cybersecurity discipline has matured, various groups in Academia, Government, and Industry have provided specific standards and frameworks for addressing their needs. Finally, we focus on Cybersecurity Educators: who they are, where they come from, and challenges they face.

History of the Cybersecurity Shortage

Keith Anderson, Marymount University

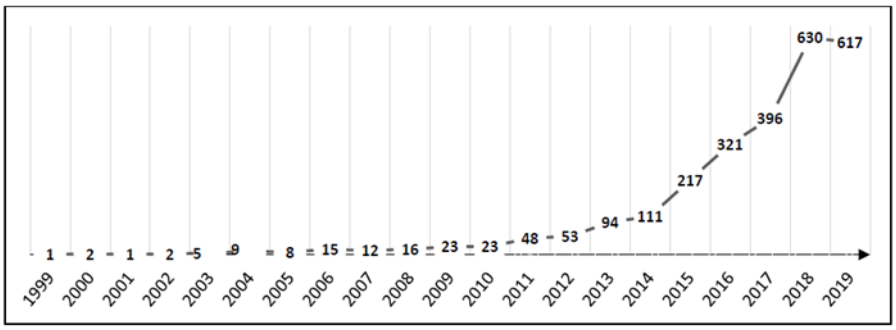
To understand the factors leading to the cybersecurity educator shortage, a sub-component and potential factor in the overall cybersecurity workforce and skills shortage, it is beneficial to understand the journey of the Internet, the evolving concept of connectedness, and how cybersecurity-related norms and strategies within cyberspace have been influenced by physical world impact. With this awareness as a backdrop, we can see where availability of services, information, and entertainment within cyberspace grew disproportionally to ensuring they were securely delivered (and stored).

The concept of online cyber risk, as it pertains to exposure of information and data in the cyber realm (with the potential for negative impact in the physical realm if successfully accessed by unauthorized actors), has been around since the late 1960s. The Advanced Research Projects Agency Network (ARPANET), the precursor to today's Internet, was created to facilitate the sharing of information for academic and research purposes. With the foundational components in place to share information electronically, the vision for establishing global connectivity amongst computer systems began to take shape (Leiner, et al., 1997).

The growing interconnectedness of governments, universities, and private sector organizations began a concept called "internetting," which, according to Leiner, et al. (1997), grew out of the original ARPANET concept. This movement established connectivity amongst multiple independent local networks (providing local services to meet the requirements of users) by way of a common set of communications rules (protocols). The growing forum for "internetting", the proverbial Internet, began to realize a shift in utility in 1985 from information sharing and research to more physical-realm human activities, such as daily communications (Leiner, et al., 1997); leading to a meteoric rise in connected hosts and available services (up to 20,000 hosts in 1988 and over 2 million by 1993), including the White House and United Nations (Zimmermann & Emspak, 2022).

The scale and maturity of services offered over the Internet began to raise concerns for public and private sector leaders, as the growing potential for cyber-related security incidents impacting critical infrastructure and the operational readiness of major organizations started to become an unplanned reality. According to Furstenau, et al. (2020), the term cybersecurity first appeared in literature in 1999; thought to be a subset of the broader field of information technology (IT), only impacting local systems. Between 1999 and 2004, conversation about cybersecurity was scarce, but Furstenau, et al. (2020) note a correlation between the rising concerns of the cyber realm and the increased production of cybersecurity-related publications from 2005-2019, as depicted in Figure 1 below.

Figure 1. *Number of publications over time (1999 – 2019)*



Furstenau et al. (2020). 20 Years of Scientific Evolution of Cyber Security: A Science Mapping

In the mid-to-late 90s, while IT teams acknowledged and considered the need for security of systems and data, holistically addressing the people, processes, and technologies required to sufficiently protect information and data was not formally conceptualized until a very specific callout of these objectives in the 2015 National Security Strategy (NSS) document, which included a section reflective of the nation's cybersecurity concerns titled, "Keep America Safe in the Cyber Era" (Karahan et al., 2019). Subsequently, cyber-related risk management has continued to rise in awareness of senior-level officials in the public and private sectors of the US, as well as around the world.

This preamble to the history of the cybersecurity educator shortage highlights a very eye-opening fact. Within the cyber realm, risk has been allowed to evolve with little-to-no strategic-level mitigation planning from 1985 to 2015; smaller tactical (and disjointed) efforts were embarked-upon to address risks throughout that period, however, these efforts were exceedingly reactionary and without holistic support from government agencies or consensus among the private sectors. Threat actors within the cyber realm have had a 30-year head start on the cybersecurity industry, growing exponentially over that period and naturally leaving cyber defenders shorthanded.

With the rising threats to governments, organizations, and people worldwide, philosophical approaches toward cybersecurity began to shift, resulting in increased funding, staffing, and of course, scrutiny.

Cybersecurity Talent Shortage and Pipeline Strategies

Kampanart Vikayanon, Marymount University

A brief history of internet innovation leads to the current landscape in 2024: the remnants of a global pandemic, regional conflicts, economic uncertainty, and disruption in the latest form of Artificial Intelligence. Amidst the turbulence, Computer and Information Technology (CIT) occupations continue to have increasing demand and projected growth (U.S. Department of Labor, 2024a). With a workforce gap of over 500,000 CIT professionals in the United States and an estimated global shortfall of 3.9 million professionals, the demand for qualified experts far exceeds the available talent pool (ISC2, 2023). Cybersecurity occupations have experienced a similar trajectory.

The ISC2 (2023) reports that the cybersecurity workforce experienced a 9% increase from 2022 to 2023 amassing a global workforce of 5.5 million cybersecurity professionals. However, Cyberseek.org (2024) estimates there are only enough cybersecurity workers in the United States to fill 85% of the cybersecurity jobs currently available despite a recent technology sector slowdown. The Q2 2024 Quarterly Cybersecurity Talent Report from Lightcast (2024) reports that employers struggle filling advanced cybersecurity roles. The current cybersecurity talent pipeline largely emphasizes hiring experienced workers from cybersecurity as well as adjacent fields. Meanwhile, entry-level professionals find it difficult to find their first role. These conclusions point employers toward a need to expand lower-level opportunities as well as an expansion of the talent pipeline. These strategies will bring in new and diverse talent that require training and education.

A multifaceted approach is essential to address the cybersecurity talent shortage. This includes expanding education and training programs at institutions of higher learning particularly in rural and underserved areas, with a focus on diversity and inclusion. Strengthening public-private partnerships can enhance collaboration between government, educational institutions, and industry while improving retention and career pathways. Government legislation and funding for workforce development is crucial for creating a robust cybersecurity workforce capable of meeting the growing demands of the digital landscape (Joshi et al., 2023).

Education and Training Programs

For many people, a general Information Technology degree or career is a springboard into cybersecurity. According to ISC2 (2023) 52% of cybersecurity professionals initiate careers in non-cybersecurity IT roles, gaining valuable experience before specializing. ISC2 further reports mentioned that employers emphasize the value placed on practical experience and specialized certifications in the cybersecurity field.

Community colleges, technical schools, and online education platforms play a crucial role in providing pathways to cybersecurity careers in these areas. By offering degree programs, certifications, and flexible learning options, these institutions are adapting to industry

demand. These institutions, and the exposure they provide for students to the industry, are the most formal pathways into cybersecurity.

Public-Private Partnerships

Public-private partnerships can significantly expand access to cybersecurity education. Regional corporations, working with public institutions, fund scholarships, sponsor educational initiatives, and provide technological infrastructure in resource-scarce areas. These cybersecurity training programs become more accessible and affordable for individuals in economically disadvantaged regions. In return, these organizations invest in a future workforce and provide opportunities for local talent. For instance, businesses or government agencies can provide internships, apprenticeships, or educational programming that directly leads to a job (Struggling with Cybercrime? Turn to Public-Private Partnership, 2015). By pooling resources and expertise, these partnerships can help build a more diverse and skilled cybersecurity workforce, strengthening national security and enabling every community to contribute to the growing digital economy (Richberg, 2024).

Government Support Through Legislation and Funding

Over the last 25 years, cybersecurity has been a bipartisan strategic initiative from the federal government which has provided guidance, critical funding, and incentives for building capacity (Healey, 2023). Even recently, the Biden-Harris administration recently unveiled the National Cyber Workforce and Education Strategy (NCWES) to enhance cyber literacy and address the increasing demand for skilled cybersecurity professionals (The White House, 2023). This comprehensive strategy aims to empower Americans from all backgrounds to pursue cybersecurity careers, with a particular focus on underrepresented communities and economically disadvantaged areas.

For example, the Cybersecurity and Infrastructure Security Agency (CISA) awarded $6.8 million to the nonprofit CYBER.ORG through the Cybersecurity Education and Training Assistance Program (CETAP). This funding will help CYBER.ORG continue promoting cybersecurity education among K-12 students, aiming to address the nationwide cybersecurity workforce shortage. CYBER.ORG provides resources and training to educators and caregivers to deliver cybersecurity content to students. The initiative currently reaches millions of students throughout the United States.

