NATIONAL CYBERWATCH CENTER

NOVEMBER 2020 | SPECIAL ISSUE
DIGITAL ONLINE FIRST EDITION

NICE FRAMEWORK SPECIAL ISSUE:
INVESTIGATING FRAMEWORK ADOPTION, ADAPTATION, OR EXTENSION

CYBERSECURITY SKILLS JOURNAL:
PRACTICE AND RESEARCH

301 Largo Rd. CAT 129C, Largo, MD 20774.

www.nationalcyberwatch.org

Cybersecurity Skills Journal: Practice and Research
NICE Framework Special Issue:
Investigating Framework Adoption, Adaptation, or Extension

National CyberWatch Center Digital Press ID NCC-2020-CSJ-02

csj.nationalcyberwatch.org

Table of Contents

Executive Letter

Dear Reader,

The Cybersecurity Skills Journal (CSJ) editorial board is pleased to present practice, research, and teaching perspectives on the adoption, adaptation, or extension of the NICE Framework. As the African proverb states, "It takes a village to raise a child." Similarly, CSJ, with its developmental peer review process, stands on the shoulders of giants in the cybersecurity community. This Special Issue is possible only because of the countless hours contributed by volunteers who shared their time and talent to nurture ideas and experiences into rigorous, systematic inquiries that can inform the development of evidence-based practices.

The contributors to this issue number more than space allows us to recognize. However, we would like to highlight a few especially noteworthy individuals. Without the inordinate contributions by these consummate professionals, CSJ would not have brought to the cybersecurity community the insights and inspirations represented in the articles and notes in this issue.

First, we would like to thank the 40 authors who submitted abstracts and the 162 cybersecurity practitioners and scholars who volunteered to serve on peer review panels. While only a select group of manuscripts were ultimately selected for publication in this Special Issue, all of the structured abstracts demonstrated the importance of achieving the new goal in the NICE Strategic Plan: "Drive Research on Effective Practices for Cybersecurity Workforce Development."

Second, we would like to thank Casey W. O'Brien and the entire leadership team at the National CyberWatch Center (NCC) and Celeste Carter, Corby Hovis, and Victor Piotrowski and other program leadership at the National Science Foundation (NSF) who support NCC. The support of NCC and NSF made it possible to experiment with developing an outlet for ideas, experiences, and investigations seeking to enhance the capability maturity of the cybersecurity workforce. These organizations provided the infrastructure support needed to manage the abstract and manuscript submission, 10-person peer review teams, paper development workshops, peer reviewer workshops, and the contracting of professional marketing, publication design, and typesetting services.

Third, we would like to thank Rodney Peterson and the entire leadership team involved in the National Initiative for Cybersecurity Education (NICE). Besides being extremely NICE people (sorry, couldn't resist), without their ongoing focus on the *human firewall*, a journal dedicated to advancing skills in designing, deterring, defending systems that protect our nation's critical infrastructure would not be possible. Mr. Peterson's keynote address brought much-needed attention to the Special Issue Call for Abstracts at the 2019 NICE Annual Conference. The NICE Strategic Plan articulates these values[1] that align perfectly with the CSJ mission:

- Foster communication and encourage openness to build trust
- Facilitate collaboration, combining the knowledge and skills of stakeholders with multiple viewpoints and approaches to achieve the best outcomes
- Share and leverage resources to support community-developed approaches and solutions
- Act based on evidence, pursuing objective and reliable sources of information and using data to inform actions or decision
- Evaluate and improve our effectiveness by using quantitative metrics and qualitative measures
- Challenge assumptions, examining rationale for past and present education, training, and workforce approaches and applying critical analysis to future solutions
- Stimulate innovation, inspiring and experimenting with new approaches in a search for creative and innovative solutions that might disrupt or defy the status quo

The first five values align with CSJ's mission to encourage and mentor practitioners, educators, and researchers to disseminate their experiences and findings beyond the small circulation venues of meetings or conferences. At every one of these convening events, the insights shared are immeasurably valuable to the advancement of cybersecurity practice. However, to fully benefit from these insights, a practitioner or scholar would need to attend every paper, presentation, or panel session - an impossibility even before COVID limited our travel and interpersonal exchanges. Thus, a primary mission of CSJ is to assist practitioners, scholars, and all cybersecurity stakeholders by disseminating rigorous investigations grounded in conceptual frameworks or empirical analysis that address current conversations in cybersecurity practice, research, or instructional design. Articles include a depth of analysis that fosters replication and extension thereby progressing the science of cybersecurity skill assessment, development, or adoption.

With this Special Issue, we are excited to introduce a new form of systematic inquiry that seeks to fulfill the NICE values of challenging assumptions and simulating innovations. *CSJ Notes* seek to inspire, enlighten, or promote critical inquiry into novel, unexplored or nebulous topics in cybersecurity practice, research, and instruction. We refer to these exploratory articles as *Notes* to emphasize emerging lessons learned or thought-provoking conjectures. Practice, Research, or Teaching Notes explore uncharted territory, rather than seeking to confirm or disconfirm the results of prior literature as is done in an article. A note may propose or review a new or emerging domain, principle, technique, or tool that can raise capability maturity, describe proposed or in-progress research, or report the results of an exploratory investigation that yields important insights and implications for practice, research, or instruction. A note may also conceptually develop a rationale for future practice development or research. In other words, a note may be the beginning of developing testable propositions/predictions of impact that later evolve into a theoretical or conceptual framework or an empirical investigation that could be published as a CSJ article.

We trust you will find the insightful articles and notes selected for this Special Issue form the beginning of an evidence-based turn in cybersecurity practice and research. Professions such as aviation[2], medicine[3], psychology[4], and social policy[5] have developed repositories of studies that identify effective practices. Effective practice begins and ends with skilled performance. The articles and notes in this Special Issue portend that the NICE Framework established the foundation for the adoption, adaptation, or extension of the tactics, techniques, and procedures that evidence shows to be effective in establishing and maintaining a secure systems environment.

Very Respectfully,

Editorial Board
Cybersecurity Skills Journal

[1] https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
[2] http://www.ebt-foundation.com/about-ebt
[3] https://www.cochranelibrary.com/
[4] https://www.samhsa.gov/ebp-resource-center
[5] https://www.pewtrusts.org/en/research-and-analysis/data-visualizations/2015/results-first-clearinghouse-database

Practice Perspectives

The CYBER security - Competency Health and Maturity Progression (CYBER-CHAMP©) model:

Extending the National Initiative for Cybersecurity Education (NICE) Framework Across Organizational Security

Jade A. Hott
Idaho National Laboratory, United States

Dr. Shane D. Stailey†
Idaho National Laboratory, United States

Donaven M. Haderlie
Idaho National Laboratory, United States

Ralph F. Ley
Idaho National Laboratory, United States

***Abstract*— Problem Statement:** There is a pervasive talent deficit in the cybersecurity industry that prevents employers from being able to fill their open positions efficiently. A holistic approach to security is required to ensure organizations have adequate prevention and response capabilities in case of a cyberattack. Specifically, industrial control systems (ICS's) and their operational technology (OT) components have become a constant target for cyberattacks.

Research Questions: It is proposed that the NICE Framework should be extended in the following areas:

1. Include guidance regarding the job roles and competencies for both IT and OT professionals.
2. Offer step-by-step solutions, based on the work role mappings from the NICE Framework, to increase cybersecurity through employee training and education.
3. Provide a streamlined, lifecycle approach to building a cybersecurity program.

Contribution: The CYBER security – Competency Health and Maturity Progression (CYBER-CHAMP©) model provides a customized solution for businesses to understand their education gaps in organizational security and target areas for improvement.

Rationale: The Framework for Improving Critical Infrastructure Cybersecurity v1.1 addresses ICS but does not offer a measurement of cybersecurity maturity or clear methods to ascertain an organization's current risk profile. In Phases 1 and 5 of the model, measurements are provided to help an organization build their current and target risk profiles. The NICE Framework provides a structure for planning an IT cybersecurity workforce, but the OT aspects of cybersecurity are only briefly discussed. The model uses Phases 2-3 to examine the competencies of an organization's workforce, which includes both IT and OT roles. Current frameworks do not offer next steps to increase an organization's cybersecurity. During Phase 4, employees' roles are mapped to training, education, and/or certifications from common vendors.

Investigative Approach: The model provides measurements and metrics for both an organization's status and continual improvement. This improvement methodology includes guidance for creating an overall strategic plan for security improvement via products designed to increase an organization's operational readiness through workforce competency health.

Lessons Learned: Depending on who was participating, there were contradicting answers given in Phase 1 due to different security cultures in the organization. This revelation has influenced the steps listed in the User's Guide, where Phase 1's first recommended step is to assemble a team that champions the facilitation and implementation of the model in the organization. During Phase 2, the discovery was made that organizations may be missing roles that are necessary to perform critical cybersecurity functions. By understanding the functional roles and competencies needed, they can contract or hire cybersecurity help to fill these gaps.

Implications: Using the model, organizations can discuss quantitative measures for improvement as a business case for advancing their security program. Future research can validate and extend the present theory and model to a variety of environments. It is of interest to investigate additional security roles and knowledge domains that are used to build standardized cybersecurity curriculum.

Keywords—Industrial control systems, cybersecurity, operational technology, information technology, workforce, maturity model, competencies

† refers to the corresponding author for communications regarding this manuscript.

I. Introduction

By 2021, it is predicted that there will be over three million unfilled cybersecurity jobs worldwide (Morgan, 2019). However, there is a pervasive talent deficit in the industry that prevents employers from being able to fill these positions efficiently (Frost and Sullivan, 2017; Morgan, 2019). Many tools are available in the informational technology (IT) security community to bridge the knowledge gap for the workforce, but few address the holistic nature of security which includes operational technology (OT). OT is the hardware and software components of control systems used within critical infrastructures such as energy and transportation (Murray et al., 2017). In recent years, IT and OT have converged and introduced vulnerabilities into the industrial environment that were previously non-existent (Murray et al., 2017). Therefore, industrial control systems (ICS's) and their OT components have become a target for relentless attacks by adversaries (Ponemon Institute LLC., 2019). ICS is an information system that controls the processes involved with industrial activities such as manufacturing and distribution (NIST, 2011). ICS and OT are the perfect target for cybersecurity attacks due to their capability to cause loss of life and injuries, financial losses, threats to national security, and impacts on public health. In a recent study of employees from various OT sectors, 90% reported a damaging cyberattack in the last two years (Ponemon Institute LLC., 2019). A holistic approach to organizational security that includes both IT and OT is required to ensure adequate prevention and response capabilities in case of a cyberattack.

Although ICS personnel are immersed in operational standards and industry best practices, research has shown that there is a knowledge gap in understanding the cybersecurity implications for an organization (Menze, 2019). One of the major concerns reported by industrial companies is that their asset owners and operators lack general cybersecurity awareness (Menze, 2019), which may be due to a lack of education and training. A working group for the National Initiative for Cybersecurity Education (NICE) created an organizational guidebook in which the main argument is that "cybersecurity is everyone's job" (NICEWG, 2018). The guidebook offers suggestions for the contributions to security that all employees can make based on their job roles. Herein, a new process is proposed to ensure everyone in an organization, despite their role, can contribute to solving cybersecurity issues.

In a recent interview with Michael Bayer, an advisor at the Pentagon, Bayer cautioned that, "The battle for cyberspace will hinge on human beings… A lack of cyber hygiene by just one employee or subcontractor of the government can be the entryway for a cyber break-in with strategic consequences" (Donnelly, 2019). Bayer's concerns are not unfounded as humans – or employees – are widely acknowledged to be the weakest line of defense against cyberattacks (Schneier, 2000; Sasse et al., 2001). This claim was further validated with an analysis of data from UK's Information Commissioner's Office (ICO), wherein it was revealed that 90% of all the data breaches examined were the result of human factors in the form of user error (Ho, 2020). Verizon's 2020 Data breach investigations report also found human error was a causal event in 22% of organizational incidents, which may represent a more conservative view of the issue and still points to the significant impact of human factors on cybersecurity.

Potential attackers have employed a variety of people-targeted methods, called social engineering, to take advantage of these vulnerabilities (Fruhlinger, 2019). The most frequently used type of social engineering is phishing attacks (InfoSec Institute, 2020). Phishing is the use of counterfeit emails or messages to convince the recipient to perform an action (e.g., clicking on a link) which will allow unauthorized access to an organization's systems or the collection of sensitive information like passwords (ODNI, 2019). In the realm of ICS, a mistake by an employee can be especially disastrous, enabling attackers to cause disruptions to critical services (e.g., power, heat), produce environmental impacts (e.g., explosions, release of chemicals or toxins), and even cause loss of human life (Murray et al., 2017). During an attack on a German steel mill, a combination of social engineering tactics and spear-phishing emails were used to gain critical login information from company employees (BBC News, 2014). Once this information was obtained, the attackers accessed the plant's production systems to cause mechanical failures and massive damage to the mill. To ensure the security of the Nation's control systems, it is vital for organizations to educate and train all employees on cybersecurity.

II. Background

In 2018, the Framework for Improving Critical Infrastructure Cybersecurity v1.1 was released by the National Institute of Standards and Technology (NIST). The focus of the NIST Framework is the security of critical infrastructure through risk management, rather than the education of the workforce. The NIST Framework has three components – a framework core, implementation tiers ("Tiers"), and a framework profile – that provide recommendations for addressing an organization's cybersecurity risk (NIST, 2018). The Tiers are intended to describe the extent to which cybersecurity risk management processes are integrated with overall risk management strategies. All Tiers are ranked with Tier 1 (Partial) representing the least sophisticated processes and Tier 4 (Adaptive) being the most sophisticated. However, it is made clear in the document that these Tiers are not intended to represent maturity levels of risk management (p.8). Other than the definitions provided, there is also no assessment method to ascertain an organization's Tier placement. The information gained from the framework core and implementation tiers can then be used to create current and target organizational risk profiles, but there aren't detailed instructions for forming the profiles. This lack of step-by-step guidance may be due to a limited framework scope that does not include assessing underlying factors that contribute to risk such as organizational objectives and business needs, the relationship between those objectives and establishing cybersecurity goals, and how those target cybersecurity outcomes are implemented and maintained (p.20).

The NICE Cybersecurity Workforce Framework – often referred to as the NICE Framework – addresses the education and training needs of the cybersecurity workforce by providing a common vocabulary for the field and a detailed list of cybersecurity Knowledge, Skills, Abilities, and Tasks (KSAT's) for each of the identified work roles (Newhouse et al., 2017, pp.2-3). The NICE Framework includes 7 categories, 34 specialty areas, and 52 work roles. The categories are Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate. With this information, the listed work roles can be directly mapped to cybersecurity KSAT's. For example, Data Analyst is a work role established within the category Operate and Maintain (OM) and the specialty area of Data Administration (DTA). A Data Analyst has 32 K's, 26 S's, 5 A's, and 23 T's, for a total of 86 KSAT's (p.101, see Table 1). The mapping is complete once descriptions for the KSAT's are selected among the tables included in the publication (pp.24-94). However, an individual's unique role or job description must be compared with the pre-determined list of work roles to determine their applicable KSAT's. Once the KSAT's are mapped, the NICE Framework also does not offer suggestions on the types of education or training needed to obtain the KSAT's. The ability to provide next steps for applying the NICE Framework in an organization may make it easier to justify the time spent conducting the mappings. It is recommended that the NICE Framework mapping process be streamlined to naturally produce the next steps for an organization. A process to streamline the mapping process for an organization's work roles, such as the Data Analyst, is proposed.

While the NICE Framework is intended to be applicable to a wide range of cybersecurity workers in an organization, IT roles and IT KSAT's are ultimately the focus of the competency recommendations provided. An initial word search of the NICE Framework for "information technology" produces over four times the results (62) than the combined hits for "critical infrastructure" (12) and "control system" (1). Specifically, the term "operational technology" is never referenced in the document. As IT and OT systems become increasingly interconnected and the vulnerabilities associated with the convergence multiply (Murray et al., 2017), educational frameworks for cybersecurity should be extended to ICS environments and operational concerns. In a survey of ICS professionals, respondents were asked to identify the biggest challenges faced in the IT/OT integration process (Filkins and Wylie, 2019). 61% reported their organization's biggest challenge was IT staff's lack of understanding regarding ICS requirements. IT staff often say the same thing about ICS staff's lack of knowledge in security (p.29). A holistic approach to security education and training, bridging the gap between IT and OT, is required to ensure organizations are adequately prepared in case of a cyberattack. The next steps provided by the NICE Framework mappings could also be clearer, enabling employees to present a strong business case for cybersecurity efforts in their organization.

Table 1: NICE Framework Data Analyst Role Mapped to KSAT's

Work Role Name	Data Analyst
Work Role ID	OM-DTA-002
Specialty Area	Data Administration (DTA)
Category	Operate and Maintain (OM)
Work Role Description	Examine data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
Tasks	T0007, T0008, T0068, T0146, T0195, T0210, T0342, T0347, T0349, T0351, T0353, T0361, T0366, T0381, T0382, T0383, T0385, T0392, T0402, T0403, T0404, T0405, T0460
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0016, K0020, K0022, K0023, K0025, K0031, K0051, K0052, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0420
Skills	S0013, S0017, S0202, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160, S0369
Abilities	A0029, A0035, A0036, A0041, A0066

III. Research Questions

Therefore, it is proposed that the NICE Framework should be extended in the following areas to increase the Framework's generalizability and benefits to organizations:

1. Provide a streamlined, lifecycle approach to building a cybersecurity program from the formation of current and target risk profiles to implementing training paths for employees.
2. Extend the focus to organizational security, which includes guidance regarding the job roles and competencies for both IT and OT professionals. The following OT work roles will be included: technician, engineer, analyst, researcher, and manager.
3. Offer step-by-step solutions, based on the work role mappings from the NICE Framework, to increase cybersecurity through employee training and education.

IV. Method

Substantial strides in closing the workforce development and training divide between IT and OT can be made by forming a model that binds together the elements of security operational readiness, workforce structure, and individual cyber competencies, and curriculum. The CYBER security – Competency Health and Maturity Progression (CYBER-CHAMP©) model provides a customized, self-help solution for government entities and private sector businesses to understand their education gaps in security and target areas for improvement. Hereafter, CYBER-CHAMP© will be referred to as "the model." The model consists of five Phases that provide measurements and metrics for both an organization's status and continual improvement. This improvement methodology includes guidance for creating an overall strategic plan for cybersecurity improvement via products designed to increase an organization's operational readiness through workforce competency health. Operational readiness, when utilized by the model, is defined as the evidence, policy, process, and practices from which an entire organization can demonstrate preparedness towards detecting, handling, responding to, and mitigating operationally impacting cybersecurity events. Workforce competency health refers to the degree to which an organization's employees can perform cybersecurity tasks across the functions of awareness, support, maintenance, implementation, and design. The five Phases of the model are:

- *Phase 1* – Measure Organizational Security State: initial assessment of an organization's progress towards security operational readiness through maturity levels, which is used to form a current risk profile; then, identify areas for improvement to create a target risk profile. An example is shown on the left-hand side of the model in Figure 1.
- *Phase 2* – Create Workforce Profile: involves mapping an organization's unique workforce role structure to the competency health functions.
- *Phase 3* – Determine Competency Health: survey the tasks required to acquire the competencies needed across each functional level by role. Once the tasks have been mapped, the organization will determine the job roles to target for customized learning paths. Learning paths consist of a broad view of the training and educational possibilities for a role.
- *Phase 4* – Prepare and Apply Learning Paths: The individuals in these roles receive their learning path(s). Then, the learning paths are tailored down to a one-two year training plan.
- *Phase 5* – Measure Organizational Security State: After the learning paths have been completed to the organization's satisfaction, reassess security status to compare with the

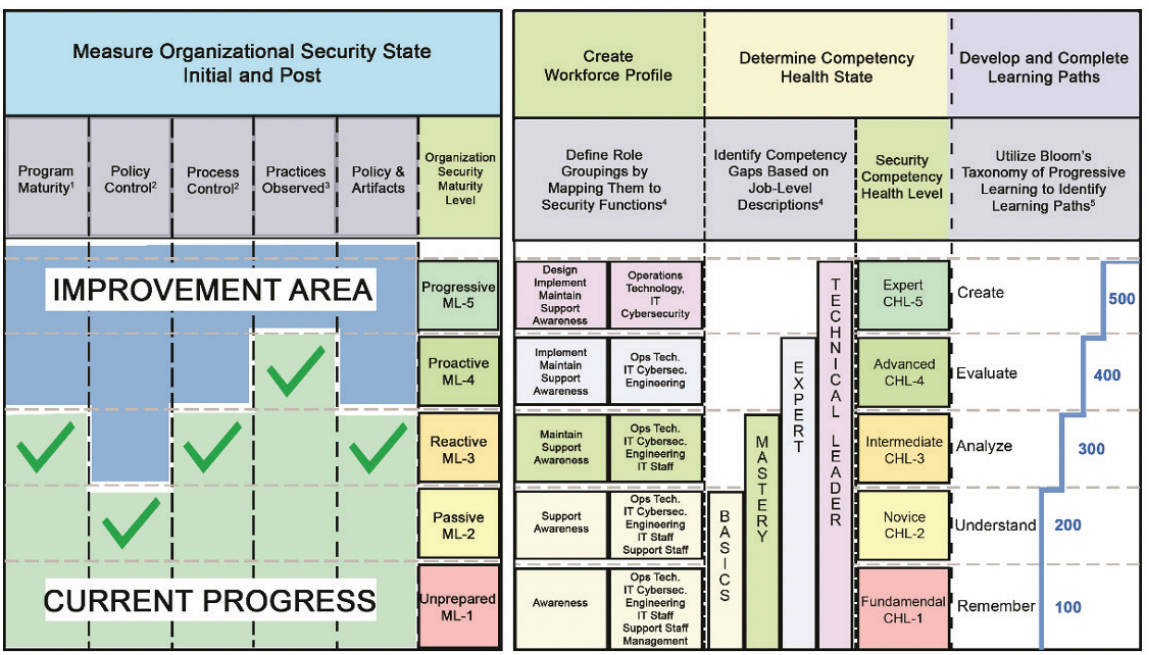
improvements outlined in the target profile that was developed in Phase 1.

A detailed description for each phase of the model is provided below. Phases 2-4 will be the focus of the direct comparison between the processes listed in the NICE Framework and the methods of extension that the model uses for an organization's workforce. Figure 1 displays the model and its various components in further detail.

