IS THE NICE CYBERSECURITY WORKFORCE FRAMEWORK (NCWF) EFFECTIVE FOR A WORKFORCE COMPRISED OF INTERDISCIPLINARY MAJORS?

Johanna Jacob jacobj5081@uhcl.edu

Wei Wei wei@uhcl.edu

Kewei Sha sha@uhcl.edu

Sadegh Davari davari@uhcl.edu

T. Andrew Yang yang@uhcl.edu

University of Houston-Clear Lake
2700 Bay Area Blvd
Houston, Texas, USA

ABSTRACT

Cybersecurity is a rapidly developing field in which job titles and role descriptions may vary from one organization to the others. The NICE Cybersecurity Workforce Framework (NCWF) provides a common language to categorize and describe cybersecurity work for organizations to build a strong workforce. As the predominant workforce prescribed by the NCWF is technical in nature, academic efforts targeted towards these career paths are likewise technical. Though technical security education is critical, an equal amount of knowledge outside the technical domain is pivotal to understand sophisticated challenges in cybersecurity. Articulating a concise, inclusive, meaningful, and unifying approach in cyber related education fosters a balanced motivation for students from both technical and non-technical majors (interdisciplinary) to pursue a career in cybersecurity. Towards this end, we analyzed competencies, knowledge, skills and abilities of interdisciplinary roles and other roles introduced in the NCWF; we then highlighted discrepancies observed.

***Keywords**: Cybersecurity Workforce, NCWF, non-technical majors, interdisciplinary*

1. INTRODUCTION

The increasing number of cyber threats and breaches to personal, national, and organizational safety has led to an increased focus on the "human" factors of cybersecurity. According to Cybersecurity Business report, cybercrime damage costs will hit $6 trillion annually by 2021 [1]. These daily occurrences of cyber incidents are posed by cyber criminals, individuals, opportunistic hackers, and professionals who master the strategies for stealing intellectual information and disrupting the business environment.

To combat this, businesses and government sectors focus on holistic, comprehensive cybersecurity solutions by re-assessing the way security is approached and emphasizing significant investments in enhancing the cybersecurity workforce and the talent pipeline. The demand for cybersecurity professionals is exceeding the present number, and estimates predict that more than 200,000 positions are currently unfilled [2]. The Bureau of Labor Statistics forecasts that the need for cybersecurity professionals will increase by more than 22%, adding 27,000 new positions through 2020 [3].

The increase in demand for cybersecurity talent leads to an increasing awareness of the skills necessary to acquire a cybersecure role in the industry. While a good number of technical skills are mandatory to understand a vulnerable cyber environment and propose solutions to resolve them, skills acquired from non-technical interdisciplinary majors also play an equal pivotal role.

2. LITERATURE REVIEW

A balanced cybersecurity workforce incorporates a basic understanding of technical skills along with other baseline interdisciplinary skills such as understanding and formulating policies, practices, risk management, business standards, frameworks, politics, governance and much more. These "Interdisciplinary skills" cover different avenues such as Criminology, Human Psychology, Management, Law, Governance, etc. This demands a "holistic education in cybersecurity".

Cybersecurity education does not pertain to technical studies alone that surround network security, malware analysis, reverse engineering, application security and network security. In fact, the rising number of cyber terrorism and hacking incidents portray the need for cybersecurity with a global perspective. A report from Frost, Sullivan and (ISC) ^{2} depicts that more than 1.5 million positions will be unfilled in the global cybersecurity workforce [4]. To overcome this enormous dearth of cybersecurity talent, businesses are looking for people with traditional technology and interdisciplinary (non-technological) credentials. PayScale, a provider of on-demand compensation and software, states that 87% of recent graduates feel well prepared to hit the fast-paced cyber industry. However, for more than 51% of those graduates, underemployment is the reality [5]. This is due to a massive gap in skills such as communication, ownership, leadership, teamwork, problem-solving and understanding cultural, social, legal, economic and political perspectives in the context of the problem at hand. [5]

Society's dependence on information technology has created a "technological sovereignty" in the education curriculum and has outpaced non-technological, interdisciplinary skills [5]**.** To combat this, infusing political, ethical, social, cultural, religious, and economic perspectives into cybersecurity education fosters a mixture of technical and interdisciplinary skills [6] and enhances preparedness to tackle a cyber related threat or investigate in a better way. This calls for an "Interdisciplinary Cybersecurity".