Government funding also directly contributes to building a skilled cybersecurity workforce by supporting education and training programs. Programs like the Scholarship for Service and the Department of Defense (DoD) Cyber Service Academy provide financial support for cybersecurity education at undergraduate and graduate levels. In return, program participants typically transition from Academia to government service.

In summary, there is a cybersecurity workforce gap and there are various initiatives to expand the talent pool. As new entrants come from a variety of backgrounds, there is a reciprocal need for educators. K-12 students need teachers. Underserved communities

need role models. Apprentices need mentors. Interns need managers. Online providers need curriculum designers. Undergraduates need professors. Educators provide the space, environment, and instruction to gain cybersecurity skills. These educators must also be either experienced in the field, where there is a low supply and high salaries, or trained specifically to provide cybersecurity education. The market, in turn, responds by creating opportunities for education through schools, universities, training organizations, certification providers, and online learning.

The Undergraduate Demand

Jason Hammon, Western Governors University

The expansion of internet-based services led to an increasing demand for cybersecurity professionals. This new expansion led to a higher demand for education and skills training. While teaching and learning is not the exclusive domain of higher education, the university response was a growth of cybersecurity courses and programs. Post-secondary degrees are becoming a growing source of training and workforce preparation for cybersecurity careers.

The growth of cybersecurity enrollments is an extension of the trends of computer science enrollment growth. Cybersecurity has traditionally been housed within the Computer Science discipline due to its curricular base in technology. The research surrounding Computer Science undergraduate enrollments provides a meaningful context and range of issues involved in expanding educational offerings.

In 2018, the National Academy of Sciences, Engineering, and Medicine published *Assessing and Responding to the Growth of Computer Science Undergraduates*. This comprehensive document is a must-read for understanding the extent of demand for computer science education, the institutional strategies used as a response to the growth, and its impact for increasing diversity. For a more historical perspective, Stanford professor Eric Roberts has followed the topic and published extensively for many decades and his research is worth perusal (See Appendix A).

At a high-level summary, the United States Department of Labor, Bureau of Labor Statistics has predicted high demand for computer occupations for the last half century and continues to predict growth at a rate that is higher than overall job growth (National Academy of Science, Engineering, and Medicine, 2018). Undergraduate enrollments and degree conferrals in Computer Science have grown significantly, especially in the early 2010's, at a rate that is significantly higher than the increase of bachelor's degree production (74% vs 16%). Despite limitations in the availability of data, "significant [Computer Science enrollment] growth is under way at many institutions" (National Academy…, 2018, p. 3).

Computer Science is also experiencing rapid expansion into other fields (a phenomenon known as “CS +X”). Over the past decade, there has been a major expansion of Computer Science at the K12 level. These factors fuel interest in Computer Science, and, like the rapid expansion of the internet, the need for cybersecurity of the commodities created. In turn, IHL’s have started creating cybersecurity programs and curriculum for students.

Building Cybersecurity Program Curriculum

Keith Anderson, Marymount University

The primary pillars associated with most cybersecurity programs have evolved to encompass some variety of 8 topic area. These are:

- Governance, Risk, and Compliance
- Security Operations (including threat detection and incident response)
- Identity and Access Management
- Application Security
- Vulnerability Management
- Incident Response
- Awareness and Education
- Cloud Security

Since 2011, organizations like the National Initiative for Cybersecurity Education (NICE) have been developing frameworks to establish alignment within the industry on the roles and responsibilities necessary to deliver a cybersecurity strategy for a given organization. In response, several initiatives have evolved to address the gap in specificity of the workforce taxonomy, as well as the education resources necessary to influence the workforce pipeline.

Training and education programs have continually evolved to meet these requirements in alignment with the expectations of organizations in the public and private sectors. In 2008, the National Centers of Academic Excellence in Cybersecurity (NCAE-C) added a cyber research designation (CAE-R) to the NCAE-C program, originally established in 1999 by the National Security Agency (NSA) and the Department of Homeland Security (DHS) to address a shortage in the intelligence community (CAE in Cybersecurity Community, 2022). This designation was changed to CAE in Cyber Defense Education (CAE-CD) in 2017 and has established very prescriptive criteria for applying IHLs to meet, specifically calling out knowledge units (KUs) and alignment with the NICE Cybersecurity Workforce Framework (NCWF) (CAE in Cybersecurity Community, 2022). The CAE-CD program grants degrees to community colleges, campus-based and online colleges, universities, and research institutes.

Cabaj et al. (2018) discusses the efforts of the Association for Computing Machinery (ACM), who also undertook initiatives to develop programs in cybersecurity at the post-

secondary level. Created in 2013, the ACM/IEEE computer science curricula guidelines (CS2013) included information assurance and security (IAS) knowledge areas (KAs), explicitly calling out cybersecurity-related content for computer science programs (Cabaj et al., 2018). Within two years, the ACM Education Board acknowledged the need for cybersecurity to exist as an alternative to computer science, as opposed to a subset of the curriculum. In 2017, the updated Cybersecurity Curricula 2017 (CSEC2017) superseded CS2013 as a curriculum guide for post-secondary degree programs in cybersecurity (Cabaj, Domingos, Kotulski, & Respicio, 2018) and was subsequently replaced by the Computing Curricula 2020 (CC2020). Figure 2 below provides a useful mapping between CSEC2017 KAs and CAE-CDE KUs:

Figure 2. *CSEC2017/NCAE Comparison*

CSEC2017 KAs	CAE-CDE KUs
Data Security	IA Fundamentals
	Introduction to Cryptography
	Advanced Cryptography
Software Security	Fundamental Security Design Principles
	Secure Programming Practices
	Software Assurance
System Security	IA Fundamentals
	IA Architectures
	Intrusion Detection/Prevention Systems
	Cyber Defense
	Software Reverse Engineering
	Digital Forensics
	Industrial Control Systems
Human Security	Vulnerability Analysis
	Cyber Threats
Organizational Security	Policy, Legal, Ethics and Compliance
	Cybersecurity Planning and Management
	Security Program Management
	Security Risk Analysis
Societal Security	Policy, Legal, Ethics, and Compliance

Cabaj et al. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs

Mapping Cybersecurity Curriculum to Workforce Skills

Lori Coombs, Marymount University

In recent years, the cybersecurity curriculum has been established with inputs from the academy, industry, and the government. Moreover, the success of graduates is gauged by their aptitude for their professional career. The top skills required for a cybersecurity career are a combination of hard skills (technical and fundamental) and soft skills. The scope of this section of research examines how specific cybersecurity jobs and required skill sets relate to cybersecurity programs in institutions of higher learning (IHL). Determining what knowledge and skills are necessary, as defined by the National Initiative for Cybersecurity Careers and Studies (NICCS), help identify and bridge the skills gaps.

The NICCS aims to promote cybersecurity awareness training, education, and career advancement in the United States. NICCS is a beneficial resource for deferral government employees, educators, students, and industry for closing skill gaps throughout the labor force. This project aims to address what cybersecurity skill sets are needed for obtaining a career in information security and cyber defense in the United States by comparing NICCS tasks, knowledge, and skills with the NCAE Knowledge Units (KUs).

Hard Skills

The National Cybersecurity Training & Education Center (NCYTE) (2024) has developed seven NICE framework categories: operate and maintain, analyze, collect and operate, oversee and govern, securely provision, investigate, protect and defend (See Table 1). These categories include cybersecurity work roles and are broken down by various topics and outcomes, including knowledge, skills, and ability (KSA) codes, descriptions, and names. These are finite descriptions of the types of labor required to fulfill specific cybersecurity roles. NCAE KUs similarly state required outcomes and topics that universities must cover to maintain their designation. The table below shows how different jobs in cybersecurity require respective NCAE KUs.

Table 1. *Seven Technical and Fundamental Skills that Align with the Core Disciplines (CD) of the Center of Academic Excellence in Research (CAE-R) Programs*

Technical & Fundamental Skills	CAE Knowledge Units (KUs)
1. Operate and Maintain 2. Analyze 3. Collect and Operate 4. Oversee and Govern 5. Securely Provision 6. Investigate 7. Protect and Defend	**Technical Core:** Basic Networking **Technical Optional:** Advanced Network Technology and Protocols, Network Technology and Protocols **Systems Technical Core:** Basic Cryptography, Basic Networking, Network Defense, Certification and Accreditation, Foundational Cybersecurity Foundations, Basic Scripting and Programming **Non-Technical Core:** Security Risk Analysis, Policy, Legal, Ethics and Compliance, Cyber Threats **Combination of Non-Technical & Technical Optional:** Basic Cyber Operations, Cyber Crime, Digital Forensics, Privacy, Cybersecurity Planning and Management, Operating Systems Concepts, Cybersecurity Planning and Management, Data Administration, Database Management Systems, Databases, Linux System Administration, Operating Systems Administration, Windows Systems Administration, Web Application Security, Cyber Security Ethics, Advanced Network Technology and Protocols, Digital Forensics, Formal Methods, Intrusion Detection / Prevention Systems, Network Security Administration, Software Reverse Engineering, Software Security Analysis, Vulnerability Analysis, Advanced Algorithms, Advanced Cryptography, Algorithms, Hardware / Firmware Security, Introduction to Theory of Computation, Penetration Testing

The Hard Skills of cybersecurity focus on protecting networks and data from digital threats. Cybersecurity safeguards sensitive data and systems from unauthorized access and cyber threats. Developing technical aptitude requires one to learn cyber fundamentals that

support protecting infrastructure and assets, as well as the ability to comprehend hacking principles. Technical aptitude should include the core disciplines defined by the NCAE programs to maximize the potential of securing a career in cybersecurity. The workforce skills deficit spans from recruits to top-tier management, encompassing cloud security, threat intelligence analysis, incident response, network security, encryption, and vulnerability management (O'Flanary, 2024).