Phase 1 - The first step for any organization looking to improve their cybersecurity program is to determine their current level of organizational security. Once their security status is known from the results of Phase 1, a target profile for the program can be created. Phase 1 is repeated during Phase 5 to determine the progress that has been made towards the target profile and/or increases in security maturity. In Phase 1 and 5, the following measurements are conducted: security program level, policy maturity level, practice maturity level, and the rigor for both policies and practices. The maturity measurements are based on the policy and practice maturity levels in the NIST Cybersecurity Framework Maturity Tool (Masserini, 2018), NICE's seven steps for "Establishing or Improving a Cybersecurity Program" (Newhouse et al., 2017), and the processes and practices provided in the Cybersecurity Maturity Model Certification (Carnegie Mellon and John Hopkins, 2020). Before implementing Phase 1, the appropriate personnel should be gathered who understand the organization's current security policies, practices, and processes. These individuals will ensure that accurate responses are given for the questions in the template. The quality of the responses directly determines which maturity levels are produced by Phase 1's completion. The results for program level, policy, and practices will be used to create a current profile and target profile for organizational security. The current profile represents the organization's security state at the beginning of the process, while the target profile serves as a goal for organizational improvements in security by the end of the process. These profiles can also be used to build a business case, showing the need for increased security resources and/or personnel. Both profiles will be used to tailor the next steps for improving security maturity, build role-based learning paths, and establish a continuous life-cycle approach to improving cybersecurity programs.

Phase 2 - Phase 2 begins the process to ensure that the cybersecurity workforce is conscious of security threats and vulnerabilities and are properly trained to address them. A workforce profile is built using SANS' Global Industrial Cyber Security Professional Job Role to Competency Level Recommendation as a template (SANS, 2019).

Figure 1: A High-level Overview of the Model's Components



Although these recommendations were originally built for an industrial cybersecurity certification, the job roles provided span a variety of positions across an organization such as management and support staff (see Figure 2). An organization's workforce profile is tailored by expanding the SANS job role template to include the job role groupings specific to their operations. These job role groupings are then mapped to the cyber functions by maturity level: awareness (level 1), support (2), maintain (3), implement (4), and design (5). The goal is to ensure that all main roles in the organization are included in at least one of the job role groupings (see Figure 3). It is critical that everyone in the organization, despite their role, assumes responsibility for solving cybersecurity issues (NICEWG, 2018). All roles may be mapped to their own training paths in Phase 3, but it is recommended for organizations to identify a few high-priority roles to receive the first learning paths. This will provide a start towards the goal that all employees are properly trained.

Figure 2: SANS ICS GCISP Job Role Groupings and Job Roles

Engineering	Operations Technology	Management	Support Staff	Cybersecurity	IT Staff
Process Engineer	Operator	Plant Manager	Remote Support	ICS Security Analyst	Networking
Electrical Controls Engineer	Site Security POC	Risk/Salary Manager	Technical Support	Security Engineering	Infrastructure
Mechanical Engineer	Technical Specialists	BU Management	Contractors	Security Architect	Host Administrator
Project Engineer	OT Security	C-Level Management	IT	Security Operations	Database Administrator
Systems/Reliability Engineer	ICS/SCADA		Physical Security	Security Response	Application Development
OT Developer	Security		Engineering	Security Forensics	ERP/MES Administrators
PLC Programmer			Procurement	Security Management (CISO)	IT Management
Emergency Operations Manager	Programmer		Legal	Audit Specialist	IT Architect
Plant Networking			Contracting Engineering	Security Tester	
Control/Instrumentations Specialist			Insurance		
Protection and Controls			Supply Chain		
Field Engineer			Lifecycle Management		
Systems Integrator			Physical Security Specialist		

Figure 3: SANS ICS GCISP Job Role Groupings and Job Roles

Engineering & Communications	Operations Technology	Management	Support Staff	Cybersecurity	IT Staff
Controls Engineer	OT Networking	Human Resources	Regulatory Compliance	ICS Security Analyst	Networking/ Telecom
Apparatus Engineer	OT Infrastructure	Plant Manager	GIS Support	IT Security Architect	Physical Infrastructure
Project Engineer	OT Architect	BU Management	Contract Crews	Security Operations	Systems Administrator
Reliability and Power Quality Engineer	OT Operator	C-Level Management	Construction Crews	Security Response	Database Administrator
PLC Programmer	OT Technicians		Training	Security Forensics	Application Development
Protection Engineer	OT Security		Contractors	Security Management (CISO)	Application Administrators
Communication Systems Engineer	ICS/SCADA		IT (Service Desk or Call Center)	Audit Specialist	IT Management
Control Technician	OT Programmer/ Developer		Physical Security	Security Tester	IT Architect
Apparatus Technician	Frontline Leader		Engineering		Disaster Recovery

Phase 3 - In this phase, competency health for the employees in the identified roles is determined by completing a survey. The survey consists of the categories, specialty areas, work roles, and associated tasks of the NICE Framework. Respondents are asked to identify, through a series of yes/no questions, which category descriptions and specialty area descriptions best match their unique organizational role(s). The mechanics of the survey are similar to the online mapping tool offered by the National Initiative for Cybersecurity Careers And Studies (NICCS) but there are few critical differences: the model's survey has OT work roles and tasks, includes specialty areas from the NICE Framework, and does not ask respondents to self-identify their KSA's (NICCS, 2020). The model also includes the following OT work roles: technician, engineer, analyst, researcher, and manager. These new roles were discovered through extensive research conducted by Sean McBride, a professor at Idaho State University, and will be published in an upcoming article.

Phase 4 - Once the work roles are produced by the survey, the mapped tasks from the NICE Framework are identified. If more than one role is identified from the NICE Framework, the role that has the highest number of tasks to perform becomes the primary focus for the education and training plans developed in Phase 4. It is assumed that the primary job role has priority over any secondary roles for training investments. Education and training are assigned based on the security tasks, out of the provided list, that the individual is not yet able to perform. One of the ways that education and training recommendations are determined is using NIST's mapping of certifications to NICE Framework (2018). A mix of other training repositories can be utilized from common vendors, academia, and/or training providers. The mapping process produces a set of courses that becomes the individual's training, education, and/or certification plan. Phase 4 is completed when the training plans are implemented for the identified employees in the organization. It is important to make sure ample time is provided for on-the-job, training, education, and certification(s) to make an impact in organizational security before proceeding to Phase 5.

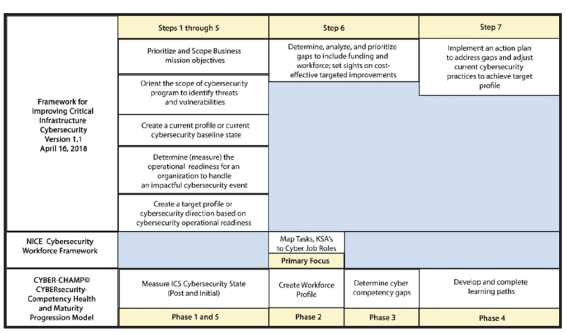
Phase 5 - To show progress made from the current profile towards the target profile, the organization should re-conduct the measurements from Phase 1. Phase 1 was a pre-test before the model was implemented and Phase 5 serves as the post-test to evaluate improvements. The difference between maturity level scores obtained in Phase 1 and Phase 5 offer quantitative evidence of any

progress obtained. However, the completion of the Phase 5 measurements does not represent the end of the model because it is intended to be a lifecycle approach. The information gained from Phase 5 should be used to create new improvement goals and restart the phased process on a recurring basis (e.g., biannually, annually).

V. Results

The model leverages existing frameworks and resources in a novel way to produce a streamlined approach for industrial companies to measure their organizational baselines and next steps for security improvements at the organizational level as well as the workforce level. The model was developed to extend these resources to increase their generalizability and it is not intended to be a replacement framework. Figure 4 demonstrates the areas where the model has incorporated and extended the concepts from these frameworks. Initial work with in-State energy providers and academic institutions has resulted in a sustainable solution for businesses wanting to attain and maintain an organization-wide cybersecurity workforce. This work has also initiated vital conversations between local education providers on how to integrate newly identified, industry validated cybersecurity training topics into their degree programs and offerings. At the time of this publication, a pilot study with a medium-sized power company in Idaho will be nearing completion. The purpose of the pilot study is to investigate the reliability and validity of the model's measurement process. The results of the pilot study will be offered in a future publication. For the purposes of this paper on the mechanics of the model and its extension of the NICE Framework, anticipated results are demonstrated via detailed examples for Phases 2-4.

Figure 4: Cybersecurity Workforce Lifecycle Development



Phase 2 Example - It is imperative for an organization to understand their current work roles and how they are oriented toward security competency health. The competencies are organized into five functions: awareness, support, maintain, implementation, and design. As previously mentioned, the first step in this process is to build job groupings to which these security functions can be assigned. This step starts with a template of job groupings and job roles that represent security across the entire organization to include management, engineering, IT, OT, and security (Figure 2). Then, the organization customizes the job role groupings, and job roles within each grouping, to match organizational job roles. In Figure 3, a customized version of the workforce structure is shown. The final step of Phase 2 is to understand how the role groupings match up to the security competency functions (see Figure 5). Figure 6 shows the job role groupings to security competency mapping established through collaboration with the organization.

Figure 5: Default Job Role Group to Functional Competency Mappings

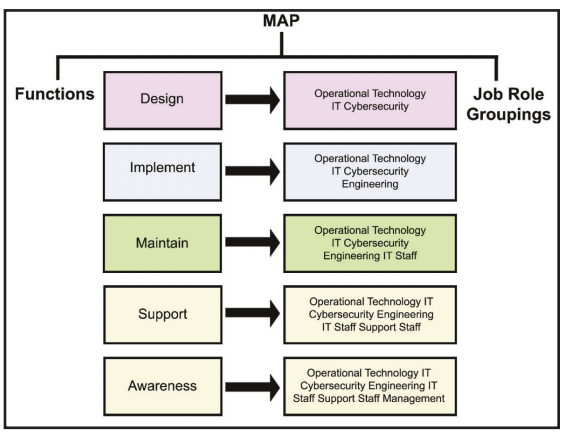


Figure 6: Mappings of Job Role Groupings to Security Competency Functional Levels

Cybersecurity Operational Readiness Maturity Level	ML-1	ML-2	ML-3	ML-4	ML-5
Security Competency Function	**Awareness**	**Support**	**Maintain**	**Implement**	**Design**
Engineering and Communications	X	X	X	X	X
Operations Technology	X	X	X	X	X
Management	X	X			
Support Staff	X	X	X		
Cybersecurity	X	X	X	X	X
IT Staff	X	X	X		

Phase 3 Example - Once the competency level of each job role grouping is known, competencies for the targeted roles can be identified. Phase 3 requires the completion of a survey consisting of the categories, specialty areas, work roles, and associated tasks of the NICE Framework. For example, the organization may decide to target the role of Database Administrator under the IT staff job role grouping for training (see Figure 3). All employees who fall into that role would fill out the survey to determine the category descriptions and specialty area descriptions that best match their organizational role as a Database Administrator. Example results of an individual survey are depicted in Table 2. The survey revealed Data Analyst as the primary role according to the NICE Framework, whereas Database Administrator is their secondary role. Although the Database Administrator fits under the IT staff role grouping, the survey determined that this employee could also require training in ICS security due to performing some ICS-related tasks in their job.

Table 2: An Example of Phase 3's Survey Results for a Database Administrator

NICE Framework Role Alignment	ICS Role Alignment
Data Analyst: 60% (Primary Role)	Industrial Cybersecurity Analyst: 15% (Tertiary Role)
Database Administrator: 25% (Secondary Role)	

Phase 4 Example - Once the major roles have been figured out that align with the NICE Framework and/or the ICS roles, the model utilizes a training repository to provide a learning path from which an organization can choose. This training repository consists of several sources such as the Illustrative Mapping of Certifications to the NICE Framework (NIST, 2018). In this case, the organization determined that both Data Analyst and Database Administrator were important roles that required training paths. Using the NIST mapping spreadsheet, the Data Analyst and Database Administrator roles are in the Data Administration column (see Figure 7). Next, the certifications applicable to each role are found by identifying an intersection between the role and a certification. Both the Database Administration role and Data Analyst role are recommended to be certified in GIAC Security Essentials (GSEC), so the GSEC certification is added to the path. This same mapping process is followed using several other sources found within the training repository to discover the full training, education, and certification(s) recommendations. The recommendations produced offer a broad view of the security training that this job role needs.

Figure 7: Illustrative Mapping of Certifications to the NICE Framework

Category	Specialty Areas	OPM Code	Work Role
Operate and Maintain	Data Administration (DTA)	421	Database Administrator (OM-DTA-001)
		422	Data Analyst (OM-DTA-002)
	Knowledge Management (KMG)	431	Knowledge Manager (OM-KMG-001)
	Customer Service and Technical Support (STS)	411	Technical Support Specialist (OM-STS-001)
	Network Services (NET)	441	Network Operations Specialist (OM-NET-001)
	Systems Administration (ADM)	451	System Administrator (OM-ADM-001)
	Systems Analysis (ANA)	461	Systems Security Analyst (OM-ANA-001)

VI. Discussion

The model provides a customized, self-help solution for a variety of organizations to understand their education gaps in security and target areas for improvement. By implementing Phases 1-5, an organization can attain quantitative results on their operational readiness and workforce competency health. Metrics for current operational readiness are gained in Phase 1 and 5, wherein an organization's security policies, practices, and processes are examined. Based on the results of Phase 1, a target profile is built aimed at better prevention, detection, and response to cybersecurity events. When suggestions for improvement in cybersecurity are aligned with business priorities, a stronger case can be presented for making more than just minimal and required changes. Results from Phase 5 can be used to demonstrate the tangible improvements made to operational readiness and the benefits of using the model.

Phases 2-4 focus on the competency health of an organization's employees. Employee's competencies are considered across the security functions of awareness, support, maintenance, implementation, and design. In Phase 2, organizations create a cyber ready workforce structure that aligns with business needs by functional level and can accomplish organizational security goals. Phase 3 pinpoints the security tasks that employees need to be able to perform according to their role(s) using a survey that streamlines the NICE Framework's workforce mapping process. Their work role may not be represented in the Framework's list, especially if it is OT-related, but the survey will tell an individual

which of the Framework's roles they most closely align with. Everyone in the organization, no matter their role, can receive recommendations on the tasks they can perform to contribute to solving cybersecurity issues. The survey's outcome gives organizations the information needed to build employee development plans that utilize tools like the NICE Framework but include additional and specific learning paths necessary to be competent and proficient in their unique security role(s).

Initial pilot work with an in-State energy provider has led to vital conversations and lessons learned. Depending on who was participating, there were contradicting answers given in Phase 1 due to different security awareness levels in the organization. This revelation has influenced the steps listed in the model's User's Guide, where Phase 1's first recommended step is to assemble a team that champions the facilitation and implementation of the model in the organization. It was also evident that organizations can get overwhelmed at the early stages of the model regarding the implementation or strengthening of a cybersecurity program. Organizations seem more willing to admit these challenges because the model is not based on penalties or fines but provides optional suggestions for improvement. During Phase 2, a self-discovery was made by an organization that they were missing roles that are necessary to perform critical cybersecurity functions. By understanding the functional roles and competencies needed, this organization can contract or hire cybersecurity help to fill these gaps. Organizations were also surprised by the cybersecurity lift that some individuals were already fulfilling to accomplish critical functions. This revelation prompted strong discussions around role separation and job succession planning.

Implications - The model is built to be performed and applied at the practitioner level, accounts for any role in an organization, and can be deployed by any size, or type of organization. Individual organizations can establish a roadmap for cybersecurity improvements based on measured cybersecurity gaps vs. just meeting minimal regulatory requirements for their industry. The roadmap can also be used to build a business case, showing the need for increased security resources and/or personnel. For the workforce, employee development plans can be used to target organizational goals such as culture change and ensure proper handling of cybersecurity incidents. These training plans can also be used by managers and Human Resources for a variety of purposes. Managers, within an organization, can measure expected performance and recommend employee training plans by understanding specific security function and role alignments. Promotions can also be awarded based on progress made in an employee's assigned training plan. Human Resources can use the training plans as benchmarks for job descriptions and task lists to fulfill security proficiencies.

The data that is gained from the cybersecurity measurement phase can be analyzed and aggregated to establish typical cybersecurity program baseline profiles as the model is applied across varying businesses and sectors. These baseline measurements can be used to inform research in the following areas: educating and training for specific industry and sector security roles, the development of targeted soft and hard skills assessments based on roles, and effective recruitment and hiring methods for cybersecurity personnel. Research can also be conducted to validate the roles included in the competency mapping survey.

VII. Conclusion

The model consists of five Phases that provide measurements and metrics for both an organization's operational readiness and its workforce competency health. Operational readiness is defined as the evidence, policy, process, and practices from which an entire organization can demonstrate preparedness towards detecting, handling, responding to, and mitigating operationally impacting cybersecurity events. Workforce competency health refers to the degree to which an organization's employees can perform cybersecurity tasks competently across the five functions: awareness, support, maintenance, implementation, and design. The model seeks to combine existing frameworks and cybersecurity resources to produce a streamlined approach for industrial companies to measure their organizational baselines and the next steps for security improvements. Figure 4 demonstrates the areas where the model has incorporated and extended the concepts from these frameworks.

References

BBC News: Technology (2014). Hack attack causes 'massive damage' at steel works. https://www.bbc.com/news/technology-30575104

Boyens, J., Paulsen, C., Moorthy, R., and Bartol, N. (2015). NIST special publication 800-161: Supply chain risk management practices for federal information systems and organizations. *U.S. Department of Commerce*: pp. ii-H4. http://dx.doi.org/10.6028/NIST.SP.800-161

Cybersecurity and Infrastructure Agency Strategic Intent: "Defend Today, Secure Tomorrow." (2019). *CISA*: p.5. https://www.cisa.gov/sites/default/files/publications/cisa_strategic_intent_s508c.pdf

Cybersecurity maturity model certification (CMMC) Version 1.02. (2020). *Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC*: pp. ii-23. https://cmmcconsultingllc.com/cmmc-information

Donnelly, J. M. (2019). America is not ready for war in cyberspace, experts warn. *Government Technology*. https://www.govtech.com/security/America-Is-Not-Ready-for-War-in-Cyberspace-Experts-Warn.html

Filkins, B., and Wylie, D. (2019). SANS 2019 state of OT/ICS cybersecurity survey. *SANS*. https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. (2018). *National Institute of Standards and Technology*: ii-44. https://doi.org/10.6028/NIST.CSWP.04162018

Fruhlinger, J. (2019). Social engineering explained: How criminals exploit human behavior. *CSO Online*. https://www.csoonline.com/article/2124681/what-is-social-engineering.html

Ho, J. (2020). Human error to blame for 9 in 10 UK cyber data breaches in 2019. *CybSafe*. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

InfoSec Institute (2020). The most common social engineering attacks. https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref

Job Role to Competency Level Recommendation. (2019). *SANS*. https://www.sans.org/security-resources/posters/ics-job-role-competency-level-recommendation/110/download

Masserini, J. (2018). NIST Cybersecurity Framework (CSF) Maturity Tool. https://johnmasserini.com/2018-nist-csf-maturity-tool-v1-0/

Menze, T. (2019). The state of industrial cybersecurity. *ARC Advisory Group and Kaspersky*. https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

Morgan, S. (2019). Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021. *Cybersecurity Ventures*. https://cybersecurityventures.com/jobs/

Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. *The Proceedings of 15th Australian Information Security Management Conference:* pp.149-155. https://doi.org/10.4225/75/5a84f7b595b4e

National Initiative for Cybersecurity Careers and Studies (2020). NICE Cybersecurity Workforce Framework Mapping Tool. https://niccs.us-cert.gov/workforce-development/mapping-tool

National Initiative of Standards and Technology (2018). Illustrative mapping of certifications to NICE Framework v1.0. https://www.nist.gov/document/illustrativemappingofcertificationstonicframeworkversion10xlsx

National Initiative for Cybersecurity Education Working Group (NICEWG) Subgroup on Workforce

Management at the National Institute of Standards and Technology (2018). Cybersecurity is everyone's job. https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

Newhouse, W., Keith, S., Scribner, B., & White, G. (2017). NIST special publication 800-181: National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework. *U.S. Department of Commerce*: pp. ii-135. https://doi.org/10.6028/NIST.SP.800-181

NIST Special Publication 800-39: Managing information security risk. Organization, mission, and information system view (2011). *U.S. Department of Commerce*: pp. ii-H-4. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Office of the Director of National Intelligence (ODNI). Counterintelligence tips: Spear phishing and common cyber attacks. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-cyber-security

Ponemon Institute LLC. (2019). Cybersecurity in operational technology: 7 Insights you need to know. https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' – A human/computer interaction approach to usable and effective security. *BT Technology Journal*.

Schneier, B. (2000). Secrets and lies: Digital security in a networked world. New York: John Wiley.

Verizon (2020). 2020 Data breach investigations report (DBIR). https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Research Perspectives

Exploring Non-Technical Knowledge, Skills, and Abilities (KSA) that May Expand the Expectations of the Cyber Workforce

Lori L. Sussman
University of Southern Maine, United States

***Abstract*— Problem Statement:** The need to produce cybersecurity workers with technical and non-technical knowledge, skills, and abilities (KSAs) is not new. NIST started the National Initiative for Cybersecurity Education (NICE) as a conference and expo in 2010. NICE was to bring together industry, government, academia, and non-profit organizations to address the U.S.'s cybersecurity education, training, and workforce needs (Petersen, 2019). The NICE Cybersecurity Workforce Framework's initial authors intended it to be a reference source for cybersecurity worker development, planning, training, and education (Newhouse, Keith, Scribner, & Witt, 2017). It was 2017 when NICE published the Cybersecurity Workforce Framework. This document provided an extensive list of technical KSAs, but not non-technical ones. At the same time, private industry started to discover the need for non-technical KSAs in their cybersecurity and other highly specialized workers. Tripwire, the security and compliance solutions provider, commissioned a survey asking 315 security professionals from over 100 US-based companies about the cybersecurity skills gap. Every participant indicated that soft skills were critical (Lapena, 2017). The report commented that the need for soft skills had increased to the point where employers were willing to hire people who were strong in these areas even if they had no security expertise. In their 2020 survey update, Tripwire noted that company security teams would be looking for some outside help to address the skills gap due to the continued strain on their teams because of the skills gap (Lapena, 2020). Despite increased data indicating the need for cybersecurity workers to master various non-technical knowledge skills and abilities, the NICE Cybersecurity Workforce Framework does not have them listed for technical roles and may not help produce the type of worker that U.S. companies need as a result (Newhouse, Keith, Scribner, & Witt, 2017). The purpose of this study is to connect with cybersecurity practitioners about the NICE Cybersecurity Workforce Framework to explore which non-technical knowledge, skills, and abilities (KSAs) should the NICE Working Group consider.

Research questions:

1. How crucial are non-technical knowledge, skills, and abilities (KSAs) to very technical cybersecurity workforce roles?
2. What are some of the essential non-technical KSAs for technically oriented cybersecurity workers?

Contribution: This research used a novel application of the Ground Truth Expertise Development Model (GTEDM) for exploring suitable non-technical, and particularly soft KSAs, for cybersecurity professional development (Assante & Tobey, 2011). The study focused on the definition and competency determination step but provided a foundational understanding for subsequent steps in further research. The only non-technical KSA exceptions were concerning training expertise for newly hired individuals, and that was an expectation of more experienced and sophisticated cybersecurity employees. However, all participants emphasized the importance of knowledge capture, sharing, and reuse. The data indicated the importance of workers integrating technical and non-technical KSAs within their role and provided a substantial list to assess for efficacy going forward. The surprising consideration is that these technical and non-technical KSAs are not the same for all roles. More work may be necessary to determine how best to account for the differences in emphasis for various roles in future research.