Ghernaouti-Hélie [8] states that cybersecurity education is "at the crossroads of technological, legal, sociological, economic and political fields, and is interdisciplinary by nature" [8]. This propels the need to leverage the effectiveness of the educational curriculum models [13]. Introducing a global perspective through interdisciplinary studies and employing "cross pollination" of disciplines closes the gap between "technically focused" cybersecurity and the non-traditional backgrounds.

In response to this, a greater collaboration has been initiated between education, research and industry fields. The collaboration has resulted in frameworks and guidelines that demonstrate an increased value for the cybersecurity workforce. In this regard, one of the prominent frameworks is focused on, and its scope for improvement in support of interdisciplinary skills is analyzed in the following sections. "Interdisciplinary" in the context of this paper refers to non-technological, non-computing domains (outside of computer science, computer information systems and information technology) that do not pertain to core cybersecurity.

3. AN ANALYSIS OF THE CRITICAL FACTORS IN THE CURRENT CYBERSECURITY GUIDELINES

The Department of Homeland Security (DHS) and the National Initiative for Cybersecurity Education (NICE) put together the NICE Cybersecurity Workforce Framework (NCWF), also called the *NICE Framework*. In response to the evolving vulnerabilities in the cyber infrastructure, the framework was developed as a reference for workforce development, education, career paths, acquiring credentials for programs in cybersecurity, and/or training purposes. The framework clearly defines cybersecurity work in the form of knowledge, skills, abilities and tasks (called as *KSATs*) [9]. The following section provides a review of the NCWF.

3.1. THE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) FRAMEWORK

The NICE framework consists of several components – Category, Specialty Areas, Work Roles, Knowledge, Skills, Abilities and Tasks [9]. Each category is composed of Specialty Areas, each of which is further composed of one or more work roles. Work roles include Skills, Knowledge, Abilities and Tasks. While categories are the overarching, higher-level groupings in the framework, work roles are the most detailed grouping of cybersecurity related work. There are seven categories in the framework: Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze, and Oversee and Develop.

- **Securely Provision**

This category encapsulates the specialty areas for overseeing, conceptualizing, designing, building and accrediting information systems using concrete security policies and processes [9]. The specialty areas included under this category are Risk Management, Software Development, Systems Architecture, Systems Development, Systems Requirements Planning, Technology R & D, Test and Evaluation.

- **Operate and Maintain**

This category includes specialty areas responsible for providing support, administration and maintenance that is necessary to ensure effective and efficient information technology (IT) system performance and security [9]. The specialty areas include Data Administration, Knowledge Management, Customer Service and Technical Support, Systems Analysis. The required KSATs are predominantly technical in this category and are well integrated into the work roles. There are no interdisciplinary work roles specified.

- **Protect and Defend, Investigate, Collect and Operate, Analyze, Oversee and Develop**

The rest of the NCWF categories are coupled together in this section due to observed commonalities in their analysis, discussed in the consecutive section. These categories collectively cover a wide range of specialty areas and work roles. Cyber Legal Advisor, Cyber Instructional Curriculum Developer/Instructor, Communication Security Manager, IT Program Manager, Threat Analyst and Exploitation Analyst are some of them.

3.2. ANALYSIS OF WORK ROLES IN NCWF CATEGORIES (OVERSEE AND GOVERN, PROTECT AND DEFEND, ANALYZE, COLLECT AND OPERATE, INVESTIGATE)

NCWF is established as a reference structure that provides a common, consistent lexicon to categorize and describe cybersecurity work [9]. The framework serves as the underlying protocol to identify, recruit, develop and maintain cybersecurity talent. It is used as a standard by educators to develop curriculum, certificate or degree programs, training programs, courses, seminars, exercises or competitions [5].

People, Process and Technology form the triad of an organization's cybersecurity. Even though many organizations focus on technology to solve their security problems by hiring more security practitioners, it doesn't necessarily solve the problem.