Soft Skills

Specific soft skills are in high demand, depending on the career or job sector. Those interested in pursuing a career in cybersecurity should have effective communication and problem-solving skills. Professionals must understand legal and ethical issues. In the cybersecurity sector, a combination of hard and soft skills provides understanding in how hacking occurs in various areas such as cloud security, computer forensics, blockchain security, artificial intelligence (AI), programming, and IoT security. These skills will help individuals become security experts who understand the cyber environment and identify malicious activity (Karan, 2024).

Soft skills are sometimes referred to as power and/or psychological skills. Being enthusiastic and possessing the ability to network, communicate, actively listen, problem solve, manage time, and work with others are all attributes' employers value (Krakoff, 2024). When it comes to careers in cybersecurity, it's not different. Table 2 below highlights how various soft skills necessary for pursuing careers in information security and cyber defense align with the seven core (CAE) disciplines.

Table 2. *Mapping Soft Skills to the Seven Core (CAE) for Pursuing Careers in Information Security and Cyber Defense*

Core Disciplines	Cybersecurity Attributes	Soft Skills						
		Team work	Problem -Solving	Communication / Interpersonal	Adaptability	Critical Thinking	Time Mgmt	Detail Oriented
Principles	Domains, Resources, Privileges, Layering	X	X	X	X	X	X	X
Security Mechanisms / Functionality	Cryptography, Virtualization, Biometrics	X	X	X	X	X	X	X
Architectures	Network Models, Critical Infrastructure Security	X	X	X	X	X	X	X
Assurance	Software, Hardware, Modeling	X	X	X	X	X	X	X

Operations	Configuration, Security Automation	X	X	X	X	X	X	X
Analysis	Forensic, Data Mining, Audit	X	X	X	X	X	X	X
Non-technical CD Issues	Legal Issues, Policy Issues, Privacy	X	X	X	X	X	X	X

Cyber Instructor Career Pathway

From this analysis, the typical career pathway for a cyber professional not only requires hard, technical skills, but a subset of soft skills. Required job tasks are based in the technical information and require interpretation across multiple disciplines. The tasks emphasize communication and problem-solving, and these skills are usually context specific. The ability to teach these skills its own specialized skillset.

The Department of Defense (DoD) (2021) has defined a Cyber Instructor Career Pathway with tasks and KSAs. While the foundational KSAs relate to cybersecurity, most Core KSAs and Tasks are soft skill and teaching related. For example, Task T0519 is "Plan and coordinate the delivery of classroom techniques and formats (…) for most effective learning environment" (DoD, 2021, p. 6). Ability A0016 is the "Ability to facilitate small group discussions" (DoD, 2021, p. 7). These soft skills often require hands-on practice and experience to implement appropriately. Cybersecurity instructors have a high number of these skills in their job role definition. However, these soft skills are ancillary to the NCAE KUs. Simply, the current focus of NCAE KUs for designation are mostly technical. Without more specialization, these KU-aligned programs are only preparing cyber professionals generally.

In 2024, the cybersecurity discipline is maturing and gaining recognition as evidenced through the various initiatives to define curriculum, job roles, and career pathways. Progressive programs have many opportunities to map what they teach to what best helps students obtain gainful employment and meet industry demand. It is a tall task, not only to define what should be taught, but to also find professionals who can teach it. Institutions that aim to bolster our nation's cybersecurity workforce should focus on developing programs that cultivate the hard and soft skills highlighted in this study.

Institutional Context and Educator Role

Andrew Spragg, Marymount University

Establishing criteria for successful growth in developing cybersecurity educators in an ever-present development pipeline requires structural alignment toward enhancing the quality throughput of educational programs. Educators are the backbone of the pipeline, where college and university educators focus on splitting the expectations between

curriculum development, research, and student education. These three phases create silos of expectations and chasms of influence on what is taught to the future workforce. Furnell (2021) depicts the requirement of getting the right skills in the workforce as a critical function of the pipeline. The criticality of knowledge, skills, and abilities (KSAs) requirements in the foundation of cybersecurity education and workforce development is the key to growth in the progress of effective and successful professionals.

Conklin et al. (2014) consider the curriculum development in the structure of educator requirements. This research set the curriculum expectations around "outcome objectives and fundamental resource elements such as laboratories and instructors" (Conklin et al., 2024, p.2008). Building a pipeline of education allowed for an agile means to create educational opportunities for many individuals. Educators are needed to facilitate multiple functions in the higher education community which includes developing curriculum, conducting research, and teaching the upcoming generations of cybersecurity professionals.

Educators often fall into a specific college or university unit focused on engineering, computer science, or information technology. Typically, specific job-roles within the university reinforce where faculty members spend their time. Tenure-track faculty members may have a research and publishing requirement while teaching faculty have a higher courseload. In a small or developing program, these requirements can be blurred. These programs usually emphasize technology and frameworks that drive a technical focus and potentially deprioritize the balance of the other functions.

Knowledge areas continue to develop over decades to enhance the curriculum and will continue to struggle to stay up to date with the hyper-speed innovation. As the curriculum is developed and approved through institutional requirements, the struggle exists to maintain the pace of the advancing threats the cybersecurity workforce is working to contain. Cybersecurity has evolved beyond expertise in computer science and now includes topics in other disciplines such as law, policy, healthcare, finance, and beyond (Bate, 2018, p. 27). This creates gaps in the theory of curriculum development that leave items on policy, business awareness, and even how to teach cybersecurity out of the equation. In addition to discipline expertise, Langner et al. (2023, p.3) continue to separate beyond the functional topics in technical skills to include the soft skills such as teamwork, problem-solving, and communication. Cybersecurity learning is viewed as an interdisciplinary field that may need more clearly defined pathways, job roles, and requirements (Mukherjee et al., 2024). The ability to build on technical skills, including policy, law, governance, and risk will help to grow the successful criteria for the cybersecurity workforce.

Leadership in higher education must balance the incentives toward developing a well-rounded and effective cybersecurity workforce. Bate (2018, p.29) identified the difficulty in maintaining the current curriculum, experienced educators, and competing for skilled experts to educate the workforce while struggling with tenured faculty's focus, which is

referenced as “generally focused on foundational research within a narrow specialty, not the newest technology.” Research on the newest technology takes focus and a high degree of effort to ensure the innovation continues to facilitate the expected growth by higher education.

U.S. institutions of higher education also have differing missions, priorities, and business models, and serve different populations with different needs. As a complex organization, there are always competing interests for funding and initiatives resulting in a lack of institutional support for an individual program. This includes various degrees of administrative support, physical space for lab environments, or the availability of teaching assistants and/or adjuncts.

Cybersecurity Educators

Jason Hammon, Western Governors University

Despite the complexities of university governance, there is a high market demand for cybersecurity professionals to teach undergraduates. Assuming this traditional framework of higher education, the primary profile of “Cybersecurity Educators” are university professor, and they are in high demand. These professors are often academics having earned terminal degrees in Philosophy (PhD) or Science (DSc). Due to the recency of the discipline, today’s cybersecurity professors usually have backgrounds in the wider field of Computer Science. Like the wider market demand, there are unique market dynamics that impact who is available to teach.

Cybersecurity Faculty Demand

Citing from *Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments*, the rate of faculty hiring has grown at a much slower pace than undergraduate enrollment (National Academy of Sciences, Engineering, and Medicine, 2018, p. 57). Using Craig Will’s recent work (2023) in analyzing tenure track job postings for CS faculty, in 2023, 423 institutions sought to fill close to 865 tenure-track faculty positions in Computer Science. The study compares research universities to universities that focus more on MS and BS/BA’s. The findings show that research schools are typically advertising more than 1 position and, for the first time in the 9 years, the most interest is shown in Artificial Intelligence/Data Mining/Machine Learning (AI/DM/ML). For MS and BS/BA Universities, the findings show that most universities are looking for 1 single open position and that Security has the highest interest. Total Security-related job postings account for 18% of total postings, which is representative of the past five years. The Security group of postings was the top requested category among 17 other categories for last 5 years.