Theory Propositions: The literature suggested cybersecurity workers should get educational, experiential, and professional exposures to certain hard, soft, and mixed non-technical KSAs to successfully interface with clients autonomously (Shank & Robinson, 2019). The current NICE Cybersecurity Workforce Framework was focus mainly on technical expertise. Yet, research suggests that non-technical soft skills, which include problem-solving, communications, collaboration, and similar behaviors, are critical items to consider integrating into educational and professional development curricula (Blair, Hall, & Sobiesk, 2019; AACU, n.d.). It is significant to note that not all non-technical skills are soft, but these skills are often a dominant area of interest by employers when discussing non-technical skills (Litecky, Arnett, & Prabhakar, 2004). This research uses the Ground Truth Expertise Development Model (GTEDM). GTEDM has six areas that include Understanding, Assessing, Educating, Measuring, Developing, and Getting Feedback (Assante & Tobey, 2011). Cybersecurity workers progress through this cycle as they gain more

expertise. GTEDM starts with Understanding which required job definition and competency analysis as an effective way to look at those KSAs that fall under the baseline non-technical skills examined. This proposed research argues for the next iterations of the NICE Cybersecurity Workforce Framework to include non-technical KSAs to complete a more holistic Understanding phase for cybersecurity education and training (Newhouse et al., 2017). This addition provides future cybersecurity workers with critical components for employability and professional growth.

Method: The researcher used a phenomenological study method using both structured and semi-structured methods for collecting data. Over three months, the researcher conducted semi-structured interviews with cybersecurity professionals performing a wide variety of cybersecurity roles. The researcher used semi-structured interviews over other methods, such as surveys.

Findings: The field overwhelmingly agreed that non-technical skills were essential to a cybersecurity worker's success. Each participant verbalized their agreement that most of the non-technical KSAs presented were essential characteristics to consider when hiring an entry-level position during their interview sessions. The exception was in the area of training. Participants agreed that some kind of ability to train others was an essential part of a cybersecurity workers' professional development and expected of experts. The participants differed on the order of importance for the KSAs evaluated. A noteworthy area was that of how role and experience impacted emphasis which depended on a participant's personal professional progression within the GTEDM model. A participant's role often shifted the weight of importance given to non-technical KSAs more than any other demographical item. Participants' responsibilities ranged from assessing aptitude during hiring to instructing fellow workers as part of a larger security team or evaluating the cybersecurity posture's performance and efficacy for the broader organization. While these disparate points of view did not change the overall list, they did change the emphasis and order of various KSAs. The qualitative process produced three themes as non-technical KSA areas of the most significant import to the cybersecurity field. These themes included critically using information, underscoring communication skills, and emphasizing collaboration in pursue customer/client success. These clusters were reasonably uniform across roles, ages, and education.

Implications for Practice: This research integrated theoretical models with the current NICE Cybersecurity Workforce Framework to produce recommended non-technical knowledge, skills, and abilities (KSA) additions for technical cybersecurity roles. This initial list may serve as a starting point when developing programs to educate the next generation of cybersecurity workers. These non-technical KSAs, elicited from expert participants, touch upon crucial steps of the GTEDM (Assante & Tobey, 2011). Most of these discussions focused on entry-level technical cybersecurity workers. As such, further research could examine cybersecurity workers who are in later parts of the GTEDM to test the validity of these KSAs for aptitude assessment, instruction, and simulation, as well as knowledge and performance-based measurement to determine the efficacy of these KSAs for later stages of the cybersecurity professional development cycle (Assante & Tobey, 2011).

Implications for Research: Since this research used a qualitative approach, the findings may be less generalizable than some quantitative analysis but still contribute to cybersecurity education, awareness, and training body of knowledge. The researcher narrowly defined the study to make the methodology as replicable as possible. The continued inquiry of practitioners may produce a more comprehensive list of hard, soft, and mixed non-technical skills that will benefit the public, private, and academic sector organizations. Specifically, this research gathered cybersecurity expert views on essential non-technical KSAs currently missing in published workforce frameworks accepted by the field.

Keywords—TNICE; KSA; higher education; specialty area; training; work role

I. Introduction

Cybersecurity workers feel the pressure of being understaffed despite aggressive actions to hire people with the right expertise (Crumpler & Lewis, 2019). Even before the COVID-19 pandemic, reports of cyberattacks, social engineering scams, identify theft, and cyber-based financial fraud frequently made news headlines (FBI, 2020; USSS, 2020). As early as 2017, more than 93% of executives and hiring managers predicted a severe skills gap in security organizations with increased difficulty hiring people with the required skills and expertise (Lapena, 2017). However, there was little coordinated response from the public or private sector to respond to this shortage.

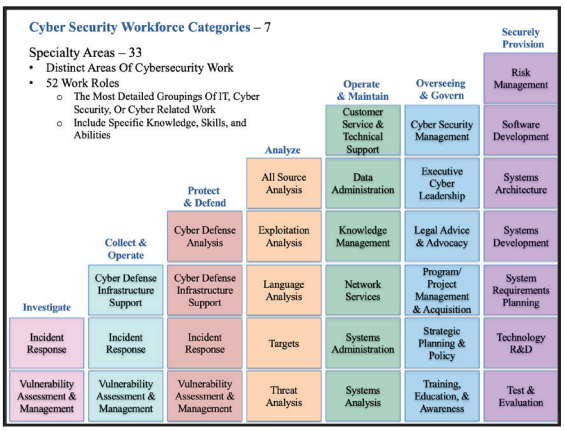
One of the organizations taking leadership surrounding this cybersecurity skills gap challenge is the U.S. Cyberspace Solarium Commission (USCSC), which released its final report on March 11, 2020. The USCSC publication coincided with

the very beginning of the COVID-19 pandemic. The significant increase of remote workers who needed secure and reliable connected technology to work at home and reduce virus exposure further exacerbated the shortage of required cybersecurity professionals (BLS, 2020). This period also saw a corresponding surge in cybercrime (USSS, 2020). The Federal Bureau of Investigation (FBI) COVID-19 Working Group, in conjunction with the Secret Service's Global Investigative Operations Center (GIOC), reported that COVID-19 related cybercrime accounted for a 300 percent jump in complaints in the first four months of the COVID-19 pandemic (FBI, 2020). The pandemic heightened the need for corporate, academic, and government institutions to work together to figure out better ways to attract and retain cybersecurity professionals.

The demand for cybersecurity workers is not new. NIST started the National Initiative for Cybersecurity Education (NICE) as a conference and expo in 2010 to bring industry, government, academia, and non-profit organizations together to address the U.S. cybersecurity education, training, and workforce needs (Petersen, 2019). NICE used the expertise model that contained three interrelated components of knowledge, skill, and abilities to formulate cybersecurity work roles (Dali'Alba, 2018). Figure 1 depicts all cybersecurity work categories, specialty areas and work roles enumerated within the NIST Special Publication 800-181 NICE Cybersecurity Workforce Framework (Newhouse et al., 2017).

There were four primary authors who queried stakeholders from academia, government, industry, and non-profit organizations for comment. NIST intended this document to be an essential reference for describing and sharing information about cybersecurity work and worker KSAs (Newhouse et al., 2017). While the NICE Cybersecurity Framework (2017) did not guide much non-technical knowledge, skills, and abilities (KSAs), it did establish both a taxonomy and a shared vocabulary for the "eyes on keyboard" worker. These common terms, language, and structures were foundational to describing cybersecurity work and workers for the public, private, and academic sectors.

Figure 1: NICE Cybersecurity Workforce Framework



Note. *Adapted from Newhouse, Keith, Scribner, and Witte (2017). Work roles are not job titles, and a practitioner could have one or more work roles assigned to their position.*

Users of the NICE Framework implemented it locally for different workforce development, education, or training purposes (Newhouse et al., 2017, p. 2). The work role descriptions were devoid of non-technical KSAs due to an overemphasis on all things technical. Examining knowledge areas illustrates this point about stressing technical KSAs. There are 630 knowledge areas, and arguably there are ten that are non-technical and are most associated with training (Newhouse et al., 2017). The impending publication of a revised NICE Cybersecurity Workforce Framework that went out for cybersecurity stakeholder comment in 2019 provides an opportunity to address the gap concerning non-technical KSAs.

The NICE Working Group (NICEWG) engaged the public, private, government, and academic sectors to produce unifying standards for recruiting, educating, and developing cybersecurity experts (NIST NICEWG, n.d.). The mission of NIST NICEWG was to understand, assess, educate, measure, and develop the next generation of cybersecurity experts. NICEWG experts understood how the emergence of a pandemic in 2020 and the associated pivot to a more remote and distributed workforce globally increased pressure on computer security teams.

Expertise Requires an Expression of Skill

Expertise is commonly represented by two systems, which are factual (technical) and heuristic (non-technical) KSAs (Buchanan, Davis, Smith, and Feigenbaum, 2018). In some circumstances, non-technical KSAs are equated with the term "soft skill." The U.S. Army created this term in 1968 to mean any skill that was not mechanical or technical, which implies the heuristic KSAs (U. S. Army United States Continental Army Command, 1968). The field now considers non-technical KSA as activities such as problem-solving, communications, collaboration, and similar behaviors (Blair, Hall, & Sobiesk, 2019, March; AACU, n.d.). It is important to note that not all non-technical skills are soft, but these are often a dominant area of interest by employers when discussing non-technical skills (Litecky, Arnett, & Prabhakar, 2004).

The need to include non-technical skills, and particularly soft skills, into cybersecurity professional development is not new. The literature showed that expert performance is enhanced by secondary traits that share the expression of expertise (Winegard, Winegard, & Geary, 2018). To this point, the security and compliance solutions provider, Tripwire, commissioned a survey asking 315 security professionals from over 100 US-based companies about cybersecurity skills gaps, and every participant noted that soft skills were essential (Lapena, 2017). The study offered that the need for soft skills had increased to the point where employers were willing to hire people with strong soft skills even if they had not technical cybersecurity expertise. In their 2020 survey update, Tripwire noted company security teams were highly strained due to difficulty staffing and continued to look for external assistance to address the skills gap (Lapena, 2020).

Tripwire's data underscores the need to integrate both technical and non-technical KSAs into every cybersecurity role. The lack of non-technical KSA in the published NICE Cybersecurity Workforce Framework indicates that it is incomplete, may not help produce the multi-faceted cybersecurity workers that U.S. companies need. The purpose of this study was to connect with cybersecurity practitioners about the NICE Cybersecurity Workforce Framework to explore which non-technical KSAs NIST and its NICE working groups should consider for inclusion in the next iteration.

Background of the NIST Cybersecurity Workforce Framework

According to the U.S. Department of Labor, most cybersecurity positions require a bachelor's degree in a computer-related field (BLS, 2020). The supposition is that this credential provides some semblance of validity to specific foundational KSAs of entry workers. However, the creation of a professional cybersecurity workforce does not fall on the shoulders of academia alone. As pointed out by the Cyberspace Solarium Commission's recently released final report, the need for a well-trained cyber workforce is a private-public imperative. Co-chairmen Senators Angus King and Representative Mike Gallagher framed the cyber talent situation in this way,

> *The U.S. government should recruit, develop, and retain a cyber workforce capable of building a defensible digital ecosystem and enabling the agile, effective deployment of all national power tools in cyberspace. Doing so will require designing innovative programs and partnerships to develop the workforce, supporting and expanding good programs where they are already in place, and connecting with a diverse pool of promising talent. Sometimes success in building a robust federal workforce depends on elements outside of the federal government. In those cases, the U.S. government can and should play a supporting role by providing its partners in workforce development with tools needed to accelerate the increase in cyber personnel. (p. 43)*

The report also recommends that standards and frameworks developed by the Cybersecurity and Infrastructure Security Agency (CISA) and its U.S. National Initiative for Cybersecurity Education (NICE) should continue to expand.

The Cybersecurity and Infrastructure Security Agency Act of 2018 established CISA to improve cybersecurity across all government levels, coordinate between the federal and state governments, and strengthen the nation's overall cybersecurity posture (CISA Act, 2018). CISA created the National Initiative for Cybersecurity Careers and Studies (NICCS) to provide the U.S. with a comprehensive resource addressing cybersecurity knowledge needs (CISA, 2020). This initiative partnered CISA with the Department of Homeland Security (DHS), the National Institute of Standards, and Technology (NIST), the Office of

the Director of National Intelligence (ODNI), and the Department of Defense (DOD). NIST published the first NICE Cybersecurity Workforce Framework in 2012, and it is updated periodically to meet the needs of this fast-evolving field (Newhouse et al., 2017).

The most recent NICE Cybersecurity Workforce Framework provides a fundamental reference resource that specifies cybersecurity work and the KSAs for cybersecurity professionals. Most of the catalogued skills require technical mastery, such as "skill in reading hexadecimal data." Notably, the category of Oversee and Govern is more integrative, including cybersecurity leadership, management, legal advocacy, program/project management, and training/education/awareness (Newhouse et al., 2017). This is the areas within the publication where the majority of non-technical KSAs are found.

The NICE Cybersecurity Workforce Framework relegates non-technical skills such as Skill ID S0102, called "skill in applying technical delivery capability" to curriculum developers and other non-technical support work listed for education, training, and awareness roles (Newhouse et al., 2017). However, cybersecurity requires teams of people with a wide range of backgrounds and skills, not all technical, to be effective (Lee, 2019; National Research Council, 2013). The current NICE Cybersecurity Workforce Framework does not fully recognize this need for a diversity of skills, which is a gap. This research explores the most imperative non-technical KSAs with cybersecurity practitioners to discover which are the most urgent for inclusion in future versions of SP 800-181. As pointed out by the National Academy of Sciences,

> *Education, training, and workforce development activities that focus too much on narrow technical knowledge and skills may discourage participation by people with much-needed non-technical knowledge and skills, may overly concentrate attention and resources on building technical capability and capacity, and may discourage technically proficient people from developing non-technical skills. The result would fall short of delivering the workforce the nation requires (National Research Council, 2013, p. 26).*

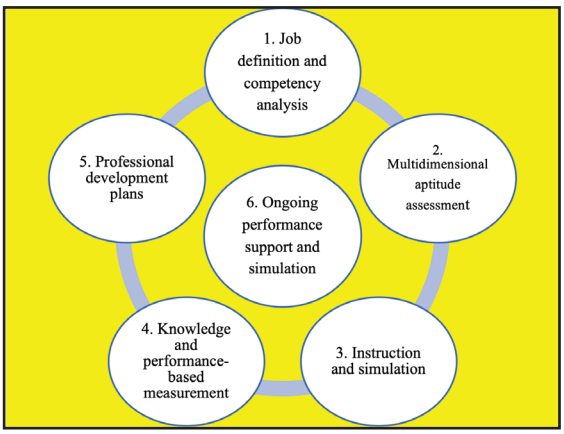
Recent research supported this call to action. Blair, Hall, and Sobiesk (2019) found that educating future cybersecurity professionals requires a multidisciplinary approach. They concluded cybersecurity curricula development should be "interdisciplinary in that they support a personal approach to problem-solving and knowledge development that requires synergy across disciplines within an individual" (Blair et al., 2019, p. 59).

Developing a Conceptual Framework

The multidisciplinary KSAs that also fall under the Association of American Colleges and Universities VALUE rubrics are identified by hiring managers as necessary KSAs for technical workers to get hired (AACU VALUE Rubrics, n.d.). There appears to be a two-stage recruiting model where requisite technical skills get candidates past the filters to an interview. It is the interview step that is most crucial in the hiring process. Hiring mangers assessed candidates for their demonstrated soft skills and cultural fit as top hiring criteria (Litecky et al., 2004). Research found that hiring officials looked for inquiry and analysis, critical thinking, creative thinking, written communication, oral communication, reading, quantitative literacy, information literacy, teamwork, and problem-solving KSAs in future workers (AACU VALUE Rubrics, n.d.; Blair et al., 2019; Litecky et al., 2004). This study used non-technical KSAs gleaned from the current NICE Cybersecurity Framework as a starting point to discuss with cybersecurity professionals and the qualitative analysis used categories noted by AACU for qualitative categorization and analysis. Current theory informed the qualitative process used when exploring the significance of non-technical KSAs with cybersecurity practitioners.

The present Cybersecurity Workforce Framework had some non-technical KSAs and those were mapped to the GTEDM model thus producing a conceptual framework for analysis. A conceptual framework uses theory, research, and experience to examine the relationship between constructs and ideas (Bloomberg and Volpe, 2016). In this case, the Ground Truth Expertise Development Model (GTEDM) and its first step requiring job definition and competency analysis provided an effective way to look at those KSAs that fall under the baseline non-technical skills examined. GTEDM's six significant areas are understand, assess, educate, measure, develop, and get feedback to create cybersecurity experts who will help continually improve the field (Assante & Tobey, 2011).

Figure 2: The Ground Truth Expertise Development Model (GTEDM)



Note. *Adapted from Assante and Tobey (2011), this model helps identify and develop future cybersecurity experts.*

The GTEDM provides the path to expertise that could be accelerated by understanding all of the KSAs necessary along the development path (see Figure 2). As noted by the National Board of Information Security Examiners (NBISE) (Tobey, 2012, pp. 10-11),

> *Traditionally it takes many years to mature a cybersecurity worker's knowledge, skills and performance. Senior cybersecurity professionals possess a special mix of information security (InfoSec), technology infrastructure, risk, operations, social, analytical, and organizational skills. To reach peak performance, senior security engineers had to first become highly proficient I.T. professionals. Years of accumulation of I.T. knowledge are then enhanced with years of additional security experiences, which eventually allows mastery of forensics, risk management and business impact principles. This path ultimately allows a seasoned InfoSec expert to perform highly skilled actions that protect grid control systems on infrastructure in a way that is aligned with organizational and regulatory policies and goals.*

The NBISE discovered that it was the non-technical skills that differentiated experts from those who were competent (journeyman) or proficient (apprentice) (Tobey, 2012). These studies concluded that identifying technical and non-technical cybersecurity KSAs at each point in a professional's progress from apprentice to journeyman could allow educators to develop curricula that engender accelerated development.

In order to get clear definitions for the GTEDM, the investigator engaged field experts to share their views on essential non-technical KSAs currently missing. The research design involved integrating theoretical models with the current NICE Cybersecurity Workforce Framework (Newhouse et al., 2017) to produce a non-technical KSA list to present to experts as a conversational starting point. Since defining KSAs are part of the Understand phase of the GTEDM, the investigator bound much of the conversation with the participants to the early career stage. Some interviews touched up subsequent steps of the GTEDM, but that was relatively limited. The use of published KSAs from the current NICE Cybersecurity Workforce model served to get immediate participant acceptance of the KSAs presented for their review. The cybersecurity field experts' involvement and insights produced rich data necessary for job definition and competency analysis (Assante & Tobey, 2011). As such, this conceptual model helped bound the inquiry process and provided ideas for future investigation.

The author interviewed 43 self-identified cybersecurity professionals from industry, non-profits, government, and higher education to address the gap. This study focused on exploring non-technical KSAs that experts believed were instrumental to a cybersecurity worker's success. This body of work focused on answering two research questions concerning the relative importance of the non-technical KSA gaps in the current NICE model. The first question dealt with ascertaining the degree of importance cybersecurity professionals placed on non-technical KSAs for their entry-level and other cybersecurity workers. The second question centered on soliciting opinions about the most urgent, if any, non-technical KSAs that the future NICE Cybersecurity Workforce Framework should consider adopting.

It is vital that most cybersecurity professionals are integral members of organizations, and their activities support a group's goals and objects. As such, the majority of participants come to cybersecurity with a customer-service-centric lens. The business world has long studied models that allowed them to define and assess its own non-technical KSAs and teach its staff these values. Sandwith (1993) identified five critical areas: conceptual/creative, leadership, interpersonal, administrative, and technical. Synthesizing the literature and the conceptual model, the researcher

used these five areas to qualitatively categorize and analyze the cybersecurity practitioners' interview transcripts (see Table 1).

Table 1: Technical Cybersecurity Role Non-technical KSAs

Competencies	Non-technical KSAs
Hard	• Knowledge of and compliance with legal and regulatory • Managing crisis situations, such as fires, employee or guest injuries, tornados, etc. • Using computers effectively
Soft	• Customer service problem resolution • Developing positive customer relations • Facilitating teams and teamwork • Leadership abilities • Managing personal stress • Negotiating techniques • Presentation skills • Professional demeanor and appearance • Using ethics in decision making • Working effectively with peers • Written communication skills
Mixed	• Critically using information for decision making • Training employees

Note. *Adapted from Sisson and Adams, 2013*

The study design used a grounded approach for data collection and interpretation of KSAs discussed and recommended by the participants. This approach allowed the researcher to create appropriate non-technical KSA recommendations for technical cybersecurity professionals based on theoretical models discussed (Haney, & Lutters, 2018; Mitchell et al., 2010; Litecky et al., 2004).

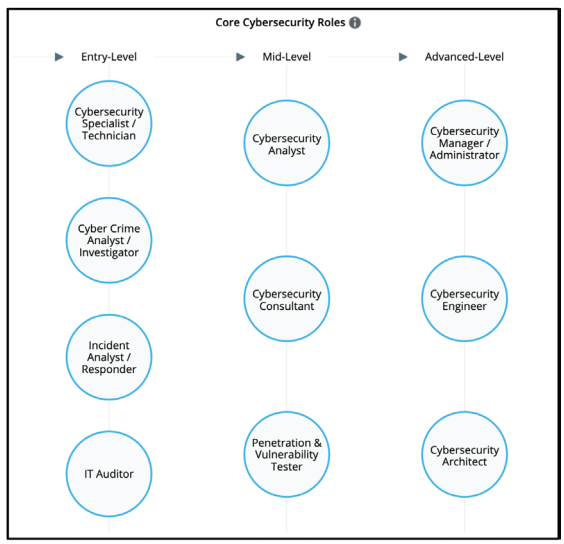
The Customer Service Model as a Point of Departure

Data from the U.S. Department of Labor suggests that customer service representatives, computer support specialists, and information security analysts are similar entry occupations regarding duties and job growth. Customer Service Representatives (CSR) typically use telephones, computers, and other office equipment, but their central role is to explore customer solutions (US BLS, 2020). CSR's that are less educated and do not have unique skills are paid substantially less than their more technical. A worker who is in these types of client interfacing roles are judged based upon their ability to deliver service that meets customer expectations (Parasuraman, Zeithaml, and Berry, 2018). Service quality research stressed five dimensions that influence customer perceptions of service quality. These dimensions included reliability, responsiveness, assurance/empathy; and tangibles such as physical cues (Nyadzayo & Khajehzadeh, 2016). These categories helped guide qualitative analysis and synthesis during the coding process.

Evaluating Entry-Level Helpdesk Jobs

It was crucial to understand the expectations managers have for positions that interface with end-users or customers. Most entry-level cybersecurity jobs are auditor, analyst, responder, and technician roles that require some level of customer interaction, often requiring the employee to educate about and advocate for cybersecurity compliance (see Figure 3) (Cyberseek Career Pathways, n.d.).