However, the Commission of Enhancing National Cybersecurity recommends acknowledging the need for socially-focused security measures to improve the overall effectiveness of the NCWF framework [21]. This leverages the need for cross-disciplinary education in cybersecurity. Though the framework integrates depth and breadth of scope for the technical roles, the interdisciplinary (non-technological) roles are outpaced in terms of competencies and KSATs. Some of the newer roles described in the framework are also brought into focus and discrepancies observed are documented below:

A. <u>There exists less competencies for interdisciplinary workforce/education.</u>

The NCWF framework is weighted higher for technical aptitude. This is explained by competencies. "Competency" is a term that is introduced into NCWF [9] and is defined as "skills or capabilities that are critical for successful job performance across various cyber roles and charts out the behaviors that elaborate the progressive levels of proficiency associated with those competencies" [9].

As shown in Figure 1, the Cybersecurity Competency Model complements NCWF by including competencies required by the average worker and cybersecurity professionals.

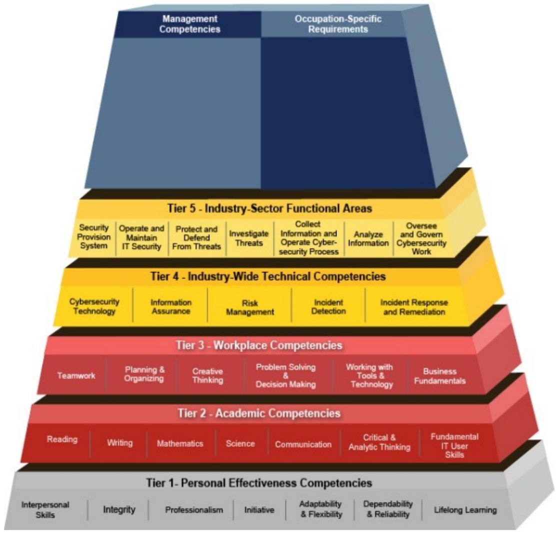
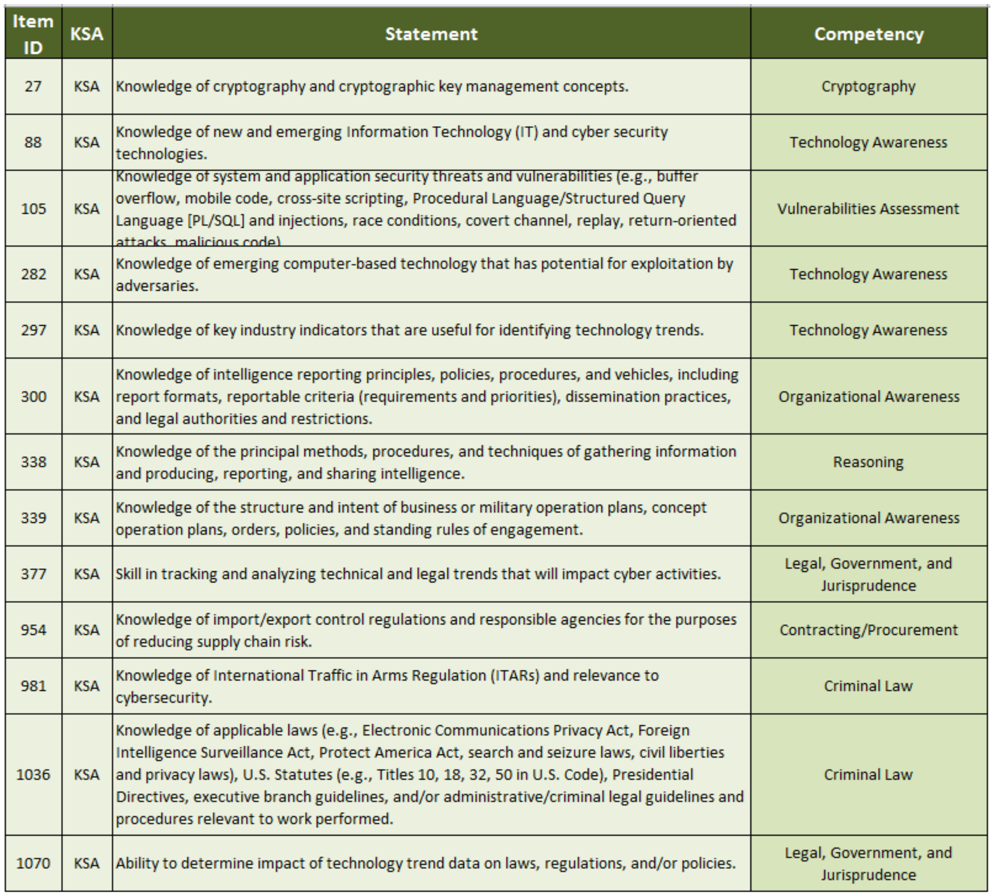