In a Georgetown Center for Security and Emerging Technology report, Zwetsloot and Corrigan (2022) explore the demand for a Computer Science similar field in Artificial Intelligence. Their evidence suggests that there is also a gap between the supply of

instructors and the demand for AI education. They conclude that the shortage of faculty due to PhDs leaving academia for industry is misattributing the root cause, citing little distortion to the job market and the interest in students to enter academia. Instead, they suggest that the issues are more related to the inability of universities to create more faculty positions, due to budgetary constraints. The paper suggests several policy interventions aimed at facilitating faculty hiring, incentivizing industry to support university education, and expanding access to data and computing resources.

Faculty Supply

While the discussion so far has settled on demand, other data points illustrate the decreased supply of individuals with doctoral degrees. IPEDs 2022 data for the Computer and Information Systems Security/Auditing/Information Assurance Doctor's degree-research show a total of 118 graduates from 7 total universities (National Center for Education Statistics, 2022, CIP Code 11.1003). This low number is likely dependent on differences in reporting, as the 2022 PhD graduates for the wider collection of CIP Codes of Computer and Information Sciences (CIP Code 11.07) in IPEDs is 2,799.

The Taulbee Study presents a subset of these awards but provides a greater picture of terminal degree graduates (referenced further as "PhDs"). For same year comparison, in 2022 the Taulbee survey reported 1,000 fewer PhDs at 1,799 (Computing Research Association, 2022). The latest survey, from 2023, reports 1,883 PhDs produced (Computing Research Association, 2023).

In this data set, only 4% or 79 graduates reported a specialty in "Security/Information Assurance." With 65% of this subset (51 graduates) going into industry, only 28 graduates reported employment at a tenure track, postdoc, teaching, research, or other academic position. This results in a total pool of 15 specially trained cybersecurity instructors added to the work force and less than 1% of the total PhDs reported produced.

Cybersecurity Faculty Supply and Demand

With Will's Study suggesting there were 156 Cybersecurity positions open in 2023 and the Taulbee study showing 15 PhD's produced specific to Cybersecurity, the demand exceeds the supply by a factor of 10! In aggregate, The Taulbee's survey's 1,883 PhDs reports that only 435 or 23% sought traditional academic positions in North America. Notably, 57.5% of the total went into industry. With 865 open positions, and 435 potential applicants, the demand is still twice the number of PhDs produced. In a ballpark range, there is an underproduction of Cybersecurity PhD of between 2 and 10 per every PhD produced. These studies and reports have data limitations that can be explored in depth in the individual reports.

Faculty members with PhDs are not the only cybersecurity educators available. Hiring qualifications differ by department and institutions along with experience and qualification

requirement. Typically, IHLs must justify to their accreditors their faculty expertise; advanced degrees are among the easiest ways to meet the requirement.

Even if requirements for an advanced degree were dropped to a MS, the potential labor supply would be expanded. IPEDs 2022 data for the Computer and Information Systems Security/Auditing/Information Assurance Master's degree-research show a total of 6706 graduates from 174 total universities (National Center for Education Statistics, 2022, CIP Code 11.1003). However, MS degrees in Cybersecurity typically focus on subject matter to further expertise, rather than job preparation for an undergraduate teaching career.

In summary, research points to an underproduction of Computer Science PhDs and related fields. The demand for more PhDs exists, especially at research universities. Other schools also seek someone to teach Cybersecurity, with a preference for a PhD. These universities and programs must lean on other institutional strategies and adjuncts to meet the need. Even with a surge in PhD enrollment and PhD capacity, any gain in production is gradual and will take years before influencing the supply due to the length of PhD programs.

Pay Gap

Oluwatomisin Giwamogorewa, Marymount University
Sapol Jirapanjavat, Marymount University

The job role "Cybersecurity educator" is one position in competition among many potential positions and is ultimately filled by a person looking for a salary. Unfortunately for our objective, this position is compensated at a rate lower than more common cybersecurity positions, despite requiring higher credentials. According to data provided by O*NET, the role "Computer Science Teacher, Postsecondary" (or similarly "Engineering Teacher, Postsecondary), often requires more than five years of experience, extensive skills, knowledge, and experience, and a master's degree or PhD for median wages of $96,000 - $106,000. Related professional positions, such as "Information Security Analysts" or "Information Security Engineers" have less stringent experience (several years to a "considerable amount" of work-related experience) and may require only a bachelor's degree for median wages of $104,000 to $120,000.

Although the prior analysis shows that instructor openings are double what is estimated by this tool, the O*Net platform can be used to show relationships between different job roles. In terms of job openings, Computer Science and Engineering Teachers are projected to have 385 positions a year while Information Security Analysts and Information Security Engineers have projected job openings of 2,515 per year.

The estimated industry role pays $10,970 (10.79%) higher than academia (from the closest similar job role) and has 2,130 (553.25%) projected job openings significantly higher than academia. In education requirements, 76 % of information security careers required a bachelor's degree as compared to teacher professions that require at least a master's degree level.

While a broader analysis of salaries and job openings is always interesting to professionals in the field (ISC, 2024), O*Net data points to the conclusion that professional can make more money with less education in industry than at the university. Other sources also point toward the same general trend.

Literature Review Summary

The literature review has demonstrated that recent and rapid technology innovation has led to a high demand for cybersecurity professionals. The high demand results in many initiatives to build the cyber talent pipeline. As more people enter the pipeline, market opportunity, strategic and spontaneous, increases for education incumbents and new entrants. These providers need experienced cybersecurity educators.

In the university setting, more students are demanding Computer Science and Cybersecurity courses. Academic and industry communities, along with state and federal government, are responding by providing standards and guidelines with varying degrees of efficacy. CAE schools are the premiere structure for training cybersecurity talent at the undergraduate level but are generally not focused on training cybersecurity educators.

Given the unique context and missions of the university, the focus is typically on building research and prestige than on educating cybersecurity graduates. The traditional model of production for faculty members is based on exclusivity and research rather than the aim of building a teaching workforce. The number of terminal degrees or PhDs produced is also much lower than the enrollment surge for technology education, notwithstanding the fact that many PhDs leave the university for higher salaries in industry.

Universities looking for educator talent have traditional high qualifications and extensive job responsibilities. The talent pool for educators is shallow due to the low supply. There is also a pay and education gap between industry and the university, incentivizing students to pursue more lucrative roles on a faster timeline.

Snapshot of Cybersecurity Education in 2024

Mike Morris, Western Governors University

Thus far, we have reviewed the literature surrounding the history and "development" of Teachers, Faculty, and Instructors, specifically for undergraduate level education. These faculty are in-demand and do an important job. The literature shows that these cybersecurity educator challenges, or similar challenges, have existed for years. To our audience readers, you may have seen many of these factors in your own education, in trying to manage your workforce supply, or in teaching the ever-increasing number of students in your classrooms.

Now, we move to the "recognition" aspect of *Champion the Development and Recognition of Teachers, Faculty, and Instructors as Part of the In-demand Workforce*. Given that many of these issues were identified nearly a decade ago, are these real concerns? Are faculty members really in demand in 2024?

As a second initiative to determine the current state of the issue, the project team developed a mixed-method survey to examine the scope and significance of the cybersecurity educator workforce gap at NCAE-C colleges and universities in the United States.

This research provided an opportunity for three project members to analyze the survey data and provide conclusions based on their analysis. While the analytical methods slightly diverged based on tools, experience, and research interests, the data is straightforward and presents a compelling story. In this section, we will present the quantitative results from survey responses presented by different team members. After the conclusions, an in-depth qualitative analysis of the open responses is presented.

A Survey of Cybersecurity Faculty in NCAE-C Schools

The Cybersecurity Educators Workforce Gap Project Team developed a mixed-method survey via Microsoft Forms to examine the scope and significance of the cybersecurity educator workforce gap at colleges and universities in the United States. The survey contained 22 questions (Q1-Q22). Key points of inquiry include current staffing levels, recruitment, strategic planning, and major obstacles pertaining to the educator workforce gap. The survey was distributed to approximately 450 colleges and universities designated as National Security Agency National Centers of Academic Excellence in Cybersecurity (NCAE-C) in March 2024. Most survey respondents were NCAE-C program administrators at their respective institutions. 105 responses were received from 42 different states.