Figure 3: Cyberseek Cybersecurity Career Pathway Excerpt



Note. *This dataset as of July 7, 2020. This interactive model shows critical jobs within cybersecurity, frequent transition opportunities between them, and detailed information about each role's salaries, credentials, and skillsets.*

Computer Support Specialists (CSS) in networking, software development, systems engineering, financial and risk analysis, and security intelligence are typical cybersecurity feeder roles (Cyberseek Cybersecurity career pathway, n.d.). While there are many paths into the occupation, many computer support specialist positions require a bachelor's degree. Still, an associate degree or postsecondary classes may be enough for others if accompanied by industry certifications (US BLS, 2020). The median income in 2019 was almost double that of a customer service representative, but that is because computer support specialists

have specialized KSAs and may need to work nights or weekends due to the need for constant computer availability (US BLS, 2020). Employment of computer support specialists is projected to grow 10 percent from 2018 to 2028, faster than the average for all occupations, but not as quickly as cybersecurity workers.

The information security analyst role is representative of entry-level cybersecurity jobs. In 2019, the median salary was $99,730 per year, as most positions require a bachelor's degree in a computer-related field and experience in a related occupation (US BLS, 2020). The U.S. Bureau of Labor Statistics (BLS) projected that employment of cybersecurity professionals such as information security analysts growing 32 percent from 2018 to 2028, which is much faster than the average for all occupations (US BLS, 2020). As of July 2020, there were more than 500,000 cybersecurity job openings, with demand growing for workers who can create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks (CyberSeek, Interactive Map, n.d.).

These roles seem related because the persons involved similarly interact with customers when delivering services face to face, by email or text, via live chat, or through social media. The differences are educational requirements and technical expectations when interacting with customers at any given time, both during the business week and during off-hours. However, hiring managers frequently report that STEM graduates often lack written and oral communication, project management, teamwork, problem-solving, critical thinking, and interpersonal skills (Jang, 2016). This frustration has led to companies hiring non-skilled workers with strong soft skills and investing in training them for technical work (Lapena, 2020). Unfortunately, this is a time consuming, costly, and ultimately unsustainable approach for hiring cybersecurity workers. It is important to future cybersecurity workers that they receive experiences and exposures to non-technical KSAs to be competitive in the job market.

Mining the NICE Cybersecurity Workforce Framework for Non-technical KSAs

The conceptual framework uses the NICE Cybersecurity Workforce Framework KSAs delineated for the cybersecurity curriculum developer role to develop the participant interrogatory. This position, and similar Oversee and Governance roles, feature six knowledge units, six skills, and thirteen abilities that relate well to the non-technical and important soft KSAs discussed earlier. In keeping with the GTEDM model's progression, the first step was to understand better and define the non-technical KSAs. To that point, the NICE Cybersecurity Workforce Framework non-technical KSAs were compared to those considered most critical by the field as confirmed by current research (see Table 2) (Blair, Hall, & Sobiesk, 2019; Newhouse et al., 2017; AACU, n.d.; Litecky et al., 2004).

Table 2: NICE Framework Non-Technical KSAs for Cybersecurity Curriculum Developer

Knowledge	K0146: Knowledge of the organization's core business/mission processes K0239: Knowledge of media production, communication, and dissemination techniques and method K0243: Knowledge of organizational training and education policies, processes, and procedures K0245: Knowledge of principles and processes for conducting training and education needs assessment K0246: Knowledge of relevant concepts, procedures, software, equipment, and technology applications K0287: Knowledge of an organization's information classification program and procedures for information compromise
Skills	S0064: Skill in developing and executing technical training programs and curricula S0066: Skill in identifying gaps in technical capabilities S0070: Skill in talking to others to convey information effectively S0102: Skill in applying technical delivery capabilities S0166: Skill in identifying gaps in technical delivery capabilities S0296: Skill in utilizing feedback to improve processes, products, and services
Abilities	A0013: Ability to communicate complex information, concepts, or ideas A0018: Ability to prepare and present briefings A0019: Ability to produce technical documentation A0024: Ability to develop clear directions and instructional materials A0063: Ability to operate different electronic communication systems A0070: Ability to apply critical reading/thinking skills A0083: Ability to evaluate information A0089: Ability to function in a collaborative environment A0105: Ability to tailor technical and planning information to a customer's level of understanding A0106: Ability to think critically A0112: Ability to monitor advancements to ensure organizational adaptation and compliance A0118: Ability to understand technology, management, and leadership issues related to organization processes and problem-solving A0119: Ability to understand the basic concepts and issues related to cyber and its organizational impact

Note. *Adapted from National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al., 2017).*

These KSAs constituted the discussion starting point during the interviews for field validation and recommendations for additions, deletions, and modifications.

II. Method

The researcher used a phenomenological study method using both structured and semi-structured methods for collecting data. Phenomenology does not seek to explain but rather facilitate more in-depth insight into an experience through a description (Bloomberg & Volpe, 2016). However, phenomenological studies can be more than just descriptive. The phenomenological investigator organizes the data into meaning-making units

that cluster into common categories or themes (Moustakas, 1994). Collecting data in many forms and using that information for spiral analysis will help with data management, coding, classifying, interpreting, and finally representing and visualizing the data (Creswell, 2018). This study used inductive reasoning to understand interview information. The conceptual Framework informs this effort and shapes themes and categories (Merriam & Tisdell, 2016). The data analysis is an iterative process requiring the researcher to frame, reframe, and interpret the information (Creswell, 2018). These findings may lead to a better understanding of the requisite non-technical skills cybersecurity workers should develop (Ravitch & Riggan, 2017).

Over three months, the researcher conducted semi-structured interviews with cybersecurity professionals performing a wide variety of cybersecurity roles. The researcher used semi-structured interviews over other methods, such as surveys. The participants received an advance copy of KSAs listed in Table 2 for review prior to the scheduled session. Interviews provide a richness of data and the latitude to ask follow-up questions. This ability to pursue detail puts the researcher in a unique position to probe and clarify, thus using the interview as a mechanism to encourage participants to add other pertinent information (Creswell, 2018).

The researcher used social media such as LinkedIn to request participation from self-described cybersecurity professionals. There were over 100 initial responses, 65 initial intakes, 45 interviews, and 43 returned approved transcripts. Participants agreed to Zoom recordings of their talks, which accelerated transcription with its automated cloud transcription capability for enterprise users. The principal investigator reviewed and corrected the automatic transcription before sending the document to the participants for review and approval. The transcripts were stored without personal identifiers and uploaded into NVIVO for qualitative coding. The researcher did not compensate participants for their involvement with this study.

Purposeful Sampling

The investigator narrowed the sample population to those who explicitly used cybersecurity as part of their job description or title for this study. As a grounded theory study, the researcher found that these cybersecurity professionals provide the most authoritative reasoning behind which non-technical skills were essential for new worker professional development (Creswell & Poth, 2018). The 43 interviews represent a wide range of roles from cybersecurity executive at a Fortune 50 company to individual contributors working in small businesses. This use of maximum variation sampling provided substantial variation in perspectives, experiences, and exposures, thus offering greater insight into the phenomena that shape the need for non-technical KSAs (Creswell & Poth, 2018). The researcher was open to snowballing, and several participants identified others for this study. The NICE Workforce Framework provided the definitional boundary for cybersecurity professional and guided recruitment. The resulting pool was more diverse and senior than the cybersecurity field writ large (see Table 3). According to ISC(2) (2019), the workforce is over 66% male, with 38% completing a bachelor's degree, 28% achieving a master's degree, and 10% doctoral or post-doctoral degrees. The workforce is also relatively young, with 37% under 35 years of age, 33% between 35 and 44, 19% between 45 and 54, and less than ten over 55.

Table 3: Participant Demographics

Age Groups		**Gender**	
50 - 59	21	Male	29
40 - 49	8	Female	14
60 - 69	6	**Years of work experience**	
30 - 39	5	Between 16 and 25 years	16
20 - 29	2	Between 26 and 35	12
70 - 79	1	36 years or more	10
Education		Between 6 and 15 years	4
Completed graduate school	27	Five years or less	1
Completed undergraduate	13	**Experience**	
Completed doctorate	2	Public Sector	35
Completed high school	1	Private Sector	37

This participant sample was 67% male. The group was also more educated, with 29% having a bachelor's degree, 64% completed a master's degree, and 5% had a doctorate or higher. The group was a bit older than the field, with 66% being 50 or older, 17% in their 40's, 12% in their 30's, and 5% in their 20's. These minor variations from the field demographics helped get the hiring manager's perspective during the interviews.

III. Data Collection

The researcher conducted 43 semi-structured interviews that were planned for 45 minutes and did not exceed one hour. The interview questions used non-technical KSAs derived from the current NICE Workforce Framework. Most of these attributes came under non-technical roles, such as Cybersecurity Curriculum Developer. The investigator asked each participant about the relative importance of these KSAs for more technical cybersecurity workers. The interviewer then asked them to identify what was missing from the list provided. Knowledge, skills, and abilities were all discussed separately (see Table 2).

The first three interviews served as a pilot to discern potential flaws and timing challenges. Because there were no revisions to the protocol, the researcher included data from these interviews in the final data set. This approach aligns with accepted qualitative research methods. The researcher coded the data until reaching theoretical saturation, the point at which no new themes or ideas emerged from the data (Creswell & Poth, 2018).

IV. Analysis

Creswell and Poth (2018) describe data collection as a series of interrelated activities that include locating the individual, gaining access and making rapport, purposeful sampling, collecting data, recording the information, resolving field issues, and storing data. Moustakas (1994) suggests that a phenomenological interview be informal, interactive and uses open-ended comments and questions to get the participant to share their full story. This study followed Creswell's (2013) steps at the macro level for its methodology. Also, this study used Moustakas' (1994) philosophy for instrument construction. These frameworks provided useful synergies to reach an optimal research methodology.

Data analysis involved a detailed coding process, pattern-matching, and meaning-making (Creswell & Poth, 2018). The researcher used software tools to remain objective and rigorous in the analysis (Roberts, 2010). A strategy is required for the successful use of this type of software to include putting information into thematic arrays, creating a matrix of contrasting categories and placing evidence underneath, creating visual displays, tabulating the frequency of different events, and creating a chronological or other types of sequence (Yin, 2018; Merriam & Tisdell, 2016). Using Computer-Assisted Qualitative Data Analysis Software (CAQDAS), the researcher first coded to develop meaning units. Subsequent coding iterations collapsed categories, clustered KSAs into common categories, and created textural descriptions of the participants' experiences (Merriam & Tisdell, 2016; Moustakas, 1994).

The non-technical skills fell into three major nodal categories of hard non-technical KSA, soft non-technical KSA, and mixed non-technical KSAs. The hard non-technical KSAs included knowledge of core business processes, using computers effectively, knowledge of and compliance with legal and regulatory requirements, and managing crises. Not surprisingly, the list of soft skills was the longest (see Table 4).

Table 4: Soft Skills Coded

Nodes	Skills
Soft competencies	Presentation skills
Soft competencies	Developing positive customer relations
Soft competencies	Customer Service Problem Resolution
Soft competencies	Written communications skills
Soft competencies	Working effectively with peers
Soft competencies	Facilitating teams and teamwork
Soft competencies	Intellectual curiosity
Soft competencies	Adaptability
Soft competencies	Professional demeanor
Soft competencies	Negotiating techniques
Soft competencies	Ethics in decision making
Soft competencies	Managing personal stress
Soft competencies	Leadership abilities

The mixed non-technical KSA was the shortest list that included critically using information for decision making and training. Data saturation occurred by the thirty-third coding, but the researcher continued to code all participant data to achieve trend data for KSA recommendations. Coding all participant data produced qualitative themes based on category aggregation and trend data based on nodal references.

The researcher used pattern coding to group summaries into smaller numbers of categories (Saldaña, 2016). These pattern codes identified both emergent themes and explanatory groupings. The pattern coding led the researcher to construct the assertion that non-technical KSAs were significant to a cybersecurity worker's professional success and development. Clustering under the

NICE Cybersecurity Framework KSAs developed over the second and third coding cycles. The CAQDAS tool supported a super coding analytical process where relationships between codes enabled future reflection and continued analysis (Saldaña, 2016). The pattern codes collapsed into NICE Cybersecurity Framework KSAs that provide insight into the participant's emphasis on some aspects of the baseline KSAs presented during the interviews. The resulting themes and inferences from coding clusters construct some useful recommendations for non-technical KSAs that should be included in the NICE Cybersecurity Framework's next iteration.

V. Findings

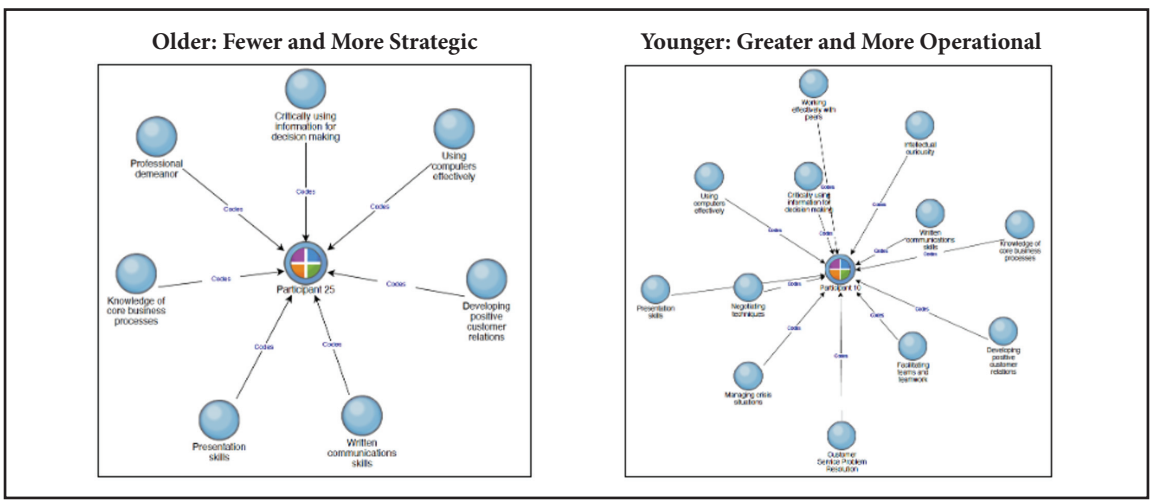
The research design provided significant data to as to which KSAs NIST should consider for inclusion in the next iteration of the Cybersecurity Workforce Framework. The first research question explored the level of importance that the cybersecurity field regarded non-technical KSAs for very technical cybersecurity workers. Each participant verbalized their agreement that most of the non-technical KSAs presented were essential characteristics to consider when hiring an entry-level position during their interview sessions. The exception was in the area of training. Participants agreed that some kind of ability to train others was an essential part of a cybersecurity workers' professional development and expected of experts. To this point, one cybersecurity expert shared,

> *Multiple times users will call the security operation center and the analysts need to walk the user through resolution of an incident. Many times, it is just simple email phishing. Or spam of some sorts, but the analysts must walk them through remediation, and the analysts have to convey what they are looking at. The user does not know what to do even though they have taken a class on it. Our analysts are now training them step by step on what they need to do to remediate that problem.*

In other words, knowledge capture, sharing, and reuse were necessary. Still, the participants did not expect entry-level cybersecurity professionals to do that well at first but develop proficiency over time. There was a range of ideas surrounding which KSAs should rise to the top as the most essential, and some depended on role and experience. The data reflects participant perceptions of proposed non-technical KSAs based on their experience, education, and exposures. This study reinforced the Tripwire findings, where participants unanimously agreed that non-technical skills were indispensable to a cybersecurity worker's success (Lapena, 2017, 2020).

The second research question probed to find which non-technical skills were most critical KSAs to address first in the Cybersecurity Workforce Framework. The participants' perceptual lens was heavily influenced their role as expressed in Assante and Tobey's (2017) GTEDM. A participant's role informed the technical and non-technical

Figure 4: Contrast Between Senior versus Junior Participants' Non-technical KSAs Emphasis



Note. *The left diagram represents a participant in an executive role and the right diagram represents a participant in a mid-level operational position.*

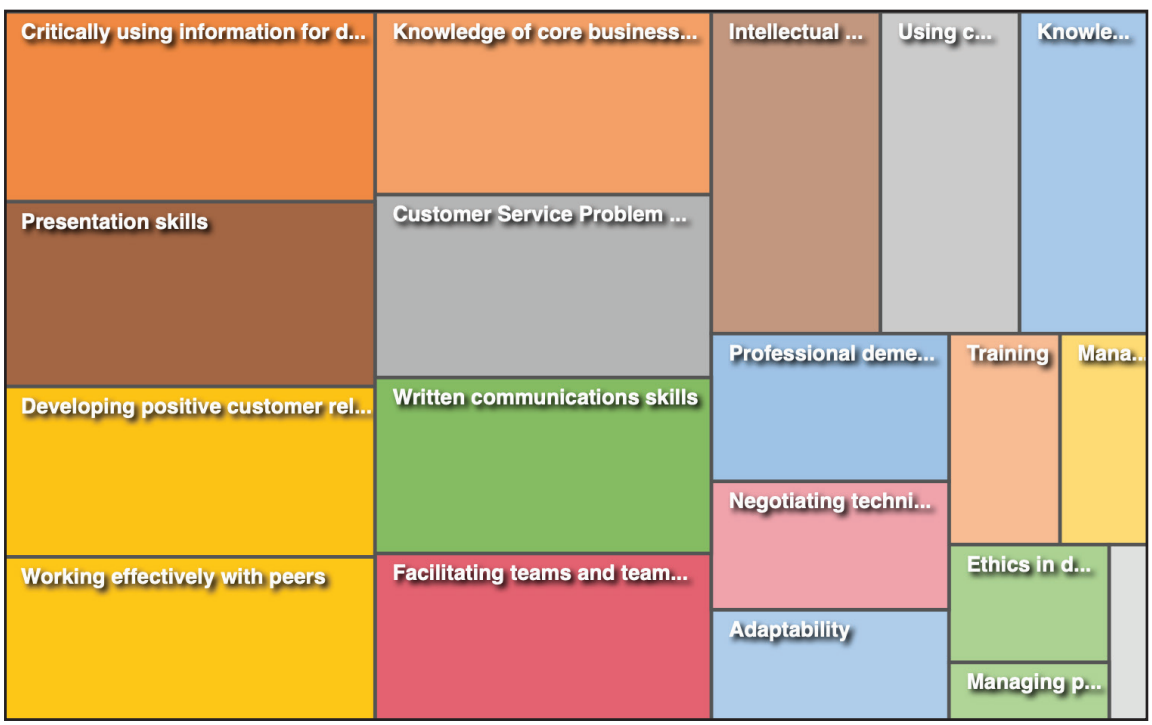
KSA conversation used to define cybersecurity competency and readiness. The more managerial the position, the more the concern shifted from customer problem resolution to assuring a positive customer experience (see Figure 4). While these disparate points of view did not change the overall list, they did change the emphasis and order of various KSAs. In part, that could be due to the difference in strategic versus the operational focus of the participant's cybersecurity role.

It is crucial to note that readers should refrain from making quantitative inferences from this work. The nature of the semi-structured format for interviews provides multiple voices and perceptions. Although the investigator used nodal reference counts emphasize a particular area, the conclusion of the significance of the trend information did not rely on frequency alone. The importance of insight does not rest solely on the number of participants who voice it. It is instructive to review those areas most often brought up by the participants to harmonize the disparate trend data due to demographic influences (see Figure 5).

After data collection, the researcher performed open coding to label, look for meaning, and begin categorizing the data. The investigator then created a codebook to code all 42 interviews after the preliminary analysis deductively. By iteratively coding, salient concepts emerged from those interviews. These activities led to the development of a codebook. The author then used this codebook to code the interviews deductively. This process

Figure 5: Summary Word Cloud Denoting Participants' Aggregate Emphasis Areas

Figure 6: Aggregated Participant Response Hierarchy Model



produced three themes as non-technical KSA areas of the most significant import to the cybersecurity field. These KSA themes required included critically using information, communications skills, and collaboration to pursue customer/client success. These clusters were reasonably uniform as they were aggregated across roles, ages, and education (see Figure 6 on the previous page).

It is significant to note that the CAQDAS clustering did not denote significance based solely on the number of items coded but included the number of participant references to a particular skill. After several code checking iterations, the skill references breakout showed the soft non-technical skills as the area of most significant emphasis (see Table 5).

Table 5: Total Coding Roll-Up of All Non-Technical KSAs By Type

Nodes	Skills	Number of coding references	Number of items coded
Soft	Presentation skills	153	40
Soft	Developing positive customer relations	145	38
Mixed	Critically using information for decision making	140	41
Soft	Customer Service Problem Resolution	134	39
Soft	Written communications skills	117	36
Soft	Working effectively with peers	114	37
Hard	Knowledge of core business processes	104	38
Soft	Facilitating teams and teamwork	96	34
Soft	Intellectual curiosity	84	35
Hard	Using computers effectively	64	30
Hard	Knowledge of and compliance with legal and regulatory requirements	63	29
Soft	Adaptability	48	22
Soft	Professional demeanor	46	19
Soft	Negotiating techniques	30	16
Hard	Managing crisis situations	26	13
Mixed	Training	14	10
Soft	Ethics in decision making	14	10
Soft	Managing personal stress	5	4
Soft	Leadership abilities	3	3

The stress on soft skills as essential non-technical KSAs for technical cybersecurity roles is a critical finding that supports the current literature specifying the desirability of these skills by the workforce (Crumpler & Lewis, 2019; Lapena, 2017).