Management Competencies
Occupation-Specific Requirements
Tier 5 - Industry-Sector Functional Areas
Security Provision System
Operate and Maintain IT Security
Protect and Defend From Threats
Investigate Threats
Collect Information and Operate Cyber-security Process
Analyze Information
Oversee and Govern Cybersecurity Work
Tier 4 - Industry-Wide Technical Competencies
Cybersecurity Technology
Information Assurance
Risk Management
Incident Detection
Incident Response and Remediation
Tier 3 - Workplace Competencies
Teamwork
Planning & Organizing
Creative Thinking
Problem Solving & Decision Making
Working with Tools & Technology
Business Fundamentals
Tier 2 - Academic Competencies
Reading
Writing
Mathematics
Science
Communication
Critical & Analytic Thinking
Fundamental IT User Skills
Tier 1- Personal Effectiveness Competencies
Interpersonal Skills
Integrity
Professionalism
Initiative
Adaptability & Flexibility
Dependability & Reliability
Lifelong Learning

Figure 1 Cybersecurity Competency Model [23]

Table 1 shows the Competencies for the Specialty Area - Legal Advice and Advocacy. Legal advisors provide sound advice and recommendations to leadership and staff on a variety of topics, advocate legal and policy changes and make a case on behalf of the client through extensive written and oral work [11]. Majorie and Sheldon [12] state that the core competencies required for successful advocacy include analysis and reasoning, creativity, problem solving, practical judgement, research analysis, time and stress management, and excellent communication skills which includes writing, speaking and listening. Comparing the above critical factors with that of the NCWF competencies (given in Table 1 [24]), the latter appears to be less competent. While the industry wide technical competencies are plugged into the NICE framework extensively, the workplace and academic competencies are fewer. This creates a skills gap by generating a technically competent workforce and comparatively incompetent interdisciplinary workforce. With evolving legal environments, it is important to embrace a holistic culture, bringing in the best of personal, academic and work place competencies specific to the occupation and management

Table 1 NICE Competencies for Specialty Area - Legal Advice and Advocacy [24]



Item ID	KSA	Statement	Competency
27	KSA	Knowledge of cryptography and cryptographic key management concepts.	Cryptography
88	KSA	Knowledge of new and emerging Information Technology (IT) and cyber security technologies.	Technology Awareness
105	KSA	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)	Vulnerabilities Assessment
282	KSA	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries.	Technology Awareness
297	KSA	Knowledge of key industry indicators that are useful for identifying technology trends.	Technology Awareness
300	KSA	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportable criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.	Organizational Awareness
338	KSA	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence.	Reasoning
339	KSA	Knowledge of the structure and intent of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.	Organizational Awareness
377	KSA	Skill in tracking and analyzing technical and legal trends that will impact cyber activities.	Legal, Government, and Jurisprudence
954	KSA	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	Contracting/Procurement
981	KSA	Knowledge of International Traffic in Arms Regulation (ITARs) and relevance to cybersecurity.	Criminal Law
1036	KSA	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	Criminal Law
1070	KSA	Ability to determine impact of technology trend data on laws, regulations, and/or policies.	Legal, Government, and Jurisprudence

B. Job descriptions and KSATs are often too generic for "newer" work roles.

Some of the work roles specified in the framework are "new comers". They pertain to the following categories – Analyze, Collect and Operate, and Investigate. A list of those work roles is presented in Table 2. Those work roles were proposed to target candidates aspiring to work for the Department of Homeland Security, Central Intelligence Agency or the U.S. government, in general.

Consider the work role "Exploitation Analyst". In NCWF, an exploitation analyst "collaborates to identify access and collection gaps, and leverages all authorized resources and analytic techniques to penetrate targeted networks" [9]. As shown in Table 2, as of April 12, 2018, in the Indeed.com job search site, there existed 32 posted positions related to the work role exploitation analysts. Instead of using a generic job title like exploitation analyst, the employer may use further specific job titles such as mobile exploitation analysts, data exploitation analysts, or financial exploitation analysts.