We highlight these key findings:

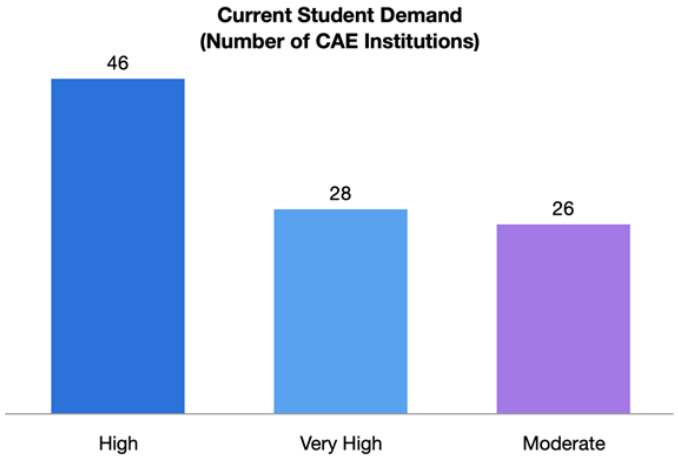
- **Research Finding 1:** Student demand is rising for cybersecurity education programs.
- **Research Finding 2:** NCAE-C institutional leadership views cybersecurity education as a strategic priority.
- **Research Finding 3:** Universities are hiring with the intent to expand the number of educators at their institution, but most efforts are small and local.
- **Research Finding 4:** Hiring efforts are affected by the limited supply of candidates and the budget and funding limitations of the institutions.

Student Demand

Oluwatomisin Giwamogorewa, Marymount University
Sapol Jirapanjavat, Marymount University

At the schools surveyed, participants report that the demand for cybersecurity courses is high. Almost three-quarters of respondents (74%) report the demand as either high or very high (see Figure 3). There were no responses in the categories of “Very Low” or “Low.”

Figure 3 - *CAE institutions' perception of the current student demand*



Of the 100 CAE institutions, 89 agreed that this student demand trend pertains to the next 3-5 years (see Figure 4). Most respondents (83) also predict that that cybersecurity education will be a growing field (see Figure 5, agree and strongly agree combined).

Figure 4 *Student Demand in the next 3-5 years*

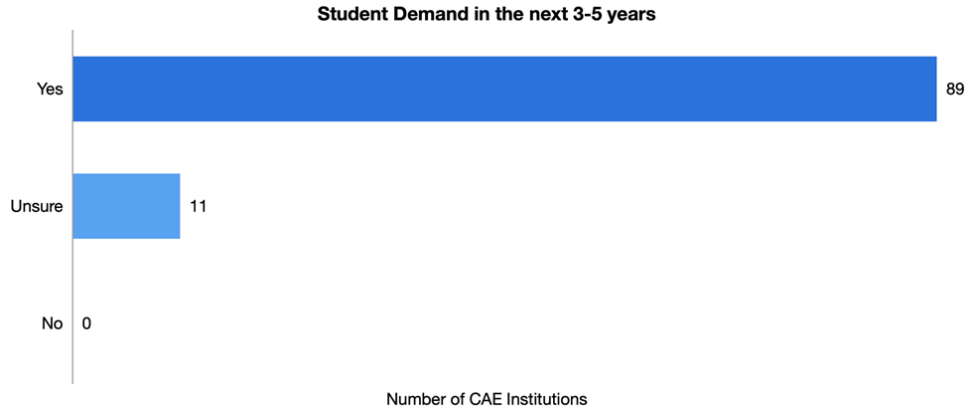
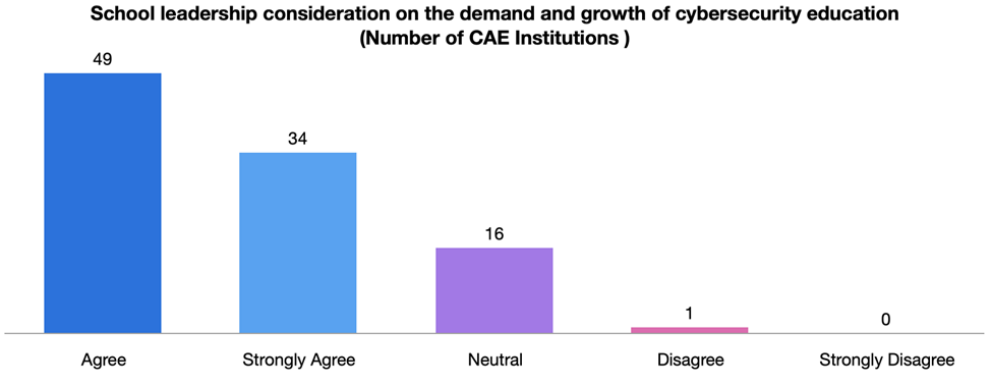


Figure 5 *School leadership consideration on the demand and growth of cybersecurity education*



Faculty Hiring

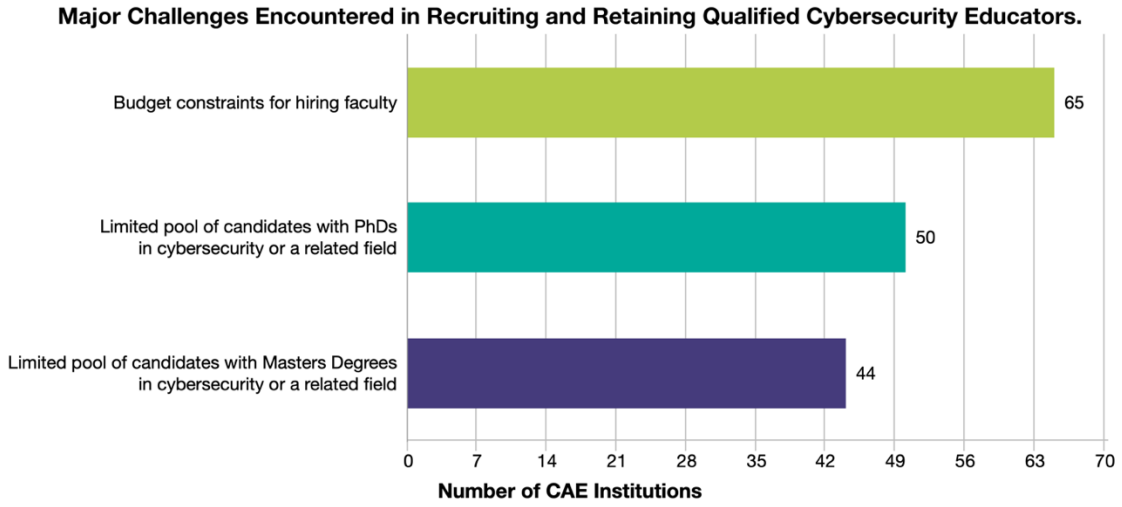
Given the rising student demand and the current shortage of cybersecurity educators, these responses indicate a significant shortfall in the supply of qualified instructors in this field, in line with general workforce shortage. Moreover, institutions are encountering considerable difficulties in hiring skilled and experienced educators. For instance, one respondent reported an ongoing search for a qualified educator that has spanned three years without success.

Other respondents shared:

- "It is difficult to hire qualified adjunct and full-time faculty. The pay gap that exists between education and industry jobs is hard to overcome."
- "Most cybersecurity professionals that have MS degree are not willing to take the drop in salary to teach unless they have a calling to be professors."
- "We are a rural school with low wages, as we do find instructors, the Community College that is 40 minutes away, offers our instructors a 25% increase in pay to go work for them. We have supplied the college up the road…with 4 new cyber employees. This makes it hard to keep qualified instructors here…"

Additionally, of the 100 CAE institutions, the survey shows 65% have budget constraints for hiring faculty, 50% have a limited pool of candidates with PhDs in cybersecurity or a related field, and 44% have a limited pool of candidates with master's degrees in cybersecurity or a related field (see Figure 6).

Figure 6 *Major Challenges Encountered in Recruiting and Retaining Qualified Cybersecurity Educators*



Based on the research previously cited in the literature review, there are other cybersecurity positions with significantly more job openings available, higher compensation, and lower time and financial investment required for education than becoming an instructor. Moreover, the pay gap between educational and non-educational roles in cybersecurity remains a significant concern.

Curriculum Development

As also noted in the literature review, curriculum development is one of the significant concerns of NCAE institutions. Respondents relay concerns related to expanding program offerings, creating cybersecurity-related minors, including more hands-on and lab learning, and updating the curriculum to include the latest in cybersecurity threats, technologies, and best practices. As the threat landscapes increases, instructors constantly work to integrate the curriculum with the skills needed to fulfill the job market. For instance, one respondent reported that the increase in hands-on learning attracts more students to their program.

Other respondents shared:

- "A cybersecurity course was just approved in the general education program. So, students will be able to take an intro cybersecurity course that will help them graduate, even if they choose not to pursue a cybersecurity degree."
- "We met with chief security/information officers to solicit the skills needed for their employees. And we integrated them into our curriculum, whenever possible."
- "We plan to expand our curriculum to include the latest in cybersecurity threats, technologies, and best practices. This will involve both the introduction of new courses and the updating of existing ones to ensure comprehensive coverage."