Intellectual Curiosity Drives Critical Approaches

Participants valued attitude over aptitude for many roles, but especially for entry-level positions. The technical prowess that a cybersecurity worker brings to bear is only useful if that person can marry critical thinking, reading, listening, and writing skills to solve the client or customer's problem. As one cybersecurity manager who works at a cybersecurity consulting firm explains,

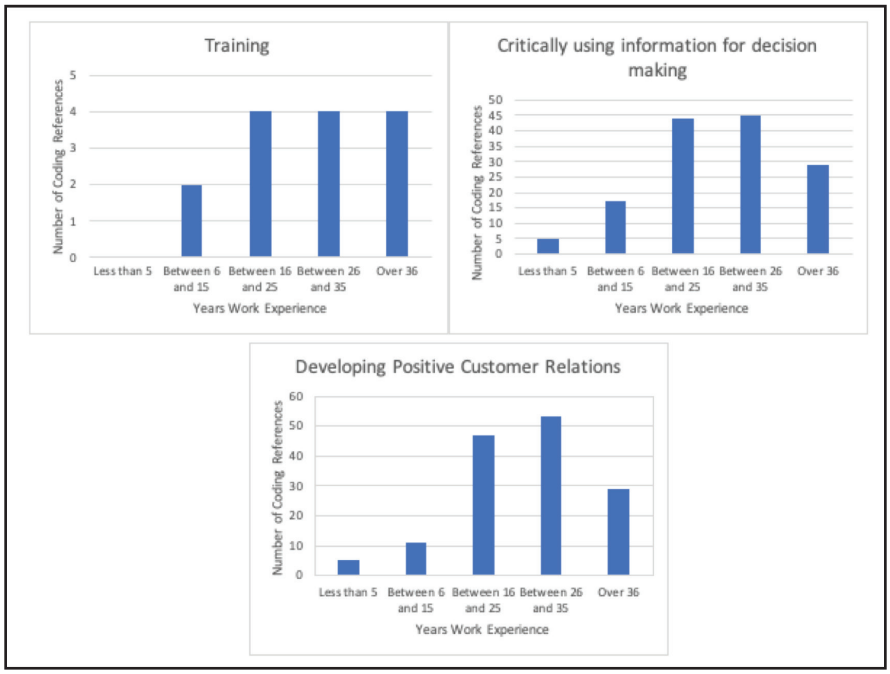
> *One of the things that I find lacking in many of the individuals who go into cybersecurity, especially junior analysts, is that they do not understand what is being done. For example, on the data loss prevention tool, the alert will fire, and the analyst will look at the alert, and they are translating it from a literal perspective. They do not understand that the software is scanning for number sequences, and that is what triggers the alert. If you understand the concepts of either the application, the software, or the equipment and how it's being applied, then analysts can actually better understand how to go about responding to the information that's provided to them.*

The field sent a clear message that cybersecurity workers need to be intellectually curious, which pushes them to both research and better understand the technical and business environment holistically. In this way, these workers can use critical thinking skills to elevate their technical knowledge, thus solving team and client issues better and faster.

The difference in participant experience did impact emphasis. There was a corresponding emphasis on the customer/client experience based on the participant's seniority (see Figure 7). KSAs such as training, critical use of information for decision-making, and presentation KSAs rose to the top for more experienced participants.

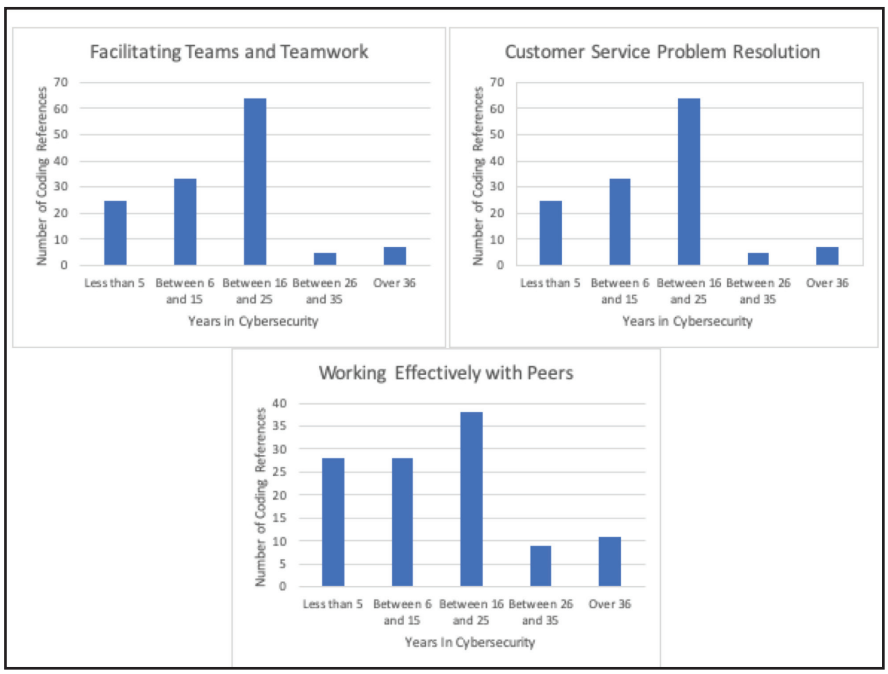
In contrast, more operationally focused participants looked for qualities that helped them integrate better into the cybersecurity team to enhance client problem resolution (see Figure 8). Despite the differences, all the participants had similar lists, but the disparity was the emphasis placed.

FIGURE 7: MORE SENIOR PARTICIPANTS CONCENTRATED ON THE CUSTOMER EXPERIENCE



Note. *Shows that participants in executive and similar senior positions emphasized those non-technical KSAs that enhance a customer/client's positive experience.*

FIGURE 8: MORE JUNIOR PARTICIPANTS EMPHASIZED COLLABORATIVE PROBLEM SOLVING



Note. *Shows that participants in manager and team leader positions emphasized those non-technical KSAs that enhance a customer/client's problem resolution through team collaboration.*

Not All Communication KSAs Are Equal Among Participants

As noted by most participants, not all cybersecurity jobs are the same, so the KSAs required for that work differ. An example is the way a worker communicates may vary dependent on role. As one executive shared, "we have a lot of people in cyber that people would say, are quiet, introverted, geeky, but everybody has to be able to communicate." That statement reinforces the reality that cybersecurity is rarely a solo effort, and workers must present information to the team as a minimum capability. As such, oral and written skills are keenly essential to work effectively in cybersecurity roles (see Figure 9).

One participant summed up how difficult but it vital it is to have strong communications skills by explaining that,

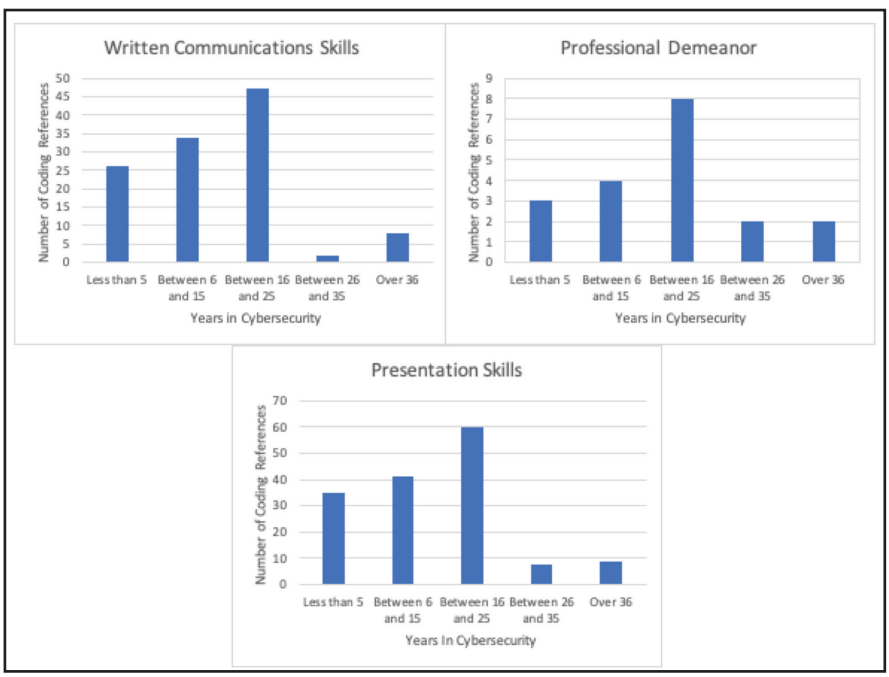
> *"they may be talking to other technical people that may interact with the businessperson during a one-off conversation. [However,} thinking and then really challenging that other technical person or going directly to the business to get the underlying reasons for these requests, these use cases, and not just purely turning on feature sets or turning on capabilities. Getting deeper in a way that taxes communication skills. I think we don't do justice, even in our hiring process, of identifying those communication skills. This is hard."*

Most participants combined critical thinking with the need for communication skills that keep the team and customer informed. Many spoke of the need for employees to present at the group rather than the customer level. Those under fifty spoke passionately about preserving the diversity of talent by making it acceptable to use various means to communicate with peers. Regardless, the participants uniformly expected any individual contributor to work effectively with peers using oral, written, or other data visualization tools.

One Role's Collaboration Is Not Like Another's

As noted in over 90% of the interviews, cybersecurity is part of everything in the increasingly connected world. One participant noted that *"as cybersecurity professionals, one of the hardest things that we have to deal with on a general basis is that cybersecurity is a part of everything. It's not like it is its own thing. You can't just do security without all of the people around you."* Yet, collaboration

Figure 9: Emphasis on Communications KSAs By All Participants



Note. *Age and position impact priority in the hierarchy of necessary non-technical KSAs.*

does not look the same for every cybersecurity role. Collaboration skills are not reserved for just in-person interactions. Cybersecurity workers must use these skills to resolve technical issues, provide security guidance, and address customer concerns in layman's language. This focus on the needs of others helps the team or organization develop positive customer relationships with clients.

More than 80% of the participants expressed the need for teaming. An executive likened cyber to a basketball team sharing that in cyber it is, *"the same type of communication and ability to clearly explain what you need as you're trying to move the ball down the field quickly."* More than half of the participants talked about the importance of working with peers and sharing knowledge. One manager was very clear that the way a cyber new hire can *"stand out is that they're able to improve the processes, improve the team, based on just being there because they came from and showed they think outside the box. When we take someone from outside of the organization and bring them in, you expect there to be change."* More than half of the participants spoke to how facilitating the team and team building ultimately resolved customer issues and fostered client relationships. While collaboration types can be diverse, the participants uniformly agreed that cybersecurity workers must get along with their team and support efforts to create positive relationships with customers.

Recommendations for the NICE Cybersecurity Workforce Framework

The pattern coding using the CAQDAS tool provided instructive inference clustering information that permitted searches for relationships to the NICE Cybersecurity Framework non-technical KSAs using Boolean search terms of AND and OR with semantic operators (Saldaña, 2016). This approach produced clustering around the KSAs, which the researcher inferred as participant emphasis of a particular knowledge, skill, or ability element. The resulting inferences from coding clusters constructs are useful for developing specific recommendations for non-technical KSAs that should be included in the NICE Cybersecurity Framework's next iteration.

The researcher presented the participants with the knowledge elements first. There was disagreement about what was most important at various stages of a cybersecurity professional's career, but the participants deemed all necessary. The knowledge of an organization and core mission areas was the area with the most remarkable clustering (see Table 6). However, knowledge of communications and computer tools were considered crucial and often referred to as *"a 'table stakes requirement to even get an interview."*

Table 6: KSA Reference Clustering Around NICE Non-Technical Knowledge Elements

NICE Cybersecurity Workforce Framework Element	KSA references
K0146: Knowledge of the organization's core business/mission processes	987
K0239: Knowledge of media production, communication, and dissemination techniques and method	382
K0246: Knowledge of relevant concepts, procedures, software, equipment, and technology applications	322
K0243: Knowledge of organizational training and education policies, processes, and procedures	266
K0287: Knowledge of an organization's information classification program and procedures for information compromise	155
K0245: Knowledge of principles and processes for conducting training and education needs assessment	108

Participants gave areas such as training less credence since the discussion focused on entry-level workers. However, many participants expressed the expectation that more senior cybersecurity professionals would teach peers and customers/clients. One experienced cybersecurity professional expressed it by sharing,

> *I would say junior people; I need them to execute their own individual training programs. But journeyman mastery level, yeah, they absolutely need to be involved in developing and executing technical training programs and passing on knowledge. I think that a cybersecurity organization can't thrive if experienced people are not passing on their skills. I think that will fail in the private sector and the public sector. There's too much information.*

There were several recommended additions to the knowledge area, but none clustered sufficiently to get included for consideration.

The skills areas clustered in ways that provided useful insight. The clustering around the criticality for cybersecurity workers to convey information effectively is noteworthy (see Table 7). Cybersecurity workers' ability to perform knowledge capture, sharing, and reuse activities took up considerable portions of the interviews. To

this point, one executive remarked that *"talking to others, giving information effectively, that cannot be emphasized enough."*

Table 7: KSA Reference Clustering Around NICE Non-Technical Skills Elements

NICE Cybersecurity Workforce Framework Element	KSA references
S0070: Skill in talking to others to convey information effectively	447
S0066: Skill in identifying gaps in technical capabilities	279
S0166: Skill in identifying gaps in technical delivery capabilities	232
S0296: Skill in utilizing feedback to improve processes, products, and services	168
S0064: Skill in developing and executing technical training programs and curricula	84
S0102: Skill in applying technical delivery capabilities	63

The clustering around the identification of gaps often brought in the need to convey information. The participants expressed the notion that once a cybersecurity worker identified a gap, they needed to quickly and effectively convey this information to their team.

Abilities were the final area discussed with the participants. As shown in Table 8, the professionals interviewed spent most of their time discussing problem-solving, critical thinking, and communications, which showed significant clustering.

Table 8: KSA Reference Clustering Around NICE Non-Technical Abilities Elements

NICE Cybersecurity Workforce Framework Element	KSA references
A0118: Ability to understand technology, management, and leadership issues related to organization processes and problem-solving	450
A0119: Ability to understand the basic concepts and issues related to cyber and its organizational impact	426
A0013: Ability to communicate complex information, concepts, or ideas	398
A0070: Ability to apply critical reading/thinking skills	273
A0106: Ability to think critically	240
A0105: Ability to tailor technical and planning information to a customer's level of understanding	186
A0018: Ability to prepare and present briefings	148
A0089: Ability to function in a collaborative environment	120
A0112: Ability to monitor advancements to ensure organizational adaptation and compliance	100
A0019: Ability to produce technical documentation	95
A0024: Ability to develop clear directions and instructional materials	38
A0063: Ability to operate different electronic communication systems	38
A0083: Ability to evaluate information	26

The participants considered areas that dealt with technical documentation that created clear directions as items for more senior cybersecurity workers. That area may have been skewed lower by the focus on more entry-level workers. However, the lack of clustering should not be interpreted as non-important areas.

VI. Implications

This study's most profound implication is that higher education and professional development training organizations that educate and train cybersecurity professionals should consider integrating non-technical KSAs into their programs. The participants unanimously agreed that cybersecurity workers need to grow non-technical knowledge, skills, and abilities. They diverge on which are most important and when, but there is universal agreement that cyber workers must think critically when they use the information for decision-making, hone communications skills that support the broader team, and collaborate to resolve customers' resolution problems. As such, it may not be necessary to have non-technical KSAs broken out for every role, but to have these KSA entities serve as core items that cybersecurity professionals should master over time.

The findings may inform a new centralized approach within the NICE Cybersecurity Framework. NICE could establish a standard set of non-technical KSAs for all cybersecurity professionals based on their professional journey timeline. In this way, curriculum developers would scaffold KSA entities based upon whether a cybersecurity professional was an apprentice, journeyman, or expert. In this way, there is a tiered approach to KSA mastery. The NICE Cybersecurity Framework authors can use the GTEDM's six significant areas of understand, assess, educate, measure, develop, and get feedback as a model for iterative progression of non-technical KSA mastery that would help continually improve the field (Assante & Tobey, 2011).

Expertise requires both factual and heuristic knowledge and the inclusion of the non-technical KSAs into the Cybersecurity Workforce Framework serves to provide the latter component, which is currently missing (Buchanan et al., 2018). Non-technical KSAs such as those represented in Tables 6 through 8 are the underpinning basis for good relationships, sound judgments, and

critical reasoning (Buchanan et al., 2018). A knowledge area would stay the same at the three levels of apprentice, journeyman, and expert with a scaffolded model, but the skills and abilities would be different. Cybersecurity certification and credentialing institutions may use these additional KSA for inclusion in their programs. At a minimum, it would provide a capability maturity model that is currently missing and could help education and training organizations assess what is lacking in their current graduates.

VII. Limitations

This research used a qualitative approach, but the trend data indicates that adding a quantitative component for future studies may yield greater fidelity to additions, deletions, and modifications to the current list of non-technical KSAs. The Boolean searches that yielded the quantity of coding references for each KSA were imperfect due to the semi-structured question format. If future research added a quantitative component, it might allow the investigator to narrow questions and develop instruments to analyze answers using statistics (Creswell & Poth, 2018). Qualitative interpretation requires a significant number of cross-checks, but researcher bias can still be problematic. However, this technique provides rich data that could help interpret the results from surveys and provide more significant insights. In turn, the addition of some type of quantitative inquiry could substantially reduce bias, whether perceived or real.

Another limitation was the number of KSAs offered for participant review. This study's semi-structured interview instrument did not have a comprehensive list of non-technical KSAs for participant consideration. The researcher derived the KSAs for the instrument used from the 2017 version of the NICE Cybersecurity Workforce Framework as a baseline. As such, the list produced is more of a starting point for inclusion in the next iteration of the NICE Cybersecurity Framework rather than a comprehensive document. These findings can provide directionality for future studies that can use other instruments to capture missing non-technical KSAs needed by apprentice, journeyman, and/or expert cybersecurity workers.

The final limitation to address is participant demographics. This study's participants are older, more educated, and in more senior roles than the field demographics. Future work endeavoring to create a more expansive non-technical KSA list may want to consider developing a participant sample that is more closely representative of the broader cybersecurity field. The field is at an inflection point where roughly one-third of its most junior workers started as cybersecurity professionals, but more than two-thirds are from feeder fields (Cyberseek, 2020). As the number of folks coming into cybersecurity from other fields shrink and the number of those who studied it from the beginning of their careers grows, the demand for a guild approach may further influence professional development. Data from this study will be triangulated with future work to reduce any bias introduced through skewed demographics.

VIII. Conclusion

Most cybersecurity staffs are functioning under great stress due to a lack of staffing. Industry, government, and academia share the responsibility to produce trained and ready cybersecurity talent for workforce demands. As such, a collaboration by all to create the next iteration of the NICE Cybersecurity Workforce Framework is paramount. Organizations will screen talent for their technical skills as a foundational expectation, but their hiring decisions will rest heavily on the candidates demonstrated soft skills and cultural fit (Litecky et al., 2004). This research-validated current understanding of this phenomenon. Every participant talked about how the integration of soft skills with a candidate's technical skills are essential skills that they look for in new hires. New cybersecurity professionals will need non-technical hard, soft, and mixed skills to progress in public, private, or non-profit organizations. Some of the most desirable traits include the precise use of information to make decisions, communications, and collaboration. These KSAs do not look the same for all roles but are critical components for employability and professional growth.

This research found that experts from the cybersecurity field deemed it imperative that its professionals possess non-technical skills that positively impact relationships with customers, peers, and effective decision-making. Participants diverged in the area of emphasis rather than the inclusion of any particular KSA. More senior participants focused on the customer experience with more references to training clients, critically using information for decision-making, and developing positive client relations. The more junior

participants spoke more about customer problem resolution, emphasizing teamwork, positive peer relationships, and problem resolution. From a holistic perspective, participants stressed that the most successful cybersecurity workers were intellectually curious people show could think critically, had different but effective ways to communicate with their organizational stakeholders, and collaborate effectively, albeit with other modalities and means depending on the role. More often than not, the discussion was how a worker approached problem-solving, communicating, or collaborating rather than the participant questioning the need to perform these critical KSAs.

Cybersecurity is a fast-paced field that is evolving quickly. There is much to learn, but it does not serve future workers to emphasize only the technical aspects of professional development. When one looks critically at cyber work roles, it is clear that these future professionals will need many non-technical skills to help them be advocates for cyber-related projects and remediation activities (Haney & Lutters, 2018). The inclusion of non-technical skills scaffolded over a cybersecurity worker's career may have a significant positive impact on their competence, confidence, and effectiveness over time.

References

Assante, M. J., and Tobey, D. (2011). Enhancing the cybersecurity workforce. *IT Professional 13*(1), 12-15, doi 10.1109/MITP.2011.6

Association of American Colleges and Universities (AACU). (n.d.). VALUE Rubrics. https://www.aacu.org/value-rubrics

Blair, J. R. S., Hall, A. O., and Sobiesk, E. (2019, March). Educating future multidisciplinary cybersecurity teams. *Computer 52*(3), 58-66, doi: 10.1109/MC.2018.2884190.

Bloomberg, L. & Volpe, M. (2016). *Completing your qualitative dissertation:* A road map from beginning to end. 3rd Edition. Thousand Oaks, CA: Sage Publications.

Buchanan, B. G., Davis, R., Smith, R. G., & Feigenbaum, E. A. (2018). Expert Systems: A perspective from Computer Science. In K. A. Ericsson, R.R. Hoffman, A. Kozbelt, and A.M. Williams (Eds.) *The Cambridge Handbook of Expertise and Expert Performance* (2nd ed., pp. 84-104). Cambridge University Press.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches*.

Crumpler, W., and Lewis, J. A. (2019) *The cybersecurity workforce gap.* Center for Strategic & International Studies (CSIS). https://www.csis.org/analysis/cybersecurity-workforce-gap

Cybersecurity and Infrastructure Security Agency Act of 2018. 115 PL 278 132 Stat. 4168, 2018 Enacted H. R. 11-454 (2018). https://www.congress.gov/bill/115th-congress/house-bill/3359

Cybersecurity and Infrastructure Security Agency (CISA). (2020, April 27). *Cybersecurity training and exercises.* National Initiative for Cybersecurity Careers and Studies (NICCS). https://www.cisa.gov/cybersecurity-training-exercises

Cyberseek. (2020). Cybersecurity career pathway [Interactive data set on July 7, 2020]. https://www.cyberseek.org/pathway.html

Cyberseek. (2020). Cybersecurity supply/demand heat map [Interactive data set on July 7, 2020]. https://www.cyberseek.org/heatmap.html

Dali'Alba, G. (2018). Reframing expertise and its development: A lifeworld perspective. In K. A. Ericsson, R.R. Hoffman, A. Kozbelt, and A.M. Williams (Eds.) *The Cambridge Handbook of Expertise and Expert Performance* (2nd ed., pp. 33-39). Cambridge University Press.

Deming, D. J. (2017). *The Growing Importance of Social Skills in the Labor Market*. The Quarterly Journal of Economics. 132 (4): 1593–1640.

Federal Bureau of Investigation (FBI). (2020, June 9). News. COVID-19 fraud: Law enforcement's response to those exploiting the pandemic. United States Department of Justice. https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic

Giuseppe Croce & Emanuela Ghignoni (2020) The evolution of wage gaps between STEM and non-STEM graduates in a technological following economy, Applied Economics, 52:23, 2427-2442, DOI: 10.1080/00036846.2019.1691142

Haney, J. M., & Lutters, W. G. (2018). It's scary … it's confusing … it's dull": How cybersecurity advocates overcome negative perceptions of security. Proceedings of the Fourteenth Symposium on Usable Privacy and Security, Baltimore: MD, August 12-14, 2018. USENIX Association. https://www.usenix.org/conference/soups2018/presentation/haney-perceptions

ISC(2) (2019) Cybersecurity workforce study: Strategies for building and growing strong cybersecurity teams https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study#

Jang, H. (2016). Identifying 21st Century STEM Competencies Using Workplace Data. *Journal of Science Education and Technology,* 25(2), 284-301. Retrieved June 29, 2020, from www.jstor.org/stable/43867797

Lapena, R. (2017, October 17). Survey says: *Soft skills highly valued by security team.* Tripwire, https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/

Lapena, R. (2020, February 10). *No relief for cybersecurity teams in sight, reveals Tripwire's latest skills gap report.* Tripwire, https://www.tripwire.com/state-of-security/featured/tripwires-skills-gap-report/

Lee, L. (2019). Cybercrime has evolved: It's time cyber security did too. *Computer Fraud and Security 2019*(6), 8-11. https://www.sciencedirect.com/science/article/pii/S1361372319300636

Litecky, C. R., Arnett, K. P., & Prabhakar, B. (2004). The paradox of soft skills versus technical skills in is hiring. *Journal of Computer Information Systems, 45*(1), 69-76. doi:10.1080/08874417.2004.11645818

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th Ed.). San Francisco, CA: Jossey-Bass.