While mobile exploitation analyst positions (Table 2) demand an extensive knowledge of networking and communication devices, data exploitation analysts are required to possess knowledge of data mining, trend analysis and financial structures. However, the framework states a generalized description for those "newer" work roles and the associated KSATs do not cover the requisite knowledge needed to acquire specific roles like mobile or data or financial exploitation analysts [9]. Relatively newer positions have less vision and scope due to poor job descriptions and lessened awareness of pre-requisite knowledge. Moreover, career paths related to the newer work roles are not covered in CyberSeek, a tool based on the NCWF framework to help employers, students, educators and policy makers to make decisions in pursuing careers or recruiting a cybersecurity workforce. As a result, a sector of candidates aspiring to get into those work roles suffer due to a fragmented focus on education and skills development.

Table 2 Statistics of Newer NICE Work Roles and Related Positions [25]

NICE Work Role Name	Recruiting Site Statistics	
	Number of Positions (as on 4/12/2018)	Diversity of Job Positions
Threat/Warning Analyst	424	Cyber Threat Analyst
Exploitation Analyst (EA)	32	Mobile Exploitation Analyst Financial Exploitation Analyst Digital Network Exploitation Analyst Audio/Video and Biometric Exploitation Analyst Cyber Operations Exploitation Analyst
All-Source Analyst (ASA)	252	Cyber Ops Military Planner
Mission Assessment Specialist (MAS)	0	
Target Developer (TD)	0	
Target Network Analyst	0	
Multi-Discipline Language Analyst	2	Multi-Discipline Language Analyst
All-Source Collection Manager		All-Source Requirements Collection Manager All-Source Intelligence Collection Manager
All-Source Collections Requirements Manager	4	
Cyber Intel Planner	1	
Cyber Ops Planner	1	Cyber Ops Military Planner
Partner Integration Planner	0	
Cyber Operator	9	
Cyber Crime Investigator	1	
Law Enforcement/Counterintelligence Forensics Analyst	5	Cyber Intelligence Analyst
Cyber Defense Forensics Analyst	1	

C. Does training and certification cover the interdisciplinary workforce? – Exploring the NICCS Initiative

The National Initiative for Cybersecurity Careers and Studies (NICCS) is a preeminent online resource for Cybersecurity training. The NICCS was formed with a vision to help citizens find the required education and training needed to enhance skills and bridge the gaps in the cybersecurity workforce. NICCS has an extensive repository of courses delivered by federal agencies, the various centers of academic excellence across the nation, colleges and universities, and private training providers. Each of the courses offered is mapped to the NICE framework categories.

Observing the learning objectives of one of the NICCS courses offered in Security Risk Management, we noticed that the learning objectives portray a mixture of organizational, technical and risk management knowledge. According to a Risk Management competency model of a top firm [13], some of the core competencies required for this position includes Business Insight, Communication, Collaboration and Consultation. However, the courses delivered in the NICCS catalog are tied to a category level and their learning objectives are not designed to impart the expected non-technical competencies along with the program. This is attributed to the high-level notional connections between the NICCS courses and the NICE categories. Previous research show that the mapping of the courses to the NICE categories is fluid since they were put through the best fit filter [16]. Therefore, a much-refined re-mapping of the NICCS courses to the NICE categories is required (by, for example, incorporating industry-wide competencies for work roles affiliated with that category). Secondly, the concentration of courses affiliated with the interdisciplinary specialty areas are fewer in number. For technical specialty areas such as Software Development, and Systems Administration, the number of courses and certifications are greater in comparison to non-technical areas such as Threat Analysis, Exploitation Analysis, All-Source Analysis, etc. On the whole, very few courses published in the NICCS are mapped to the following categories – Analyze, Collect and Operate, and Investigate.

D. Extensive technical knowledge is required in interdisciplinary roles.

Risk Management, an interdisciplinary area under this category, includes work roles such as Authorizing Official/Designating Representative, and Security Control Assessor [9]. The expected knowledge as defined by NCWF to acquire those roles include cryptography, emerging cybersecurity technologies, embedded systems, network security architecture, penetration testing, etc. These knowledge items are exclusive of the six foundational knowledge items – (a) knowledge of computer networking concepts, (b) risk management processes, (c) laws, regulations, policies and ethics, (d) knowledge of cybersecurity and privacy principles, (e) knowledge of cyber threats and vulnerabilities, and (f) knowledge of cybersecurity lapses – and are defined by the framework for all work roles [9].