While most responses indicate individual initiatives, these schools have increasing opportunity to improve curriculum. According to Crabb et al. (2024), NCAE-C provides the required standard cybersecurity course content included in curricula; however, institutions could work with NIST, ACM, and IEEE to ensure their curricula is up to date with industry standards. Crabb et al. (2024) show there is still deviation between the skill level achieved by cybersecurity graduates and the expected skill level of cybersecurity professionals. Generally, there is limited research evaluating the efficacy of cybersecurity pedagogies, including methods, tools, and content in these areas.

Other respondents have leaned on many cybersecurity industry certifications (such as CompTIA, SANS, Cisco, Microsoft, AWS, etc.). These certification requirements are also crucial in crafting effective cybersecurity instructional pedagogy, especially for widely used technologies.

Finally, the inclusion of cybersecurity within general education programs provides opportunity for students in other fields of study. These introductory courses help promote cybersecurity and provides exposure to the high demand and high compensation. These students might consider cybersecurity professions within their fields of study in the future since cybersecurity has broader implications across industries.

Qualitative Analysis

Clinton L. Ilges III, Marymount University

The quantitative analysis of the responses indicates NCAE-C educational institutions face a cybersecurity educator shortage in an environment that is experiencing increasing demand by incoming student populations. The NCAE-C educational institutions note a competitive job market for cybersecurity talent and internal budget constraints for hiring faculty as contributing factors to the shortage. Most respondents indicate this gap is a strategic priority for institutional leadership.

The qualitative analysis supports the quantitative data while providing additional insight into the strategies and mechanisms NCAE-C institutions consider when addressing the cybersecurity educator workforce gap. Forty-one percent of NCAE-C institutions consider hiring more educators a top priority. However, numerous barriers exist, and institutions struggle to maintain a consistent cadre of qualified educators.

Methodology

A three-stage grounded theory coding process was utilized for the qualitative analysis of three survey questions (Q15, Q21, Q22). The questions were analyzed for relevant concepts. The concepts were manually coded and labelled with descriptive keywords (or key phrases). The “Code Frequency Analysis” function in MaxQDA Analytics Pro platform was utilized to calculate final keyword frequencies across the 105 responses.

Approximately 310 unique keywords were manually coded in stage one. The keywords from stage one were synthesized and grouped into approximately 26 related categories in stage two. The 26 related categories from stage two were grouped into eight major themes in stage three. Five of the eight themes are currently being utilized by NCAE-C respondents to manage the cybersecurity educator workforce gap crisis. These include collaboration with stakeholders, recruitment pipelines, recruitment initiatives, retention initiatives and expanding cybersecurity programs.

Collaboration with Stakeholders

A large group (46%) of NCAE-C institutions consider collaboration and partnerships a top priority in addressing the cybersecurity educator workforce gap crisis. Categorical analysis indicates approximately one-third of respondents collaborate with industry to fill multiple gaps within institutional resource allocations. Resource allocation categories are designated as "Institutional Support” and “Student Support”.

“Student Support” includes providing experiential learning through mechanisms such as cyber ranges and cyber camps. Industry also provides students with learning opportunities through internships, apprenticeships, mock hiring boards and other collaborative engagements. These engagements are instrumental in providing students with the

knowledge, skills and abilities required to work in industry. These collaborations often lead to full-time employment opportunities post-graduation.

Recruitment Pipelines

Industry collaborators overwhelmingly support institutions through existing recruitment pipelines. Skilled industry professionals and subject matter experts (SME) are utilized as adjunct educators and curriculum developers at NCAE-C institutions. SMEs lack the academic credentials (degrees) required for tenured faculty positions but are technically skilled professionals with current "real-world" experience. Cybersecurity professionals with advanced degrees are often deterred by the industry-academia pay gap. Academia is unable to compete with industry pay scales and most industry professionals are unwilling to take a significant decrease in pay to teach full-time.

NCAE-C respondents cite high turnover rates due to low salaries and increased burnout rates due to high course loads among adjunct educators. High turnover in conjunction with hiring gaps lead to vacated positions going unfilled due to lengthy onboarding processes for newly hired educators. Adjunct educators routinely provide their own material for courses and often leave a curriculum gap when they vacate a position. This often forces unskilled educators to teach the course or remove it from the curriculum. Adjunct educators focus on classroom engagement and do not assist with other administrative duties required of tenure-track educators. Some of these duties include advising students, maintaining NCAE-C designations, and conducting research

Recruitment and Retention Initiatives

While most NCAE-C respondents employ this model to fill current gaps, reliance on adjunct educators to maintain a NCAE-C program is unsustainable. The widening of the industry-academia pay gap exacerbates reliance on industry adjuncts. About a quarter (26%) of NCAE-C institutions have begun to broaden recruitment pipelines as part of new initiatives to recruit and retain additional educators. Numerous respondents reported recruiting current students, recent graduate students, and former alumni to teach cybersecurity courses. Several other institutions have cross-trained adjacent faculty, recruited advisory board members and sponsored visas for international educators. Some institutions rely on other higher education partners to share instructor pools with them. Respondents reported collaboration with other stakeholders including K-12 institutions, cybersecurity advisory boards and state and federal entities.

It should be noted respondents reported exceptionally low collaborations with government entities and no recruitment pipeline exchanges were reported. This phenomenon requires additional research as various departments and agencies within government entities can be utilized for institutional and student support. Support includes awarding grants, providing student engagement opportunities, and providing subject matter expertise for instruction and curriculum development.

Expanding Cybersecurity Programs: The Double-Edged Sword

The expansion of cybersecurity programs is a widely stated goal:

- 78% of respondents reported they are actively recruiting to expand the number of cybersecurity educators at their institution.
- More than half of the respondents (65%) were trying to fill between one and three active vacancies.
- Budget constraints have a significant impact on filling active vacancies.
- Respondents reported high turnover rates and increased burnout among adjunct educators.
- Approximately one-third of respondents (33%) indicated they are expanding cybersecurity programs to meet the increasing demand for cybersecurity education.

Student demand is increasing. Educator demand is increasing. Faculty vacancies remain unfilled. Yet, additional cybersecurity courses, certificates, degrees, and programs are being instituted at a fast pace within NCAE-C institutions. This model seems counter-intuitive to balancing the cybersecurity educator workforce gap crisis. Some respondents reported additional faculty positions could not be justified without demonstrating increased (overwhelming) demand for cybersecurity education by incoming student populations. NCAE-C institutions need to increase cybersecurity programs to meet student demand and justify additional faculty positions. However, this must be accomplished with a cadre of mostly unskilled tenure-track faculty and a revolving door of highly skilled, overworked, and underpaid adjuncts. A crisis indeed.

Bridging the Gap

NCAE-C institutions are at a tipping-point and "still haven't found what they're looking for" regarding cybersecurity educators (U2, 1987). Research indicates the current models for filling the cybersecurity educator gaps within NCAE-C institutions are not sustainable long-term. Remediation is required to narrow the gaps. NCAE-C respondents report a significant lack of resources in combatting the cybersecurity educator workforce gap. NCAE-C institutions need additional resources. This will require significant collaboration between the NCAE-C institutions and their governing bodies.

The NSA National Cryptologic University (NSA NC-U) is the managing body of the NCAE-C and provides governance and resources for designated institutions (NSA, 2024). The NSA NC-U is uniquely positioned to develop and institute a roadmap for success in combatting the cybersecurity educator workforce gap within NCAE-C institutions. This research serves as the necessary bridge between identifying current NCAE-C challenges and providing actionable feedback to the NSA NC-U for review. The researcher advocates for additional resources aimed at narrowing the cybersecurity educator workforce gap within NCAE-C institutions.

Discussion

Our working group's objective is akin to shining a small light on broad field of inquiry. The discussion arising can appear fragmented as we've only can see various pieces and shadows. The first point is that the data and research for strong conclusions is nascent and immature—the lot of a rapidly developing field! We invite more researchers to participate in illuminating the landscape of issues.

The next opportunity for discussion ranges into what makes an effective cybersecurity educator. Our assumption is that the typical instructor is one with a terminal degree, but there are many instructors and adjuncts who do the work. This paper has not fully addressed the institutional support and resources need, theories of pedagogy and assessment, and baseline competencies related to the many course subject areas. Future research can be applied by studying the top schools producing the most successful cybersecurity professionals based on the State-by-State Guide to Schools that Hold DHS and NSA NCAE-CD schools list to determine what skills are being produced. Finding exemplar schools is a first step to creating a model or template that meets the objective.

Another limitation of our study is that of only undergraduate degree programs. During our research, we found that most new cyber professionals are sourced from other roles and not from a traditional undergraduate background. There is a wide variety of informal learning that is taking place along with a strong landscape of certifications. What do hiring authorities rely on to meet their workforce gaps? We have not discussed the scope and variety of cybersecurity-adjacent feeder lanes.

Given our charge to *recognize teachers, faculty, and instructors as part of the in-demand workforce*, we wave our light vigorously and invite others to add to the discussion.

Recommendations

We conclude with a few recommendations particular to our study as well as reiterating recommendations found within our research.