Mitchell, G. W., Skinner, L. B., & White, B. J. (2010). Essential soft skills for success in the twenty-first century workforce as perceived by business educators. Delta Pi Epsilon Journal, 52(1), 43–53.

Moustakas, C. (1994) *Phenomenological research methods*. Thousand Oaks, CA: SAGE. 800-181. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-181

National Institute of Standards and Technology. (n.d.). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* Oversee and Govern. U.S. Department of Commerce. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework?category=Oversee-and-Govern

National Institute of Standards and Technology. (n.d.). *National Initiative for Cybersecurity Education (NICE)*, National Initiative for Cybersecurity Education (NICE) Working Group (NICEWG). U.S. Department of Commerce. https://www.nist.gov/itl/applied- cybersecurity/nice/about/working-group

National Research Council 2013. Professionalizing the nation's cybersecurity workforce?: Criteria for decision-making. Washington, DC: The National Academies Press.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication (S.P.) https://doi.org/10.17226/18446.

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (2018). Reassessment of expectations as a comparison standard in measuring service quality: Implications for further research. Journal of Marketing, 58(1), 111-124. doi:10.1177/002224299405800109

Petersen, R. (2019, November 12). *NICE! 10 years in the Making*. National Institute for Standards and Technology (NIST) [Blog]. https://www.nist.gov/blogs/cybersecurity-insights/nice-10-years-making#:~:text=While%20the%20inception%20of%20NICE,held%20until%20two%20years%20later.

Ravitch, S. M., & Riggan, M. (2017). *Reason & rigor: How conceptual frameworks guide research.* (2nd ed.). Thousand Oaks, CA: SAGE Publications.

Roberts, C. M. (2010). *The dissertation journey. A practical and comprehensive guide to planning, writing, and defending your dissertation* (2nd ed.). Thousand Oaks, CA: Corwin, A SAGE Publication.

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Thousand Oaks, CA: SAGE.

Sandwith, P. (1993). A hierarchy of management training requirements: The competency domain model. Public Personnel Management, 22(1), 43–62. https://doi.org/10.1177%2F009102609302200104

Sisson, L. G. & Adam, A. R. (2013). Essential hospitality management competencies: The importance of soft skills, journal of hospitality & tourism education, 25(3), 131-145, DOI:10.1080/10963758.2013.826975

Tobey, D. (2012). *Smart grid cybersecurity: Job performance model report*, NBISE technical report, SGC working group 12-01 Draft. National Board of Information Security Examiners.

U.S. Bureau of Labor Statistics (BLS). (2020, July 2). *News Release,* The employment situation – June 2020. U.S. Department of Commerce. https://www.bls.gov/news.release/pdf/empsit.pdf

U.S. Bureau of Labor Statistics (BLS). (2020, April 10). *Occupational Outlook Handbook*, Computer Support Specialists. United States Department of Labor. https://www.bls.gov/ooh/computer-and-information-technology/computer-support-specialists.htm

U.S. Bureau of Labor Statistics (BLS). (2020, April 10). *Occupational Outlook Handbook,* Customer Service Representative. United States Department of Labor. https://www.bls.gov/ooh/office-and-administrative-support/customer-service-representatives.htm#tab-2

U.S. Bureau of Labor Statistics (BLS). (2020, April 10). *Occupational Outlook Handbook*, Information security analysts. United States Department of Labor. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

U.S. Bureau of Labor Statistics (BLS). (2020, April 23, 2020). TED: *The Economics Daily*, Unemployment rates rose in 29 states and the District of Columbia in March 2020. U.S. Department of Labor. https://www.bls.gov/opub/ted/2020/unemployment-rates-rose-in-29-states-and-the-district-of-columbia-in-march-2020.htm#:~:text=Bureau%20of%20Labor%20Statistics,-The%20Economics%20Daily&text=Twenty%2Dnine%20states%20and%20the,to%204.4%20percent%20in%20March.

United States Continental Army Command (USCAC). (1968). Regulation 350-100-1, Training. Fort Monroe, VA. https://stacks.stanford.edu/file/druid:tv440px2527/tv440px2527.pdf

U.S. Secret Service (USSS). (2020, March 9). *Secret Service issues COVID-19 (COVID-19) phishing alert,* [Press Release]. U.S. Department of Treasury. https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_COVID-19_Phishing_Alert.pdf

Winegard, B., Winegard, B., and Geary, D. C. (2018). The evolution of expertise. In K. A. Ericsson, R.R. Hoffman, A. Kozbelt, and A.M. Williams (Eds.) *The Cambridge Handbook of Expertise and Expert Performance* (2nd ed., pp. 40-48). Cambridge University Press.

World Economic Forum. 2016. *The future of jobs, employment, skills and workforce strategy for the fourth industrial revolution.* Geneva. http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf

Yin, R. K. (2018). *Case study research and applications: Design and methods.* (6th ed.). Thousand Oaks, CA: SAGE Publications.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. & Basim, H. M. (2020): Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, DOI:10.1080/08874417.2020.1712269

Exploring Cognitive Processes to Develop Cybersecurity Defender Proficiency

David Schuster
San José State University, United States

***Abstract*—Problem Statement:** Despite the mission-critical role of people in protect and defend roles, relatively little is known about how cognition supports defender proficiency, a pressing problem given a workforce shortage and skills gap (Crumpler & Lewis, 2019). Understanding of the cognitive processes relevant to cybersecurity roles could support strategies to develop the skills of defenders and increase workforce participation. These processes, called macrocognition, are the result of cognitive resources at work in operational environments (Klein et al., 2003).

Research questions: The cognition of defenders is not well understood, and defender proficiency is only starting to be defined; what cognitive processes support proficiency in defender roles? To address the skills gap, a critical question is how to develop the proficiency of defenders efficiently; how can understanding of defender cognition be used to strengthen the cybersecurity workforce?

Contribution: A methodology using cognitive task analysis (CTA) is presented to describe the macrocognition of defenders. CTA is a collection of "tools and techniques for describing the knowledge and strategies required for task performance" (Schraagen et al., 2000, p. xiii). This work is complementary to prior defender CTAs in that CTA is used to describe the cognition of individuals with the aim of generalizing those processes across related work roles.

Rationale: This approach connects work roles based on related cognitive skills. Understanding of macrocognition could help defenders connect how they think with their work outcomes and may unlock novel, evidence-based strategies for workforce development, especially in training and recruitment.

Investigative Approach: Macrocognition's role in describing cognition at a useful layer of abstraction and complement to the NICE Framework (NIST SP 800-181; Newhouse et al., 2017) is introduced. CTA is discussed as a method of understanding proficiency in support of workforce development, and CTAs relevant to this perspective are reviewed. A use case with two industry defenders is presented, and lessons learned are offered to accelerate replication.

Lessons Learned The use case shows how concept mapping can lead to macrocognitive themes. The themes suggest practice implications and new research questions. Successes and failures in the use case are discussed so that researchers can more efficiently link CTAs to defender macrocognition.

Implications for Practice: The NICE Framework defines knowledge, skills, abilities, and tasks mapped to work roles with emerging discussion of qualifications; the methodology complements the NICE Framework by establishing the cognitive mechanisms that support individuals performing the skills and abilities. Macrocognition for cybersecurity may predict performance across similar roles even when policies, departments, organizations, sectors, and technologies change. There is potential value in diagnosing macrocognition to improve performance outcomes. This research can result in a more prepared cyber workforce, trained and recruited on the basis of cognitive skills relevant to their role.

Implications for Research: This work serves as a call and framework for additional CTA research to understand cognitive processes, and replication is necessary. Through the methodology, quantitative researchers can benefit from better understanding of relevant contextual factors, which can lead to more meaningful experimentation and establish reliable measurement.

Keywords—Macrocognition, Proficiency, Cyber Defense, Case Study

I. Introduction

Problem Statement

Defending against cyber threats is a large and growing problem for companies, with a 67% increase in breaches in the last five years (Bissell et al., 2019) and an expected annual cost of $6 trillion by 2021 (Morgan, 2019). It also provides challenging, mission-critical work for defenders, cybersecurity professionals who "identify, analyze, and mitigate threats to internal information technology systems and/or networks" (Newhouse et al., 2017, p. 11). Defenders can be defined as a category of cybersecurity professionals within the NICE Framework's Protect and Defend category (Newhouse et al., 2017); they include the work roles of analyst, defense infrastructure support specialist, incident responder, and vulnerability assessment analyst.

This work is challenging because of the asymmetry between attackers and defenders (Yurcik et al., 2003). Successful defense requires defenders to succeed in every instance, and a single failure can result in consequences to the business. This asymmetry is compounded by fact that organizational infrastructure can be large in scale and continuously changing as it supports the activity of the organization, resulting in a massive amount of data. Organizations are vulnerable to external attacks and insider threats. On their own or as part of a team, defenders must ensure that alerts are analyzed and understood, understand the severity of threats, and coordinate appropriate responses (Shah et al., 2018). They apply a great deal of knowledge to time-sensitive, high-stakes situations while juggling stakeholder requirements, available resources, and uncertainty (Rooney & Foley, 2018).

A cybersecurity workforce shortage underscores the critical need for people in effective cyber defense. In the United States alone, a shortage of over half a million workers existed in 2020, evidenced by the number of openings (NIST, 2020). Over 100,000 of these openings were for Protect and Defend roles (NIST, 2020). A contributing factor to the workforce shortage is a lack of available workers possessing the necessary skills for the job (Crumpler & Lewis, 2019). Solutions are needed to close the skills gap, including by developing the skills of defenders and increasing participation in the workforce.

NIST SP 800-181, known as the NICE Framework, provides a common language of Work Roles and knowledge, skills, and abilities (KSAs) that support cybersecurity roles (Newhouse et al., 2017). The NICE framework facilitates workforce development in several ways, including: (1) describing the elements of work common across organizations, sectors, and situations, defined as Work Roles and Tasks, and (2) describing what defenders know and do, defined through KSAs. In doing this, the NICE Framework also facilitates understanding of cognition by describing what cybersecurity professionals know (as knowledge) and do (as skills and abilities) for a given situation (as Work Roles and Tasks).

Despite the critical role of people in Protect and Defend roles, relatively little is known about the cognitive processes, the ways of thinking, that enable cyber defenders to perform their work. This problem is a knowledge gap between what highly proficient defenders do and how they are able to do it. A lack of understanding of cognition limits the ability to leverage human capabilities in cybersecurity work.

Research Questions and Contribution

This article addresses two research questions: (1) what cognitive processes support proficiency in defender roles? And, (2) how can understanding of defender cognition be used to complement the NICE Framework and develop the workforce? A research methodology, focused on the cognitive processes of individual defenders, is proposed to address these two questions.

Cognitive processes in cyber defense can be understood at a macrocognitive level, the result of cognitive resources at work in operational environments (Klein et al., 2003). Macrocognitive models have been used in other complex, high stakes environments, including transportation and healthcare to improve practice by describing how cognition supports performance (Klein & Wright, 2016). Cognitive task analysis (CTA) is a collection of qualitative research methods to develop and apply macrocognitive models to improve practice (Klein & Wright, 2016). The foundation of the research methodology presented in this article is the use of CTA to explain defender cognition. The methodology complements existing CTAs in that it uses CTA to describe the how cognitive processes of individuals support cyber defense with the aim of

generalizing those processes to related tasks across situations and organizations.

Rationale

As the NICE Framework (Newhouse et al., 2017) provides a common language to further professionalize cybersecurity careers, so too could a better understanding of cognition further professionalize cybersecurity careers by connecting cognitive processes across situations, Tasks, and Work Roles. Identification of cognitive processes that apply to cybersecurity Work Roles addresses the gap between cognition and performance. It can describe the ways of thinking that predict success in identification, analysis, and mitigation of threats. This knowledge can be used for workforce development, specifically, in recruitment and proficiency development, through training. Recruitment and selection, and employee development and retention, are two of four components of the human capital management lifecycle, and they complement workforce planning and succession planning in the draft NISTIR 8193, the NICE Framework Work Role Capability Indicators (Stein et al., 2017).

As a recruitment outcome, potential cybersecurity professionals might be recruited on the basis of cognitive skills, which could be used to increase the diversity of people participating in the profession. That is, interests in other domains that utilize similar cognitive skills might suggest talent and interest in cybersecurity careers. This strategy is already being used informally. For example, the career website DICE lists "grasping the big picture" as one of six skills needed to succeed in cybersecurity ("Six skills," n.d.). Research on defender cognition could provide further specificity and empirical evidence for these claims. It could also accelerate training, such that training of known cognitive skills readies people for a cluster of cybersecurity Work Roles, in complement to other training strategies. Training involves a process of learners acquiring KSAs; this can be done more efficiently and effectively with understanding of how such knowledge and skills are used in the field. Together, the cybersecurity workforce could be further developed through increased career participation and novel, evidence-based training strategies.

Investigative Approach

The purpose of this article is to provide a framework for researchers and practitioners to help them leverage understanding of cognition for workforce development. In the background section that follows, macrocognition's role in describing cognition at a useful layer of abstraction and complement to the NICE Framework is introduced. CTA is discussed as a method of understanding proficiency to suggest interventions for workforce development, and CTAs relevant to this perspective are reviewed. Following this, a use case with two industry defenders is presented as an example of how CTA could be used to describe macrocognition. Immediate, albeit limited, practice implications of the use case are presented. As a use case, more value comes from lessons learned; increased participation in research on the human aspects of cybersecurity is necessary for the successful application of the methodology, and the lessons learned can accelerate implementation of the methodology. The article concludes with a discussion of the research and practice implications of the methodology on workforce development.

II. Background

The NICE Framework and Cognition

The NICE Framework was developed through an iterative process of participation from industry, government, and academic stakeholders with opportunities for public input (Newhouse et al., 2017). One outcome has been the definition of KSAs and Tasks mapped to Work Roles. KSAs help explain defender cognition by enumerating what defenders know and what they are able to do. The acquisition of knowledge and skill in a domain supporting high levels of performance are components of high proficiency, also called expertise (Feltovich, 2018).

Understanding of defender cognition can be used to augment the NICE Framework by explaining how proficiency develops and is used in operational settings. Knowledge in the NICE Framework is defined as, "a body of information applied directly to the performance of a function" (Newhouse et al., 2017, p. 5). Knowledge elements, for example as "Knowledge of encryption algorithms" (p. 59) refer almost exclusively to declarative knowledge or to the use of technologies (e.g., "Knowledge of virtualization products (VMware, Virtual PC)," p. 76). Skills are distinguished by being observable, defined as "observable competence to perform a learned psychomotor act." For example, "Skill in

using knowledge management technologies" could, with further specification, be demonstrated. Abilities are similarly defined as observable behaviors, albeit behaviors that result in an observable product. At present, a draft revision to the NICE Framework refactors Skill and Ability statements into Skill statements, defined by observability (Petersen et al., 2020). Knowledge and Skills describe capabilities of the defender; Tasks describe the work. Given this, Skills and Abilities will be considered together and distinctively from Knowledge. Given its prevalence in the literature, the abbreviation KSA will be used to refer to the collective of Knowledge and Skills/abilities.

What is not provided by KSAs is understanding of how defenders are able to perform or demonstrate the KSAs. Understanding the cognition used by defenders in performance of their work would help the field understand how their proficiency develops. This requires an understanding of how interactions of NICE Framework Task requirements (Newhouse et al., 2017), defenders' thought and behavior, and the organizational and world context affect outcomes. One challenge to understanding cognition is that it is not directly observable; it occurs within an individual. This may be why Woods and Roth (1988) observed that the development of a technology generally outpaces our understanding of how to best use the technology.

Proficiency in Cyber Defense

Research on expertise across domains suggests that proficiency may be identified by differences in the process of thinking and reasoning (Feltovich et al., 2018). Proficiency goes beyond holding a greater amount of knowledge in a domain; it is also evident by thinking in different ways. Decades of expertise research have shown that, generally, highly proficient individuals can process larger and more integrated cognitive units, have deeper and more functional representations of tasks, are better able to apply their knowledge to problems, are more able to engage in self-monitoring, and can better recognize patterns in problem solving (Feltovich et al., 2018). To address the skills gap, a critical question is how to develop the proficiency of defenders efficiently.

The thinking of proficient defenders is not well understood, and defender proficiency is only starting to be defined. Agyepong et al. (2020) conducted a systematic literature review to identify challenges to the use of metrics in security operations centers. They found a combination of metrics that are objective and easily captured but limited, such as number of alerts analyzed, and the number of tickets closed per day. These contrast with metrics that are more comprehensive but subjective, and difficult to capture, such as the quality of analysis and quality of incident reports. They concluded that, "An understanding of how analysts addressing the difficult aspects of their work can be used will provide insights into their performance" (Agyepong et al., 2020, p. 14).

The NICE Framework Workforce Indicators describe proficiency at three levels: entry, intermediate, and advanced. These levels are distinguished by the level of knowledge, the ability to perform successfully under limited guidance, the ability to serve as a resource for others, and the ability to perform successfully "in complex, unstructured situations" (Stein et al., 2017, p. 302). These levels map to proficiency categories Hoffman et al. (2014) adapted from craft guild terminology. The entry level of Stein et al. (2017) corresponds to the apprentice, a student who is working within the domain (Hoffman et al., 2014). The intermediate level of Stein et al. (2017) is referred to as journeyman by Hoffman et al. (2014), a person who can perform a day's work without supervision. The advanced level of Stein et al. (2017) corresponds to the expert level of Hoffman et al. (2014), distinguished with high regard from peers, the highest levels of task performance, and the ability to respond to rare or complex situations. This comparison usefully extends the NICE Framework Workforce Indicators (Stein et al., 2017) because Hoffman et al.'s (2014) characterization includes two additional levels of interest. The naïve individual is ignorant of the domain. This is the target population for interventions that bring new people into the domain. As a population, getting individuals to advance from naïve to higher levels means increasing participation in the domain. On the other end is the master level, distinguished by qualifications to teach. While there exist cybersecurity practitioners at all of these levels, the field currently has limited understanding of how to label and develop proficiency.

In several cases, general models of proficiency have been applied to cyber defense with limited success. One missing element is the understanding of cognition in context, specific to cyber defense. Ben-Asher and Gonzalez (2015) developed a surveyg

to classify participants as cyber defense experts or novices based on domain knowledge and self-reported experience. Their novice category included individuals with no cybersecurity experience and more closely aligns with the naïve category. They observed differences in the dichotomized groups but relatively small differences in the ability of the two groups to detect attacks in a simulated task. The authors concluded that pulling professionals from their operational environment to participate in the study may have resulted in fewer cues available to them, suggesting that defenders leverage cues from the operational environment that are not easily captured in simulation-based experiments (Ben-Asher & Gonzalez, 2015).

Saner et al. (2016) aimed to identify naïve individuals who may excel in cybersecurity careers based on relevant cognitive skills. They used an approach of inferring cognition from NICE Framework KSAs and then placing them in a framework with two dimensions. The first dimension was the difference between initiating (e.g., attacking) and responding (e.g., defending). The second dimension was the difference between real-time roles requiring action under time pressure and exhaustive roles allowing for greater planning and deliberation. This characterization provides a link between tasks and cognitive demands required to perform them. However, they struggled with the linkage from KSAs to cognition, noting that too few details about the steps involved in the operations were available in KSAs to make inferences about cognition. Together, these studies have established a need to better understand cognition of proficient defenders and suggest an approach that incorporates the complexity inherent in the work. Towards developing understanding of this context, Goodall et al. (2009) conducted a field study and found evidence of two aspects of defender proficiency: technical knowledge of the domain and knowledge of the specific network environment involved, which they called situated expertise. While efforts are emerging to label, measure, and understand defender proficiency, better understanding of human cognitive performance in defender Work Roles is needed.

Macrocognition: Managing Complexity

Rasmussen et al. (1990) recognized the issue of levels of abstraction in describing complex work. Different levels of abstraction provide different perspectives on the work. Models at a low level of abstraction are closely linked to specific circumstances in the physical world. Models at higher levels of abstraction are closely linked to a specific purpose. Rasmussen et al. (1990) suggested that a work function can be seen as a goal for a lower level of abstraction and an explanation for how higher levels of abstraction are realized. The levels of abstraction, as summarized by Crandall et al. (2006), were goals, measures of the goals, general functions and activities, specific functions and activities, and workspace configuration. The work of defenders can be understood at each of these levels, from overall goals at the top, to physical processes at the bottom. Defending the organization is a high-level goal, supported by measures of the goals and general functions. The use of a tool, as a specific activity, explains how a general function is realized. Thus, understanding a task involves mapping lower level operations to higher level goals.

By analogy, cognition can be understood at various levels of abstraction. Individual cognition can be understood at micro (low) and macro (high) levels of abstraction. At the micro level, of interest to cognitive psychologists, cognition is partitioned into resources, such as attention, perception, and memory, so that their function can be understood. A common assumption in cognitive psychology research is that cognitive resources can be understood independent from their cultural and societal context (Braisby & Gellatly, 2005). The benefit of this approach is that it can identify laws, which apply universally; however, because it is separated from a specific purpose, it leaves unanswered questions about how cognition supports goals and tasks.

The macro level, called macrocognition, is the result of cognitive resources at work in operational environments, stepping towards a specific purpose, incorporating context, and emphasizing a descriptive approach over normative models. Macrocognition is a set of cognitive functions that support human performance. Microcognition includes the mental operations that explain macrocognition. Klein et al. (2003) identified six macrocognitive functions (see Table 1) in support of six macrocognitive processes (see Table 2. In their model, goals drive the use of macrocognitive functions. Macrocognitive processes are employed to support the macrocognitive functions. Importantly, macrocognition does not attempt to describe physiological circumstances or operations. There is no physical mental model,

for example. Instead, mental models reflect an application of cognitive operations towards a specific purpose. This is why macrocognitive constructs are defined by the outcomes they support; mental models are mechanisms to "generate descriptions of system purpose and form, explanations of system functioning and observed system states, and predictions of future states" (Rouse & Morris, 1986, p. 351).