Integrating extensive technical knowledge into interdisciplinary roles reduces the scope for students from non-technical majors to pursue a career in cybersecurity. This is because job descriptions based on the framework portray an expectation to possess higher technical knowledge rather than the desired discipline-specific knowledge. While the curriculum of the 70 Risk Management Programs offered across universities in the United States broadly cover business law, insurance, marketing, management and accounting, etc. [22], very few programs adhere to technical knowledge within the discipline. Top recruiting sites list very few job positions (Table 2) with respect to those work roles; most of those posted positions are predominantly offered only by service providers to the U.S. government.

To fill the growing demand for cybersecurity professionals [3], the framework must consider it inherent to attract available talent from non-technical majors and motivate the adopting organizations to foster desired technical skills through relevant on-the-job training and certifications.

E. <u>The NCWF provides no measurable outcomes.</u>

While one of the vision statements behind designing the framework was to train and educate students to get into the ever-growing cyber workforce [5], it is also important to measure the outcome or effectiveness of adopting the framework for curricular development. The framework does not formulate any measurable outcomes or predictable results for academic institutions or the workforce. This could be overcome by designing a Cybersecurity Maturity Assessment to measure and identify the effectiveness of the framework for technical and non-technical majors.

F. <u>Does NCWF create a siloed workforce?</u>

Historically, cybersecurity originated as a technical subfield of Computer Science. However, evolving pervasive computing technology has leveraged security, integrating management and policies under its umbrella. In 2015, the European CAMINO Project created the THOR acronym approach of “(T)echnical”, “(H)uman”, “(O)rganizational” and “(R)egulatory”. The project ascertains that cyber security could be comprehensively perceived as a combination of the above four dimensions [17]. In lieu of this, some of the areas that require a higher leverage in the framework are Usable Security, Cybersecurity Research, Criminology, Information Science and Behavioral Science.

Cybersecurity as a multidisciplinary field is often misunderstood as requiring input only from Computer Science and not from other fields such as Economics, Mathematics, Accounting, Political Science, Social Science, etc. As a result, the workforce that results from such an education becomes siloed and stove-piped, keeping them within a shell of a specific career path (or a discipline). On a much higher level, previous research [18] indicates that “Cybersecurity workforce members tend to be less bound to organizationally constructed career paths. Rather, they have a tendency towards a boundaryless career precisely motivated by personal achievement and external career dimensions, such as organizational position, mobility, flexibility and organizational goals” [18]. The NICE framework should consider such non-traditional conceptualizations of career management too.

4. CONCLUSION

Attacks exploiting human behavior are inseparable from cybersecurity. Training to prevent, respond and defend systems from those attacks depend as much on the technical aspects as on the human factors. Emphasizing technical aspects within cyber education prepares a workforce to respond to only a certain part of the problem.

Cybersecurity education necessitates a reconciliation between the technical and the non-technological, interdisciplinary avenues, benefitting workforce in both estates. The NICE framework provides consistent language, role definitions and a working taxonomy. In lieu of certain work roles which fall under the non-technological side of cybersecurity, we have noticed some discrepancies in the framework; those include poor job descriptions for specific work roles, inadequate competencies and training and career guidance, no predictable outcomes or metrics to determine effectiveness, etc. Articulating a concise, meaningful and inclusive approach to cybersecurity workforce development will enhance a balanced workforce, by incorporating both technical and discipline-specific work roles, to tackle challenges with more preparedness and sophistication.

REFERENCES

[1] S. Morgan, "Top 5 cybersecurity facts, figures and statistics for 2018", *CSO Online*, 2018. [Online] Available:https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html. [Accessed: 10- Apr- 2018].

[2] A. Setalvad, "Demand to fill cybersecurity jobs booming - Peninsula Press", Peninsula Press, 2018. [Online]. Available:http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/. [Accessed: 10- Apr- 2018].

[3] “Home: Occupational Outlook Handbook: U.S. Bureau of Labor Statistics", Bls.gov, 2018. [Online]. Available: http://www.bls.gov/ooh/. [Accessed: 10- Apr- 2018].