Our first recommendation is recognition that Cybersecurity is a relatively new field and is a new area of opportunity for industry, government, academia, and, especially, future talent looking to start a career. There are clear efforts to expand the talent pipeline which further creates opportunities for cybersecurity educators and universities. IHLs, by themselves, will not have a national strategy to address the gap, however, there are opportunities for coordination, specifically through the CAE network in alignment with government initiatives.

Secondly, the undergraduate demand and the structure of institutions require careful planning and secure, long-term funding. Budgets are often short-term and change with wider demographic cycles. However, the requisite skills for cybersecurity and the emergence of threats in an ever-connected world will continue to increase. An investment in this domain is part of a long-term institutional strategy. These strategies must address the pay gap in this in-demand field and the rising workload on faculty and staff. Further, institutional leadership should engage directly to develop appropriate faculty hiring and targets, improve retention efforts, and consider offering more teaching faculty positions.

Conclusion

Yes. There is a shortage! And it is ongoing! We end where we began, with our Objective 2.6: *Champion the Development and Recognition of Teachers, Faculty, and Instructors as Part of the In-demand Workforce*.

We need teachers, faculty and instructors! Even though this is an old problem, today's CAE institutions see and experience it. There is hiring demand and low supply. Institutions would do well to reassess qualifications, budgets, and curriculum to attract candidates. Candidates are in low supply and must be persuaded in a competitive manner. The status quo will not adequately address the issue.

References

Bate, L. (2018). Cybersecurity workforce development: A primer. *New America,* Florida International University. https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-11-01_183611.pdf

Bingham, A. J. (2023). From Data Management to Actionable Findings: A Five-Phase Process of Qualitative Data Analysis. *International Journal of Qualitative Methods,* (22). https://doi.org/10.1177/16094069231183620

Blazic, B. J. (2021). Changing the landscape of cybersecurity education in the RU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies,* 3011-3036. https://doi.org/10.1007/s10639-021-10704-y

Cabaj, K., Domingos, D., Kotulski, Z., & Respicio, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, 75, 24-35. https://doi.org/10.1016/j.cose.2018.01.015

CAE in Cybersecurity Community. (2022). *What is a CAE in Cybersecurity?* https://caecommunity.org/about-us/what-cae-cybersecurity#:~:text=The%20National%20Centers%20of%20Academic,(CAE%2DIAE)%20program.

Computing Research Association. (2022). *The CRA Taulbee Survey*. http://cra.org/resources/taulbee-survey/

Computing Research Association. (2023). *The CRA Taulbee Survey*. http://cra.org/resources/taulbee-survey/

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering cybersecurity education in the US: an analysis of the critical factors. In *2014 47th Hawaii international conference on system sciences* (pp. 2006-2014). IEEE.

Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024, March 7). A critical review of cybersecurity education in the United States. Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1. http://dx.doi.org/10.1145/3626252.3630757

Cybersecurity Education Guides. (2024). *State-by-State Guide to Schools that Hold DHS and NSA CAE-CD Designations*. https://www.cybersecurityeducationguides.org/dhs-and-nsa-cae-cd-designated-schools-by-state/

Cyberseek.org. (2024). *Hack the gap: Close the cybersecurity talent gap with interactive tools and data.* https://www.cyberseek.org/index.html

Department of Defense. (2021, March 18). The Interagency Federal Cyber Career Pathways Working Group. *Career Pathway Cyber Instructor (712).* https://dl.dod.cyber.mil/wp-content/uploads/ccp/pdf/712_Cyber_Instructor-Career-Pathway.pdf

Dimolfetta, D. (2024). White House cyber czar is working to grow a new generation of cybersecurity workers. Defense One. https://www.defenseone.com/policy/2024/08/how-white-house-cyber-czar-working-breathe-new-life-americas-cybersecurity-workforce/398880/?oref=ds_update_nl&utm_source=Sailthru&utm_medium=email&utm_campaign=Defense%20Systems%20Update:%20August%2020%2C%202024&utm_term=newsletter_ds_update

Field Effect Software Inc. (2024, May 29). *Cybersecurity Education: Overcoming the cybersecurity talent shortage in 2025.* https://fieldeffect.com/blog/overcoming-the-cybersecurity-talent-shortage#:~:text=When%20treated%20as%20a%20global,ISC)2%20Cybersecurity%20Workforce%20Study

Frechtling, J. & Sharp Westat, L. (1997). *User-Friendly Handbook for Mixed-Method Evaluations.* Directorate for Education and Human Resources. Division of Research, Evaluation and Communication. National Science Foundation.

Furnell, S. (2021). The cybersecurity workforce and Skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Furstenau, L. B., Scott, M., Kipper, L., Homrich, A., Cardoso, T., Abri, A., . . . Cobo, M. (2020). 20 Years of Scientific Evolution of Cyber Security: a Science Mapping. *Proceedings of the International Conference on Industrial Engineering and Operations Management,* (pp. 314-325). Dubai.

Glaser, B., & Strauss, A. (1967). *The Discovery of Grounded Theory*. Aldine.

Healey, J. (2023, June 2) *Twenty-Five Years of White House Cyber Policies.* Lawfare Media. https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies

ISC2. (2023). *ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Security Workforce.* https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e

ISC2. (2024, April 11). *Research: How Much Do U.S. Cyber Professionals Make* https://www.isc2.org/Insights/2024/04/How-Much-Do-US-Cyber-Professionals-Make

Joshi, A., Doyle, S., & Perucica, N. (2023, December 29). *Here's how to address the global cybersecurity skills gap*. World Economic Forum. https://www.weforum.org/agenda/2023/05/the-cybersecurity-skills-gap-is-a-real-threat-heres-how-to-address-it/

Karan, R. (2024). 9 Most In-Demand Cybersecurity Skills To Learn In 2024. https://www.shiksha.com/online-courses/articles/most-in-demand-cybersecurity-skills-to-learn/

Karahan, S., Wu, H., & Armistead, L. (2019). Evolution of US Cybersecurity Strategy. *International Conference on Cyber Warfare and Security,* (pp. 168-176).

Koslosky, L. Crawford, A. Abdulla, S. (2023). Building the Cybersecurity Workforce Pipeline. A Study of the National Centers of Academic Excellence in Cybersecurity. https://cset.georgetown.edu/publication/building-the-cybersecurity-workforce-pipeline/

Krakoff, S. (2024). *Top Cybersecurity Skills in High Demand*. Champlain College Online. https://online.champlain.edu/blog/top-cybersecurity-skills-in-high-demand

Langner, G., Furnell, S., Quirchmayr, G., & Skopik, F. (2023). A comprehensive design framework for multi-disciplinary cyber security education. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 105-115). Cham: Springer Nature Switzerland.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). *A Brief History of the Internet*. Internet Society. https://www.internetsociety.org/internet/history-internet/brief-history-internet/

The Lightcast Quarterly Cybersecurity Talent Report. (2024) Lightcast. https://lightcast.io/resources/research/quarterly-cybersecurity-talent-report-june-24

Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). *Strategic approaches to cybersecurity learning: A study of educational models and outcomes*. MDPI. https://doi.org/10.3390/info15020117

National Academies of Sciences, Engineering, and Medicine. (2018). Assessing and responding to the growth of computer science undergraduate enrollments. The National Academies Press. https://doi.org/10.17226/24926

National Center for Education Statistics. (2022) "Integrated Postsecondary Education Data System (IPEDS)," http://ncsesdata.nsf.gov/webcaspar/

National Cryptologic University. (2024). *Overview*. *https://www.nsa.gov/academics/national-cryptologic-university/*

National Cybersecurity Training & Education Center. (2024). *NICE Framework and CAE Knowledge Units (KUs)*. https://www.ncyte.net/faculty/faculty-resources/nice-framework-and-cae-knowledge-units-kus

National Initiative for Cybersecurity Careers and Studies (NICCS). (2024a). *Cybersecurity Education and Training Assistance Program*. https://niccs.cisa.gov/cybersecurity-career-resources/cybersecurity-education-and-training-assistance-program)

National Initiative for Cybersecurity Careers and Studies (NICCS). (2024b). *Cybersecurity Instruction*. https://niccs.cisa.gov/workforce-development/nice-framework/work-role/cybersecurity-instruction

National Security Agency. (2024). *National Centers of Academic Excellence in Cybersecurity*. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

O'Flanary, K. (2024). *The cyber security skills shortage: What skills are missing?* https://www.itpro.com/security/the-cyber-security-skills-shortage-what-skills-are-missing

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). Sage Publications, Inc.