Situation awareness (SA) is another macrocognitive construct frequently of interest in research on defender cognition (for a review, see Gutzwiller, 2019). In simple terms, it is the outcome of the process of sensemaking (see Table 1), which is also called situation assessment. Situation awareness is most frequently defined according to Endsley's (1988) model, involving perception of relevant elements in the situation, comprehension of the elements in the situation, and projection of the future status of elements. The relevance of elements in the specific situation is what distinguishes macrocognitive SA from microcognitive perception. The content of SA is defined by the goal and situational context. Because of this, the SA of an airline pilot cannot be meaningfully compared to the SA of a defender. Separated from a situational context, SA has no meaning. This also requires measurement of SA to be goal specific. This challenge may be one of the causes for dilution of this term in the literature. As Gutzwiller et al. (2016) noted, authors have increasingly been using situation awareness as a term to define the result of data fusion rather than a macrocognitive process. They suggest cyber-cognitive situation awareness (CCSA) to describe defender SA according to Endsley's (1988) model. Although this term is not yet widespread in the literature, using CCSA instead of SA identifies it as a construct of human macrocognition.

Table 1: Macrocognitive functions identified by Klein et al. (2003) with definitions quoted and adapted from Crandall et al. (2006

Function	Definition
Problem detection	Spotting "potential problems at an early stage" (p. 139)
Coordination	"The way team members orchestrate the sequencing of their actions to perform a task" (p. 139)
Adaptation	"Modifying, adjusting, or replacing a plan that has already been implemented" (p. 138)
Planning	"Modifying action to transform a current state into a desired future state" (p. 138)
Sensemaking / situation assessment	Diagnosing "how the current state of affairs came about" (p. 138)
Naturalistic decision making	Relying "on experience to identify a plausible course of action" (p. 137)

Table 2: Macrocognitive processes identified by Klein et al. (2003) with definitions quoted and adapted from Crandall et al. (2006)

Function	Definition
Managing attention	Using "perceptual filters to determine the information a person will seek and notice" (p. 142)
Identifying leverage points	"Identify opportunities and turn them into courses of action" (p. 141)
Managing uncertainty and risk	Developing "skills for coping with uncertainty" (p. 141)
Mental simulation and story building	"Enacting a series of events and pondering them as they lead to possible futures" (p. 141)
Developing mental models	"How sense is made of situations" (p. 140) involving "mental imagery and event comprehension" (p. 140)
Maintaining common ground	"The continuous maintenance and repair of calibrated understanding amongst members of a team" (p.140)

Macrocognition connects cognition to tasks and goals. But because macrocognitive processes and functions are specific to context, they need to be specified for cyber defenders. The last needed piece is a method to understand macrocognition applied to tasks. As a collection of applied, qualitative research methods, CTA provides this piece.

Cognitive Task Analysis (CTA)

CTA is a collection of "tools and techniques for describing the knowledge and strategies required for task performance" (Schraagen et al., 2000, p. xiii). Klein and Militello (2001) explained CTA in terms of its description of cognition, focus on tasks in natural settings, and attempt to explain the cognitive processes observed. CTA involves three main components: knowledge elicitation, data analysis, and knowledge representation (Crandall et al., 2006). Knowledge elicitation involves data collection with practitioners in the domain. Data analysis is the process by which the researcher synthesizes data and discovers meaning. Knowledge representation summarizes the meaning uncovered in data analysis.

Many CTAs have been conducted with defenders, though relatively few of the CTAs have provided data on individual defender macrocognition in organizations outside of government and defense. In the methodology, past CTAs inform future CTAs and suggest research questions for quantitative research. Integrating CTAs can be challenging. Because they are not testing theory, each provides its own insights and a complementary glimpse into the cognitive work of defenders. There are also a wide variety of techniques available (for a review, see Wei & Salvendy, 2004).

Categorizing CTAs based on their knowledge representation can be useful. Some CTAs have resulted in knowledge representations that are workflow-oriented (e.g., Erbacher et al., 2010). The CTAs that are most aligned to the methodology resulted in a list of goals and subgoals of defenders and/or reflect decision making through the questions asked by defenders (e.g., Buchanan et al., 2016). It should be noted that, although outside the scope of this review, work has been done to understand processes at the team-level (e.g., Cooke et al., 2013; Nyre Yu, 2019; Tetrick et al., 2016).

Erbacher et al.'s CTA (2010) resulted in a workflow representation. They conducted a seven-phase CTA for the purpose of developing visualization techniques. Participants included network analysts, network managers, and security researchers at Pacific Northwest National Laboratory. This work resulted in a task-flow diagram in four stages: assessment, detailed analysis/cleanup, response, and audit. The model is circular, reflecting an iterative process of re-assessment. It features a big picture construct at the center, supporting all steps and being affected by cleanup. The big picture includes a variety of constructs, including world view, known players, cyber-attacks, host information, and coordination.

Trent et al. (2019) used CTA to describe the workflow of US military cyber protection teams. As with Erbacher et al. (2010), this CTA emphasized the high-level process of the work. It was also idealized in that some steps are skipped in practice. One theme of the model is that the work does not necessarily proceed in sequence. Rather, the work, "needs to be described in terms of parallel tasks and feedback loops, not as a series of steps or stages" (Trent et al., 2019, p. 129). The role of periodic communication with intelligence sources was also highlighted.

Narrowing to CTAs that help explain the cognition of individual defenders provides a more succinct list. Many CTAs aimed to describe the content of CCSA for defender tasks. Utilizing a number of methods, including an extended period of observation, Paul and Whitley (2013) investigated how analysts establish and maintain awareness of large computer networks. They suggested two components: event detection and event orientation. In a review of such studies through 2015, Gutzwiller (2019, p. 41) noted that CCSA needed to be defined for particular roles, measurement was still needed, there was limited understanding of the linkage between defender CCSA and performance, and there was a need for research to understand other macrocognitive functions and processes.

Some CTAs focused on defining the categories of defender CCSA. In an early example, Biros and Eppich (2001) suggested categories of recognition of nonlocal Internet protocol (IP) addresses, identification of source IP addresses, development of a mental image of normalcy, creation and maintenance of analyst situational awareness, and facilitation of knowledge sharing. D'Amico et al. (2005) described detection, situation assessment, and threat assessment being developed in a largely

linear process of building understanding. D'Amico and Whitley (2007) developed a three-stage process model mapped onto Endsley (1988); CCSA was represented as a hierarchy of raw data being filtered to leave what is interesting, then what is suspicious, then events, then incidents, and finally intrusion sets, which are groups of related incidents (D'Amico & Whitley, 2007).

D'Amico et al. (2005) represented questions asked by defenders, the first example of an approach used by others. They also suggested site-specific knowledge as a challenge to proficiency development; defenders must know what is normal for their environment, a theme that emerged in other sources, such as Goodall et al.'s (2009) situated expertise. Mahoney et al. (2010) created six preconstructed scenarios, which they discussed with a single subject-matter expert. The result of the CTA was a list of nine preliminary categories of CCSA. Buchanan et al. (2016) conducted a goal-directed CTA to elicit the subgoals and decisions, also phrased as questions, under two high level goals: detecting threatening incidents and characterizing those incidents. Describing the content of CCSA as lists of questions can be understood as an answer to the question, *what should a defender attend to?* This level of abstraction can reveal cognitive process (i.e., how CCSA works for defenders) and offers implications for practice.

The approach of Zhong et al. (2015) represented defender behavior at a lower level of abstraction. They used automation to capture defender behavior in combination with participant self-reporting, which suggested 11 operations: browse, filter, search, inquire, select, selected, link, new hypothesis, modify hypothesis, switch context to a different hypothesis, and confirm or deny a hypothesis. These operations could suggest building block operations of decision making but are less connected to goals; additional context is needed to connect the behaviors to goals.

Gutzwiller et al. (2016) conducted a CTA with six participants in three phases. They combined a semi-structured interview, a knowledge audit, and a concept mapping activity. Gutzwiller et al. provided a three-component model of CCSA: understanding and awareness of the network, the team, and the world. The network includes elements of network architecture and behavior, which map onto elements of Mahoney et al.'s (2010) CTA. The world component includes awareness of novel threats and abnormal behavior (Gutzwiller et al., 2016). Finally, the team component represents awareness of team members to facilitate coordination and support. This model differs from others in that it gives more prominence to contextual factors.

This section has described how CTA has been used to better understand the work of defenders. CTAs in this area have contributed to understanding how cognition supports this challenging work. Despite this, more research is needed to describe how macrocognition of individual defenders in industry works to affect security outcomes. A methodology to achieve this aim is described next, followed by a case study to illustrate how the methodology can be applied to the work of defenders.

III. Research Methodology

Figure 1: Research Methodology

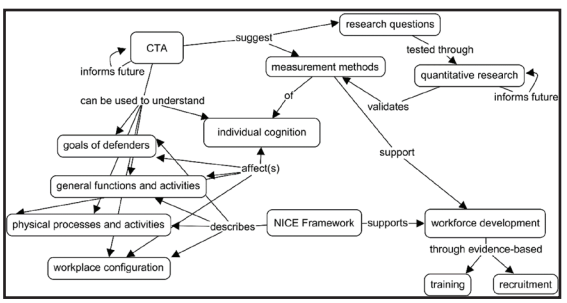


Figure 1 depicts the research methodology using CTAs to understand the cognition of individual defenders. While no single link in the methodology is novel, the methodology augments current research methods by suggesting mutual support between CTA and quantitative research. In the next section, a use case illustrates how the methodology can be applied to understand defender cognition.

IV. Method

Participants

Two participants were cybersecurity professionals at technology companies in the San Francisco Bay area. Organizations with defenders were invited to participate in the research through convenience sampling. Organizations were discovered through professional networks and by attending cybersecurity-related conferences. CISOs and managers were contacted by e-mail to discuss the study. Upon organizational agreement

to participate and IRB approval, organizations were invited to announce the study to employees, who participated voluntarily as part of their workday.

Defenders were defined broadly as professionals who monitor networks and/or respond to network threats on a daily basis. While defenders were the focus of the investigation, the inclusion criteria were broadened to any employee in an operational cybersecurity role to encourage participation of cybersecurity professionals regardless of their job title.

Of the 19 individuals who participated, two met our definition of a defender, resulting in a sample size of N = 2 from two different companies. One company was a large networking technology company. Participant 1's company employed between 50,000 and 100,000 individuals at the time of the interview. Participant 2's company provided cloud services and had between 100 and 500 employees. One interview was conducted in early 2018; the other was conducted in early 2019.

Materials

Participation involved two activities, a survey and a concept mapping interview. Both of these activities were exploratory, with the goal of identifying themes appropriate for future investigation. The purpose of the survey was to describe the expertise of the participants and qualify them for inclusion in the study. The purpose of the concept mapping interview was to elicit the knowledge of participants and represent it visually.

Exploratory Survey - A survey was used to qualify cybersecurity professionals as defenders and document their experience. Participants were sent a link to complete the survey using Qualtrics. The survey items were adapted from a survey used with an earlier sample (Schuster & Wu, 2018). As part of the survey, participants were asked their gender, age, job title, years they have been in their current role, and total number of years of experience working in cybersecurity. The survey then asked whether they respond to network threats on a regular basis, the highest level of education obtained, the name of degrees obtained, and certifications held.

Concept Mapping Interview - An individual concept mapping interview was conducted with each participant lasting approximately 60 minutes. The concept mapping protocol was adapted from Crandall et al. (2006). The interview was conducted over teleconference using audio and screen sharing but without video. IHMC Cmap Tools Knowledge Modeling Kit (version 6) was used to create the concept maps, and this software was made visible to the participant during concept mapping using screen sharing.

Members of the research team included the author and student research assistants. Training for the research team involved study of Crandall et al. (2006), review of the research protocol, and participation in mock data collection sessions with other members of the team. Data collection required three researchers. The facilitator led the interview and was the only member of the research team in regular communication with the participant. Meanwhile, a second researcher operated the concept map software, and a third researcher took notes. Participants did not manipulate the concept map software directly. To facilitate the mapping, the concept mapper could interject to slow or repeat parts of the interview. The notetaker took notes without interacting with the participant.

After an introduction of the members of the research team, the informed consent notice was displayed and discussed with the participant. Next, the concept map activity was introduced with an example using driving as a domain. This tutorial introduced concepts, linking words, and propositions. Concepts are the major concepts in the domain. Concepts are connected to other concepts by linking words. Together, two concepts form a complete sentence with a linking word, called a proposition. Propositions are directional and are read in the direction of the arrow. Participants were provided an overview of the process of generating the concept map and given a suggested list of linking words suggested by Crandall et al. (2006, p. 60).

Following the introduction and tutorial, participants were presented with a focus question designed to anchor the concept map. The guiding priority was to represent the participants' individual perspective of their work, not the work of their company as a whole or the basics of the field. Therefore, the map was anchored with a focus question of "What do you need to be aware of when monitoring for and/or responding to threats?" This question proved insufficient when the sample started to include non-defenders. Thus, the approach

was modified to instead co-create a focus question tailored to the participant's job title. The focus question was structured in the format, "What do you need to be aware of when…," with a job description following. The default question was "What do you need to be aware of when creating secure network systems?" Participants were then asked to confirm that the question applied to their daily work. In both interviews, participants chose to revise the question. The focus question was collaboratively revised to, "What do you need to be aware of when responding to cyber security incidents?" for Participant 1 and, "What do you need to be aware of when supporting network security systems?" for Participant 2.

The revised focus question was entered as the highest-level concept in the map. From here, the concept map was constructed in four general steps. The first step was initial concept generation, in which participants were asked to list the most relevant concepts that came to mind after reading the focus question. Participants were asked to, "identify the most relevant concepts that you think of when you read the focus question" and that "it is important to know that these concepts are not final, and you can choose to add, remove, or change any concept at any moment. We will write them down as you say them aloud." The second step was to organize the terms of the map. Participants were asked to suggest the most general or important concepts, which were then moved toward the top of the screen. The goal of this step was to organize concepts so that they were descending from more general to more specific at the bottom. The third step was to link concepts, starting with one relationship. Participants generated propositions by forming a complete sentence from one concept to another, with the linking words in the middle. The fourth step was the refine the map. In this step, the facilitator navigated the map, reading and confirming propositions aloud. Before concluding, participants confirmed that they were satisfied with the map representation.

Results

Survey Responses - Participant 1 held the title of InfoSec Tier 2 analyst, worked in incident response, and had been in the role for five years. Participant 1 reported eight years of experience in cybersecurity. This participant held security-related bachelors and master's degrees. Participant 2 held the job title of security analyst, supported a web application firewall, and had been in that role for a single year. This participant reported three total years of experience in network security. Participant 2 participant held a non-security bachelor's degree. In terms of the NICE Framework, Participant 1's work mapped to the cyber defense incident responder role, while Participant 2's work mapped to the cyber defense infrastructure support specialist. Participants held two or three certifications each with no overlap.

In all, the two participants differed in the duration of their work experience and job title. Participant 1 had more experience in the current role and the field while working for a much larger organization. The participant from Company 2 had less experience in the current role and the field while working at a smaller organization.

Concept Map Analysis - The purpose of the concept map analysis was to identify elements of macrocognition in the work of defenders. This was done by analyzing map structure and content and identifying macrocognitive themes.

Map Structure and Content. Following the interview, concepts on the maps were adjusted so that all propositions were visible and directionality clear. Concepts that were listed by the participant but not used in the map were removed. Participant concept maps are shown in Figure 2 and Figure 3. As a first step, the maps were examined to see if they differed in the quantity of concepts and propositions. Concept frequency was assessed by listing concepts used in each proposition. If a concept was connected to more than one other concept, it was counted each time it appeared in a proposition. For example, "asset targets include cloud asset" and "asset targets include user asset" were counted separately.

The two maps were different in their complexity. Comparing across the two maps, Participant 1 generated a greater number of concepts (45) and propositions (46) than Participant 2 (23 and 36, respectively) but fewer links per proposition. The following concepts were common to both maps: Logs (as logs or web logs), assets (as high value assets, user asset, cloud asset, ownership of the asset, asset targets, host asset, or data asset), and monitoring (as monitoring or established monitoring plan deployed within your infrastructure).

Figure 2: Concept Map for Participant1

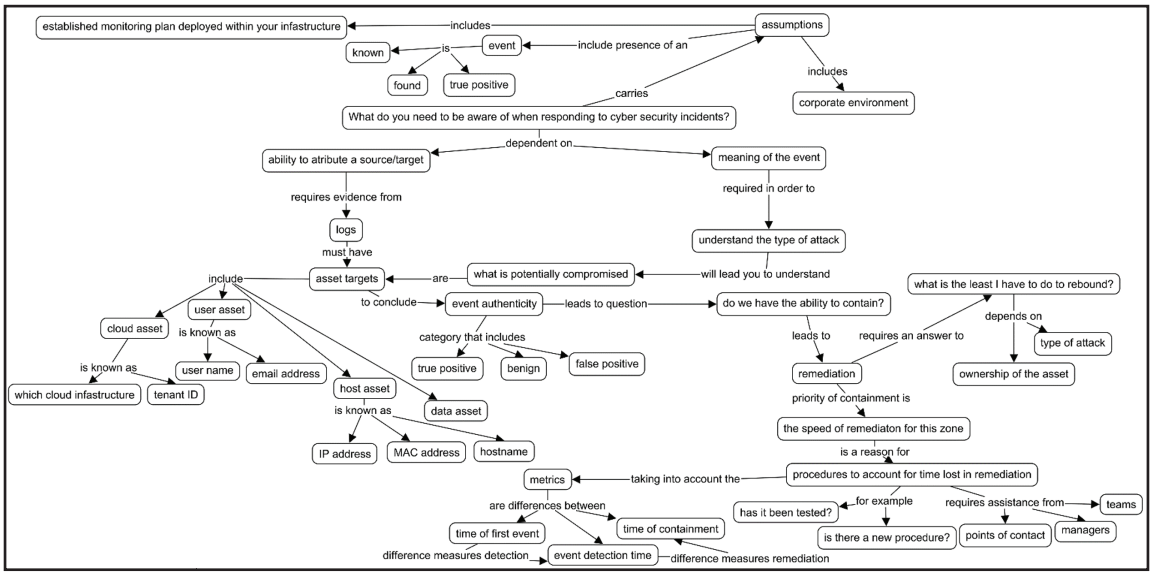
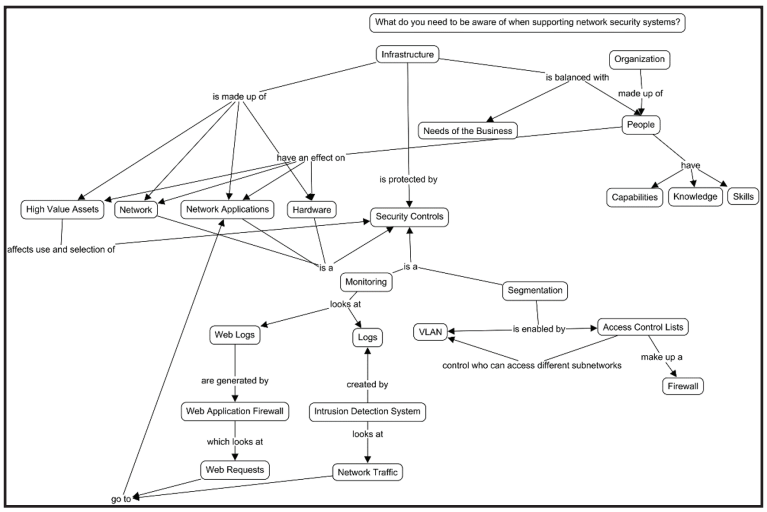


Figure 3: Concept Map for Participant 2



Participant 1's map was organized around the attribution of source and target and the meaning of the event. For Participant 1, assets were considered in the context of the attack, and four asset types were specified (cloud, user, host, and data) and associated with logs (as the target of the log). For Participant 2, the major elements were the infrastructure and the organization. Security controls, which include monitoring and segmentation, protect the infrastructure. For Participant 2, assets were part of infrastructure, although they are at the same level as the network, network applications, and hardware. By including it as a separate concept, the map suggests asset value is a relevant factor.

Evidence of Macrocognition - The concept maps were examined to identify macrocognitive themes. Using the definitions described in Table 1, two members of the research team independently identified potential macrocognitive elements in each concept map. The two lists were aggregated, and propositions using these concepts were examined. This process revealed themes for each participant. Table 3 lists collective themes of macrocognition created by aggregating the participant-level themes. Additionally, practice and research implications are suggested for each theme.

Figure 3: Macrocognitive Themes and Implications

Theme	Implications
1. Defenders maintain mental models of assets: the elements of the infrastructure (such as targets, zones, and events) and their business context.	**Practice implication**: Defenders need to develop an understanding of relevant infrastructure. Defenders may benefit from awareness of other organizational perspectives so that they can best incorporate business context into their understanding and decisions. **Research questions**: How do defenders' representations of elements of the infrastructure relate to the reality of these resources? How do defenders' representations of elements of the infrastructure evolve over time? How do organizational goals and culture affect mental models of assets?
2. Selecting information from asset targets is an example of managing attention.	**Practice implications**: As defenders develop proficiency, they may be identified by their ability to manage attention; in support of CCSA, proficient defenders understand where to find needed information. **Research questions**: How do defenders learn and know where to find needed information?
3. Technology contributes to sensemaking by filtering and providing perceptual cues.	**Practice implications**: Technology affects sensemaking in the quality and relevance of cues provided. Defender proficiency may be identified by the ability to put relevant cues together to develop meaning. **Research question**: How do defenders adapt to the limitations of imperfect cues?
4. Sensemaking is a prerequisite for remediation but continues during remediation. Sensemaking in remediation pulls in organizational, infrastructural, and situational factors.	**Practice implications**: Defenders need to be able to draw connections between the organization, infrastructure, and situation. They must understand how the situation relates to the organizations' goals. **Research questions**: How does sensemaking before remediation relate to, and differ from, sensemaking during remediation? At boundaries between tasks, how does macrocognition change?
5. Event detection is an example of spotting anomalies.	**Practice implications**: Defenders could learn the critical cues experts use to spot anomalies. Defenders' use of critical cues may suggest strategies for detection of novel events. **Research questions**: What are the critical cues that hint at anomalies? How are previously unknown anomalies detected by defenders?
6. Planning occurs throughout the remediation process. Adaptation occurs during remediation when implementing procedures to account for time lost in remediation.	**Practice implications**: Defenders mental models help them adapt to the needs of the situation. Adaptation requires understanding of what the situation means for the organization. **Research questions**: Where is adaptation situated? How are handoffs managed? How do defenders decide to alter their plans?
7. Knowledge, capabilities, and skills of people in the organization are leverage points.	**Practice implications**: Organizational factors beyond the team affect the quality of their cyber defense because they are resources that can be drawn upon by defenders. All parts of the organization are potential resources in response; others in the organization may need awareness of what defenders do to maximize this resource. **Research questions**: How are knowledge, capabilities, and skills of people leveraged by defenders? How do differences in organizations affect how human resources are leveraged by defenders?

V. Discussion

The use case shows how CTAs can be used to learn about the macrocognition of defenders. Macrocognition informs the practice of cybersecurity by connecting the KSAs and Work Roles described in the NICE Framework to the strategies and processes of individuals. Implications and lessons learned through the use case are discussed next. Finally, implications of the methodology are presented to distinguish the potential of the larger methodology from the limitations of the specific use case.