[4] J. Peeler, Management, "(ISC)² Study: Workforce Shortfall Due to Hiring Difficulties Despite Rising Salaries, Increased Budgets and High Job Satisfaction Rate", (ISC)² Blog, 2018. [Online]. Available: http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html. [Accessed: 10-Apr- 2018].

[5] M. Zadelhoff, "Cybersecurity Has a Serious Talent Shortage. Here’s How to Fix It", Harvard Business Review, 2018. [Online]. Available: https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it. [Accessed: 10- Apr-2018].

[6] M. Stockman, "Infusing social science into cybersecurity education," Proceedings of the 14th annual ACM SIGITE conference on Information technology education, Orlando, FL, October 2013, pp. 121- 124.

[7] L. Dishman,"These Are The Biggest Skills That New Graduates Lack", Fast Company, 2018. [Online]. Available: https://www.fastcompany.com/3059940/these-are-the-biggest-skills-that-new-graduates-lack. [Accessed: 10-Apr- 2018].

[8] S. Ghernouti-Hélie, "A National Strategy for an Effective Cybersecurity Approach and Culture", 2010 International Conference on Availability, Reliability and Security, 2010.

[9] NIST, NICE Cybersecurity Workforce Framework Tutorial. National Initiative for Cybersecurity Education, 2018.

[10] “Education - Risk Manager Core Competency Model", RIMS - The Risk Management Society, 2018. [Online]. Available: https://www.rims.org/education/Pages/RiskManagerCoreCompetencyModel.aspx. [Accessed: 10- Apr- 2018].

[11] "NICE Cybersecurity Workforce Framework", NIST, 2018. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework. [Accessed: 10- Apr- 2018].

[12] M. Maguire Shultz and S. Zedeck, "Final Report - Identification, Development and Validation of Predictors for Successful Lawyering", SSRN Electronic Journal, 2009.

[13] “Education - Risk Manager Core Competency Model", RIMS - The Risk Management Society, 2018. [Online]. Available: https://www.rims.org/education/Pages/RiskManagerCoreCompetencyModel.aspx. [Accessed: 10- Apr- 2018].

[14] "Career Fields | Intelligence Careers", Intelligencecareers.gov, 2018. [Online]. Available: https://www.intelligencecareers.gov/iccareers.html. [Accessed: 10- Apr- 2018].

[15] Sans.org, 2018. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615. [Accessed: 10- Apr- 2018].

[16] B. Caulkins, K. Badillo-Urquiola, P. Bockelman and R. Leis, "Cyber workforce development using a behavioral cybersecurity paradigm", 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016.

[17] R. Ramirez and N. Choucri, "Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review", IEEE Access, vol. 4, pp. 2216-2243, 2016.

[18] L. Hoffman, D. Burley and C. Toregas, "Holistically Building the Cybersecurity Workforce", IEEE Security & Privacy Magazine, vol. 10, no. 2, pp. 33-39, 2012.

[19] B. Technologies and B. Technologies, "Production Skills Gap | Burning Glass Technologies", Burning Glass Technologies, 2018. [Online]. Available: https://www.burning-glass.com/research-project/production-skills-gap/. [Accessed: 10- Apr-2018].

[20] A. McGettrick, "Toward Effective Cybersecurity Education", IEEE Security & Privacy, vol. 11, no. 6, pp. 66-68, 2013.

[21] T. Kerfoot, "Cybersecurity: Towards a Strategy for Securing Critical Infrastructure from Cyberattacks", SSRN Electronic Journal, 2012.

[22] 15 Best Bachelor of Risk Management Degree Programs 2017-2018 - Online Accounting Degree Programs", Online Accounting Degree Programs, 2017. [Online]. Available: http://www.online-accounting-degrees.net/best/bachelor-of-insurance-risk-management-degree-programs/. [Accessed: 20- Apr-2018].

[23] U.S. Department of Labor, Cybersecurity Competency Model. [Online]. Available at https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

[24] "NICE Cybersecurity Workforce Framework", NIST, 2018. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework. [Accessed: 21- Apr- 2018].

[25] "Job Search | Indeed", Indeed.com, 2018. [Online]. Available: https://www.indeed.com/. [Accessed: 12-Apr- 2018].