Paul, S. A., Gjorgov, E., English, I. B., Rajkumar, Y., & Glasgow, R. (2023). What are the Criteria and Standards Used to Appoint Adjuncts, Assistants and Associate Professors, and How Do Their Roles and Functions Differ in a University? *Stallion Journal for Multidisciplinary Associated Research Studies*, *2*(3), 11-19. https://doi.org/10.55544/sjmars.2.3.3

Richberg, J. (2024, January 24). *The Power of Public-Private Partnerships | CISO Collective*. Fortinet Blog. https://www.fortinet.com/blog/ciso-collective/the-power-of-public-private-partnerships

Struggling with Cybercrime? Turn to Public-Private Partnership. (2015). Palo Alto Networks. https://www.paloaltonetworks.com/cybersecurity-perspectives/struggling-with-cybercrime-turn-to-public-private-partnership

U2. (1987). I Still haven't Found What I'm Looking For [Song]. On *The Joshua Tree*. Island Records.

United States Department of Labor. Bureau of Labor Statistics. (2024a, August 29). *Occupational Outlook Handbook: Computer and Information Technology Occupations.* https://www.bls.gov/ooh/computer-and-information-technology/home.htm

United States Department of Labor. Bureau of Labor Statistics. (2024b, August 9). *Occupational Outlook Handbook: Information Security Analysts*. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

The White House. (2023, July 31). *FACT SHEET: Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America's Cyber Talent | The White House*. The White House; The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%E2%81%A0harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent/

Williams, M. & Moser, T. (2019). *The Art of Coding and Thematic Exploration in Qualitative Research*. International Management Review, 15(1), 45-55. http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v15n1art4.pdf

Wills, C. E. (2024). Analysis of current and future computer science needs via advertised faculty searches for 2023. *Computing Research News*, 36(1). https://web.cs.wpi.edu/~cew/papers/CSareas24.pdf

World Economic Forum (WEC). (2024). *Bridging the Cyber Skills Gap*. https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home

Zimmermann, K. A., & Emspak, J. (2022, April 8). Internet history timeline: ARPANET to the World Wide Web. Future US, Inc.: Live Science. https://www.livescience.com/20727-internet-history.html

Zwetsloot, R., & Corrigan, J. (2022, July). *AI Faculty Shortages: Are U.S. Universities Meeting the Growing Demand For AI Skills?* Center for Security and Emerging Technology. https://doi.org/10.51593/20190049

Acknowledgements

We sincerely thank the colleges and universities that participated in this study. Your collaboration and input were essential to the success of this project and greatly advanced our understanding of the current snapshot of cybersecurity education at NCAE institutions.

Anne Arundel Community College
Baker College
Bellevue University
Binghamton University
Bismarck State College
Blue Ridge Community and Technical College
Boise State University
Bossier Parish Community College
Bowie State University
Brigham Young University
Butler Community College
California State University, San Bernardino
California State University, San Marcos
Central Michigan University
Chippewa Valley Technical College
City University of Seattle
Clark State College
College of Southern Nevada
Columbus State Community College
Community College of Rhode Island
County College of Morris
Dakota State University
Des Moines Area Community College
Eastern New Mexico University - Ruidoso Branch Community College
Eastern Washington University
Embry-Riddle Aeronautical University - Daytona Beach Campus
Fairleigh Dickinson university
Florida International University
Florida Memorial University
Florida State College at Jacksonville
George Mason University
Grand Canyon University
Gwinnett Technical College
Hampton University
Hennepin Technical College
Hinds Community College
Honolulu Community College
Jackson State Community College
Johns Hopkins University
Johnson County Community College
Kean University
Lakeland Community College
Lansing Community College
Leeward Community College
Loyola University Chicago
Macomb Community College
Marymount University
McLennan Community College
Metro State University
Mississippi State University
Missouri University of Science and Technology
Moorpark College
National University
Naval Postgraduate School
Northampton Community College
Northern Kentucky University
Northern Michigan University
Northwest Missouri State University
Norwich University
Oklahoma Christian University
Pueblo Community College
Purdue University Northwest
Roane State Community College
Rowan College at Burlington County
Sacred Heart University
Sinclair Community College
Southern Utah University
St. Mary's University
St. Petersburg College
Strayer University
Suffolk County Community College
Terra State Community College
The College of Westchester
The George Washington University
The University of Texas at San Antonio
Trident Technical College
University of California, Davis
University of Cincinnati
University of Colorado, Colorado Springs
University of Colorado, Denver
University of Dayton
University of Detroit Mercy
University of Findlay
University of Hawaii Kapiolani Community College
University of Maine at Augusta
University of Nebraska at Omaha
University of New Orleans
University of North Florida
University of Puerto Rico - Rio Piedras
University of San Diego
University of South Alabama
University of South Florida
University of Southern Maine
University of Texas at Dallas
University of Washington
Valencia College
Virginia Western Community College
Weber State University
Wichita State University
Wright State University

Appendix A – Key Resources

These resources have been instrumental to forming this paper and for understanding the context of the shortage. We have placed them here with our recommendation.

The Recent Growth of Cybersecurity

Blazic, B. J. (2021). Changing the landscape of cybersecurity education in the RU: Will the new approach produce the required cybersecurity skills? Education and Information Technologies, 3011-3036.

Cabaj, K., Domingos, D., Kotulski, Z., & Respicio, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 24-35.

Furstenau, L. B., Scott, M., Kipper, L., Homrich, A., Cardoso, T., Abri, A., . . . Cobo, M. (2020). 20 Years of Scientific Evolution of Cyber Security: a Science Mapping. Proceedings of the International Conference on Industrial Engineering and Operations Management, (pp. 314-325). Dubai.

Karahan, S., Wu, H., & Armistead, L. (2019). Evolution of US Cybersecurity Strategy. International Conference on Cyber Warfare and Security, (pp. 168-176).

Cybersecurity Career Pathways

Cybersecurity and Infrastructure Agency. (n.d.). Cybersecurity for students. National Initiative for Cybersecurity Careers and Studies. https://niccs.cisa.gov/education-training/cybersecurity-students

CyberSeek. (n.d.). Cybersecurity career pathway. CyberSeek. https://www.cyberseek.org/pathway.html

Occupational Information Network. (n.d.). O*NET Online: See All Occupations. O*NET. https://www.onetonline.org/find/all

The Undergraduate Demand

National Academies of Sciences, Engineering, and Medicine. (2018). Assessing and responding to the growth of computer science undergraduate enrollments. The National Academies Press. https://doi.org/10.17226/24926

Computing Research Association. (2023). *The CRA Taulbee Survey.* http://cra.org/resources/taulbee-survey/

CAE Schools

Cybersecurity Education Guides. (2024). *State-by-State Guide to Schools that Hold DHS and NSA CAE-CD Designations*. https://www.cybersecurityeducationguides.org/dhs-and-nsa-cae-cd-designated-schools-by-state/

Cybersecurity Instruction

National Initiative for Cybersecurity Careers and Studies (NICCS). (2024b). *Cybersecurity Instruction*. https://niccs.cisa.gov/workforce-development/nice-framework/work-role/cybersecurity-instruction

Paul, S. A., Gjorgov, E., English, I. B., Rajkumar, Y., & Glasgow, R. (2023). What are the Criteria and Standards Used to Appoint Adjuncts, Assistants and Associate Professors, and How Do Their Roles and Functions Differ in a University?. *Stallion Journal for Multidisciplinary Associated Research Studies*, *2*(3), 11-19.

Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024, March 7). A critical review of cybersecurity education in the United States. Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1. http://dx.doi.org/10.1145/3626252.3630757

Appendix B – Quantitative Analysis

The quantitative analysis of key points of inquiry indicates NCAE-C educational institutions face a cybersecurity educator shortage in an environment that is experiencing increasing demand by incoming student populations. The NCAE-C educational institutions note a competitive job market for cybersecurity talent and internal budget constraints for hiring faculty as contributing factors to the shortage. Most respondents indicate this gap is a strategic priority for institutional leadership.

The Cybersecurity Educators Workforce Gap Project Team utilized Microsoft Forms to generate a report of the 105 survey responses. The following questions were extracted from the report and correlate to the key points of inquiry.

Q7. How many FULL-TIME cybersecurity educators (instructors, professors, etc.) does your school currently employ?
- 1-5 (71%)

Q8. How many PART-TIME or ADJUNCT cybersecurity educators does your school currently employ?
- 1-5 (63%)

Q9. Are you actively recruiting to expand the number of cybersecurity educators at your institution?
- Yes (76%)

Q10. Specify the number of cybersecurity positions you are trying to fill.
- 1-3 (63%)

Q11. What challenges have you encountered in recruiting and retaining qualified cybersecurity? (Check all that apply)
- Competitive job market for cybersecurity talent (76%)
- Budget Constraints for hiring faculty (66%)

Q12. How do you perceive the impact of the cybersecurity educator workforce gap on your school's ability to meet the student demand for cybersecurity education?
- Moderate to Significant (83%)

Q16. How would you describe the current student demand for cybersecurity education programs at your school?
- High to Very High (74%)

Q19. Do you anticipate an increase in student demand for cybersecurity education programs at your school in the next 3-5 years?
- Yes (88%)

Q20. Your school leadership considers the demand and growth of cybersecurity education as a strategic priority:
- Agree to Strongly Agree (82%)