Implications of the Use Case

The macrocognitive themes affirm findings from prior CTAs that CCSA, as developed through the process of sensemaking/situation assessment, is a salient component of defenders work to detect, analyze, and respond to events. The themes also suggest the importance of mental models; in combination with domain knowledge, defenders make use of a variety of continually evolving representations of interconnected elements. These include contextual factors such as who owns the asset and the business context (e.g., how people in the organization affect an asset). This representation extends the CCSA types of both Mahoney et al.

(2010) and Gutzwiller et al. (2016). Mahoney et al. (2010), incorporated the business context in compromise extent awareness and situational factors as social/ organizational/ behavioral awareness. Gutzwiller et al. (2016) represented these as team and world components. Based on the present representation, these factors could broaden to infrastructure (extending beyond the network) and organization (extending beyond the team).

The biggest limitation in interpretation of the use case as standalone research is the combination of a small convenience sample with limited time with each participant. Most past CTAs enjoyed larger samples and/or more comprehensive observation. In this case, the immediate value of the use case is the suggestion of themes for further investigation. A number of practical lessons are discussed next.

Lessons Learned

Lessons were learned at each step of the use case, starting with the recruitment. Encouragingly, when organizations responded to discuss the study, there was no shortage of support expressed for research to improve the proficiency of cybersecurity professionals. Being affiliated with San José State University and working on a National Science Foundation project may have facilitated participation. Managers and CISOs were generally eager to offer their teams for participation, but barriers to participation included concerns about confidentiality and limited access to cybersecurity professionals. In discussing the aims of the study, members of the research team emphasized the goal of the research in describing cognition but not describing specific incidents or threats. As the use case illustrates, there is value for methods which do not elicit information about specific incidents; however, this also constrained the research, as many CTA methods rely on discussions of specific cases, especially challenging ones, to understand how experts address them. Finding cybersecurity professionals in the correct role was also a challenge, evidenced by two participants despite a multiyear recruitment effort. In some cases, defenders were outsourced or distributed worldwide, making access more difficult. This required a pivot to remote data collection. Future research can address these limitations by seeking more depth within one organization through close partnerships, rather than trying to sample across many organizations. This could allow more precision in job role selection. Researchers should be aware that building the collaborative partnerships for recruitment requires substantial time. Meanwhile, the research needs to be ready to run on a short timeframe, as short windows for participation can appear after long delays from due diligence and participant availability. This can challenge an academic research team due to the seasonality of the academic calendar.

While the survey roughly identified participants as cybersecurity professionals in a defender role, it provided a limited picture of the training and experience of cybersecurity professionals. Informal and self-directed learning also contribute to the experience of many cybersecurity professionals, including in childhood (Champion et al., 2014), and this information was not captured. Beyond degrees earned, information about experience outside of cybersecurity was not captured. A better survey would be more comprehensive in describing the cybersecurity and non-cybersecurity education and experience of the participants. A succinct survey is also desirable; using the NICE Framework's Categories and Specialty Areas (Newhouse et al., 2017) may provide a way to quickly categorize participants. Categories and Specialty areas are presently deprecated in the NICE Framework Revision draft (Petersen et al., 2020); an alternative approach could be to sample representative work roles and ask about frequency of performing in those roles.

In future research, a more comprehensive survey could allow researchers to unify the focus question across maps. In hindsight, the research team started each concept map interview with limited information about defenders' experience, so revising the focus question was necessary to understand the participant's role. Differences in experience of the participants may be evident in the content and organization of the concept maps. Participant 1 reported more years of experience and drew a more detailed map oriented around decision making. Participant 2's map suggests a greater role of automation, but inferences comparing the proficiency of these individuals is speculative, largely due to the limitations of the survey.

Finally, concept mapping worked well for this purpose but is not the only CTA technique. Concept mapping resulted in a knowledge representation that could be generated in a single meeting. Limited time and access prevented use of certain

CTA methods that may provide more clarity into aspects of macrocognition or teamwork. These include direct task observation and critical decision methods. The critical decision method involves a subject-matter expert retroactively or concurrently walking the researcher through a specific incident (Crandall et al., 2006). Examination of standard operating procedures and lists of specific tools were also unavailable. Crandall et al. (2006) suggested that the representations from CTA be refined in a collaborative process with the original participants; this was only done immediately after constructing the map. A second interview with our participants to vet our conclusions was not part of the research protocol, resulting in a lack of data about how the resulting representation is viewed by the participants.

Research Implications of the Methodology

This work serves as a call and framework for continued CTA research to understand cognitive processes. By applying the methodology, quantitative researchers can benefit from better understanding of relevant contextual factors, which can lead to more meaningful experimentation and establish reliable measurement. For example, by enumerating and refining the types of CCSA, a richer picture of proficiency development in defenders can emerge. The methodology can explain the cognition behind proficiency. This can suggest strategies for its measurement, which can be developed and validated through quantitative research. Measured reliably, cognitive process measures would complement measures of KSAs in the NICE Framework to describe what defenders do and how they are able to do it. This could facilitate training for defenders in how to think, addressing a gap in the current state of practice.

The use case shows how research questions could be tested in quantitative research. CTAs are resource-intensive and can generate more questions than they answer. New questions can be supplied to quantitative researchers, who need testable hypotheses and the ability to isolate a limited number of variables of interest. This work suggests variables that may be able to be measured, such as CCSA for an incident; experimentation is needed to establish reliable measurement. Hoffman (2020) described challenges to conducting experiments to understand cyber operations including accounting for all important variables, especially ones embedded in the operational environment. As part of the methodology, researchers can use existing CTAs to list and prioritize variables for experimentation. Hoffman (2020) suggested a mixed-method approach of implementing CTA methods into their experimental protocols, essentially giving participants the opportunity to explain the cognition used in an experimental task. When this is not feasible, the methodology suggests how CTAs of defender cognition and quantitative studies may inform each other.

CTAs have great potential to augment each other. As an example, rather than offering a focus question tied to a person's role, a concept map could be made of asset targets, zones, and events. Insights can be derived even if participants reject the categorization and describe their own categorization and mental model. Further themes may emerge by analyzing concept maps with the same prompt from employees with, near, and outside a defender team.

Practice Implications of the Methodology

Defenders are the innovators in the practice of their profession, and this is especially evident in their central role in CTA. The scientific study of situation awareness emerged from interviews of pilots (Endsley, 1988), who discussed it as a familiar concept. The methodology shows how research can contribute to professionalization of cybersecurity careers by informing practice through understanding the cognition of high performing individuals.

The methodology and use case offer both near-term and long-term implications for defenders. In the near term, defenders could improve their practice by focusing on what happens before decisions are made. Outcomes are more salient than cognitive processes, which are not directly observable. Given this, there is value in discussing the hidden-yet-valuable role of macrocognition in performance outcomes, even as understanding of how it works is still emerging. That is, talking about macrocognition could help defenders connect how they think with their work outcomes. Encouraging discussion and debate of macrocognition among practitioners may help them reflect on their own thinking and development, a process called metacognition. Metacognition has been shown to predict performance and training effectiveness (Cuevas et al., 2004). Thinking about their thinking may help defenders better apply their skills and match them to the KSAs in the NICE Framework. This may help proficient defenders

mentor novices. In this way, individual defenders themselves will continue to contribute insights about how their work is conducted.

In the long-term, much interdisciplinary research is needed to realize the aims of the methodology, which itself is only one perspective on the work of cybersecurity professionals. In this regard, the methodology serves as a call for replication and participation by researchers and practitioners within and outside of cybersecurity. Envisioning this possibility, well-developed understanding of macrocognition may unlock novel and validated strategies for workforce development, especially in training and recruitment. Measurement of macrocognition would allow practitioners to diagnose human performance and to more fully utilize people as part of cyber defense. For training, it could provide an explanation for why and how skills are missing and suggest interventions. It would provide a layer of understanding of cybersecurity work that is relevant to, but not specifically tied to, an organization, Work Role, or Task.

Understanding macrocognition can also augment recruitment strategies by better answering the question of what qualities help people succeed in cybersecurity careers. It may allow people in other professions and pathways, or people who have not yet picked a profession, to be recruited to participate in cybersecurity careers on the basis of skill or interest in other tasks that involve thinking like a defender. Together with training, this approach may support broader participation in the field.

Conclusion

The methodology presented in this article complements the NICE Framework with research to understand defender cognition. The NICE Framework provides the language of Work Roles, Tasks, and KSAs. The methodology supplies explanation of how KSAs are used and develop. Together, they can help close the cybersecurity skills gap by connecting the elements of work to the capabilities of people.

VI. Acknowledgements

This work is based upon work supported by the National Science Foundation under Grant No. 1553018. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

The author gratefully acknowledges the participation of cybersecurity professionals and their employers. The author also wishes to thank the student members of his lab for their assistance with data collection and coding.

References

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2020). Challenges and performance metrics for security operations center analysts: A systematic review. *Journal of Cyber Security Technology,* 4(3), 125–152. https://doi.org/10.1080/23742917.2019.1698178

Bissell, K., Lasalle, R. M., & Dal Cin, P. (2019) *Ninth Annual Cost of Cybercrime Study*. Dublin, Ireland: Accenture https://www.accenture.com/us-en/insights/security/cost-cybercrime-study. Also available at https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51–61. https://doi.org/10.1016/j.chb.2015.01.039

Biros, D. P., & Eppich, T. (2001). Human element key to intrusion detection. *Signal*. https://www.afcea.org/content/human-element-key-intrusion-detection

Braisby, N. & Gellatly, A. (2005). *Cognitive psychology.* Oxford University Press.

Buchanan, L., D'Amico, A., & Kirkpatrick, D. (2016). Mixed method approach to identify analytic questions to be visualized for military cyber incident handlers. *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 1–8. https://doi.org/10.1109/VIZSEC.2016.7739578

Champion, M., Jariwala, S., Ward, P., & Cooke, N. J. (2014). Using cognitive task analysis to investigate the contribution of informal education to developing cyber security expertise. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 310–314. https://doi.org/10.1177/1541931214581064

Cooke, N. J., Champion, M., Rajivan, P., & Jariwala, S. (2013). Cyber situation awareness and teamwork. *ICST Transactions on Security and Safety,* 1(2). https://doi.org/10.4108/trans.sesa.01-06.2013.e5

Crandall, B., Klein, G. A., & Hoffman, R. R. (2006). *Working Minds: A Practitioner's Guide to Cognitive Task Analysis*. MIT Press.

Crumpler, W., & Lewis, J. A. (2019). *The Cybersecurity Workforce Gap.* Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-workforce-gap

Cuevas, H. M., Fiore, S. M., Bowers, C. A., & Salas, E. (2004). Fostering constructive cognitive and metacognitive activity in computer-based complex task training environments. *Computers in Human Behavior,* 20(2), 225–241. https://doi.org/10.1016/j.chb.2003.10.016

D'Amico, A., & Whitley, K. (2007, October 9). The Real Work of Computer Network Defense Analysts. *2007 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 19–37. https://doi.org/10.1007/978-3-540-78243-8_2

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*(3), 229–233. https://doi.org/10.1177/154193120504900304

Endsley, M. R. (1988). Situation Awareness Global Assessment Technique (SAGAT). *Proceedings of the National Aerospace and Electronics Conference (NAECON),* 3, 789-795. http://doi.org/10.1109/NAECON.1988.195097

Erbacher, R. F., Frincke, D. A., Wong, P. C., Moody, S., & Fink, G. (2010). A multi-phase network situational awareness cognitive task analysis. *Information Visualization*, 9(3), 204–219. https://doi.org/10.1057/ivs.2010.5

Feltovich, P. J., Prietula, M. J., & Ericsson, K. A. (2018). Studies of expertise from psychological perspectives: Historical foundations and recurrent themes. In K. A. Ericsson, R. R. Hoffman, A. Kozbelt, & A. M. Williams (Eds.), *The Cambridge handbook of expertise and expert performance* (2nd ed., pp. 59–83). https://doi.org/10.1017/9781316480748.006

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People,* 22(2), 92–108. https://doi.org/10.1108/09593840910962186

Gutzwiller, R. (2019). *Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment Through 2015* (No. TR-3184). NIWC Pacific San Diego United States. https://apps.dtic.mil/sti/citations/AD1074248

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA),* 14–20. https://doi.org/10.1109/COGSIMA.2016.7497780

Hoffman, R. R. (2019). The Concept of a "Campaign of Experimentation" for Cyber Operations. *The Cyber Defense Review, 4*(1), 75-84. Retrieved August 31, 2020, from https://www.jstor.org/stable/26623068

Hoffman, R. R., Ward, P., Feltovich, P. J., DiBello, L., Fiore, S. M., & Andrews, D. H. (2014). *Accelerated Expertise: Training for High Proficiency in a Complex World.* Psychology Press.

Klein, G., & Militello, L. (2001). Some guidelines for conducting a cognitive task analysis. *In Advances in Human Performance and Cognitive Engineering Research* (Vol. 1, pp. 163–199). Emerald. https://doi.org/10.1016/S1479-3601(01)01006-2

Klein, G., Ross, K. G., Moon, B. M., Klein, D. E., Hoffman, R. R., & Hollnagel, E. (2003). Macrocognition. *IEEE Intelligent Systems, 18*(3), 81–85. https://doi.org/10.1109/MIS.2003.1200735

Klein, G., & Wright, C. (2016). Macrocognition: From Theory to Toolbox. *Frontiers in Psychology*, 7. https://doi.org/10.3389/fpsyg.2016.00054

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). A Cognitive Task Analysis for Cyber Situational Awareness. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 54*(4), 279–283. https://doi.org/10.1177/154193121005400403

Morgan, S (Ed.). (2019). 2*019 Cybercrime Report*. Sausalito, CA: Cybersecurity Ventures. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

National Institute of Standards and Technology (NIST). (2020). Cyberseek [Web-based heat map of cybersecurity supply and demand]. http://cyberseek.org/heatmap.html

Newhouse, W., Keith, S., Scribner, B., Witte, G. (2017). *National initiative for cybersecurity education (NICE) cybersecurity workforce framework* (Report No. SP 800-181). Gaithersburg, MD: National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-181/final

Nyre-Yu, M., Gutzwiller, R. S., & Caldwell, B. S. (2019). Observing Cyber Security Incident Response: Qualitative Themes from Field Research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63*(1), 437–441. https://doi.org/10.1177/1071181319631016

Paul, C. L., & Whitley, K. (2013). A Taxonomy of Cyber Awareness Questions for the User-Centered Design of Cyber Situation Awareness. In L. Marinos & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (Vol. 8030, pp. 145–154). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39345-7_16

Petersen, R., Santos, D., Smith, M., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE Framework*; Report No. SP 800-181 Revision 1). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1-draft

Rasmussen, J., Pejtersen, A. M., & Schmidt, K. (1990). *Taxonomy for cognitive work analysis.* Risø National Laboratory.

Rooney, V. M., & Foley, S. N. (2018). What You Can Change and What You Can't: Human Experience in Computer Network Defenses. In N. Gruschka (Ed.), *Secure IT Systems* (Vol. 11252, pp. 219–235). Springer International Publishing. https://doi.org/10.1007/978-3-030-03638-6_14

Rouse, W. B., & Morris, N. M. (1986). On looking into the black box: Prospects and limits in the search for mental models. *Psychological Bulletin, 100*(3), 349–363. https://doi.org/10.1037/0033-2909.100.3.349

Saner, L. D., Campbell, S., Bradley, P., Michael, E., Pandza, N., & Bunting, M. (2016). Assessing Aptitude and Talent for Cyber Operations. In D. Nicholson (Ed.), *Advances in Human Factors in Cybersecurity* (Vol. 501, pp. 431–437). Springer International Publishing. https://doi.org/10.1007/978-3-319-41932-9_35

Schraagen, J. M., Chipman, S. F., & Shalin, V. L. (2000). *Cognitive task analysis*. Psychology Press.

Schuster, D., & Wu, S. (2018). Toward Cyber Workforce Development: An Exploratory Survey of Information Security Professionals. *Proceedings of the ' Human Factors and Ergonomics Society Annual Meeting, 62*(1), 1242–1246. https://doi.org/10.1177/1541931218621285

Shah, A., Ganesan, R., Jajodia, S., & Cam, H. (2018). A methodology to measure and monitor level of operational effectiveness of a CSOC. *International Journal of Information Security, 17*(2), 121–134. https://doi.org/10.1007/s10207-017-0365-1

Six skills you need to succeed in cybersecurity. (n.d.). *In Dice Insights*. Retrieved August 31, 2020, from https://insights.dice.com/cybersecurity-skills/

Stein, D., Scribner, B., Kyle, N., Newhouse, W., Williams, C., & Yakin, B. (2017). *National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles* (Report No. Draft NISTIR 8193). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/nistir/8193/draft/documents/nistir8193-draft.pdf

Tetrick, L. E., Zaccaro, S. J., Dalal, R. S., Steinke, J. A., Repchick, K. M., Hargrove, A. K., ... Wang, V. (2016). *Improving Social Maturity of Cybersecurity Incident Response Teams*. Fairfax, VA: George Mason University. https://calctraining 2015.weebly.com/the-handbook.html

Trent, S., Hoffman, R. R., Merritt, D., & Smith, S. (2019). Modelling the Cognitive Work of Cyber Protection Teams. *The Cyber Defense Review, 4*(1), 125-136. https://www.jstor.org/stable/26623071

Wei, J., & Salvendy, G. (2004). The cognitive task analysis methods for job and task design: Review and reappraisal. *Behaviour & Information Technology, 23*(4), 273–299. https://doi.org/10.1080/01449290410001673036

Woods, D. D., & Roth, E. M. (1988). Cognitive Engineering: Human Problem Solving with Tools. Human Factors: *The Journal of the Human Factors and Ergonomics Society, 30*(4), 415–430. https://doi.org/10.1177/001872088803000404

Yurcik, W., Barlow, J., & Rosendale, J. (2003). Maintaining perspective on who is the enemy in the security systems administration of computer networks. *Proceedings of the ACM CHI Workshop on System Administrators Are Users* (pp. 345-347). ACM Press.

Zhong, C., Yen, J., Liu, P., Erbacher, R., Etoty, R., & Garneau, C. (2015). An integrated computer-aided cognitive task analysis method for tracing cyber-attack analysis processes. *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security.* https://doi.org/10.1145/2746194.2746203

Teaching Perspectives

Wireless Security: Examining the next NICE Framework Iteration based on Industry Requirements

Suzanna Schmeelk and Denise Dragos
St. John's University, United States

***Abstract*—Problem Statement:** Wireless security is expanding at an unprecedented rate and is essential for untethered consumer goods, either organizational or private. Organizations ranging from hospitals, banks, and Armed Forces, to Uber Drivers employing wireless technologies, are adopting implicit and explicit risks. This research contributes an examination of industry best-practice certifications, curriculums, and recent books with respect to wireless security to inform on relevant industry topics needed for the next iteration of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

Research Questions: There remains a research gap on best-practice topic coverage in wireless security courses. The gap is due in part to rapid changes in IoT, near-field communications, and vehicle designs. Particularly, we ask, what wireless security topics are currently covered in the NICE with respect to leading certifications?

Contribution: This paper identifies important gaps in the learning of wireless security. We compare the leading industry certifications and leading academic curriculums to identify gaps, for the next iteration of the NIST NICE framework. Specifically, we identify gaps in the wireless technology protocol coverage, wireless technology element coverage, wireless attacks/defenses topic coverage, and wireless forensics topics coverage. Based on these findings, we develop two curriculums, as there exists no literature on these industry educational gaps.

Rationale: Based on the industry review, we design two semester-long wireless security courses to address the changing wireless security needs and develop course topic categories that are useful to map the NICE Cybersecurity Workforce Framework and that can be useful for continual course improvement for ABET (re)accreditation.

Investigative Approach: We investigate our advanced courses in wireless security and industry best practices for both a quantitative and qualitative analysis of wireless security educational topics coverage. Quantitatively, we analyze wireless security topics coverage count in leading frameworks and cybersecurity courses. Qualitatively, we examine actual wireless topics, based on the authors extensive industry experience, to cover to keep pace with the industry wireless trends.

Lessons Learned: Since the NICE Cybersecurity Workforce Framework was published as NIST Special Publication 800-181 in August 2017, NIST intends to review and update the NICE Framework. This qualitative and quantitative analysis provides insights into wireless security topic coverage which should be included in a new NICE framework iteration.

Implications for Practice: We as researchers spent many years at Bell Laboratories in New Jersey, at top-tier hospitals in New York City, and 20+ years with the New York Police Department (NYPD). During these experiences, we worked on many wireless technologies and their underlying security, from development and implementation to forensics perspectives. Our industry experience permeates our developed curriculums. We compare our curriculums with leading practitioner exams (e.g., OSWP) and frameworks (e.g. NICE) to advance the training requirements. All organizations accept wireless security risks; therefore, it is fundamental that the cybersecurity workforce understands these implicit and explicit risks.

Implications for Research: There remains a wireless security educational literature gap. Understanding the limitations and benefits for current frameworks and certifications on wireless security raises fundamental cybersecurity training questions. Additional investigations can transpire on quantity and quality of topics, developing working training labs, and understanding key security engineering.

Keywords—Wireless Security, Mobile Forensics, NICE Cybersecurity Workforce Framework, Offensive Security Wireless Professional (OSWP), Certified Information Systems Security Professional (CISSP), CompTIA Security+, National Security Agency-Knowledge Units (NSA-KUs), Accreditation Board for Engineering and Technology (ABET), Computing Sciences Accreditation Board (CSAB), The Association of Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE).

I. Introduction

Wireless security is essential for the security of system communications and underlying data. The Open Web Application Security Project's (OWASP) top third mobile security threat is of Insecure Communications (OWASP, 2020). Insecure communications can result in the loss of confidentiality, integrity, and availability (CIA) of systems and their data. To guard against the insecure dissemination of wireless data, typically referred to as the protection of data-in- motion, mitigating against threats to wireless transmissions is essential. In addition to the design and deployment of secure wireless transmissions, is the need for incident response and wireless network forensics in the result of cybersecurity incidents and crimes. The design, deployment, decommissioning, and forensics of wireless systems encompass the full technology lifecycle understanding needs for industry leading and data breach aware cybersecurity risk management professionals.

This work compares wireless security curriculums with leading practitioner exams (e.g. OSWP, CompTIA Security+, CISSP) and frameworks (e.g. NICE, ACM, NSA) to advance the training requirements for workforce capabilities. We report on a developed curriculum for an advanced Wireless Security course taught in New York by cybersecurity industry veterans. As all organizations accept wireless security risks, it is fundamental that the cybersecurity workforce understands these explicit and implicit associated risks.

Problem Statement

Wireless security is expanding at an unprecedented rate and is in many cases essential for untethered consumer goods either organizational or private. Organizations from hospitals, to banks, to Armed Forces, to Uber drivers employing Bluetooth and Near Field Communication (NFC) technologies, are adopting risks by employing these technologies. This research examines both the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework and the Offensive Security Wireless Professional (OSWP) certification with respect to an advanced Wireless Security course within a Cybersecurity B.S. program to discover framework coverage gaps such as in Internet of Things (IoT), NFC, Bluetooth, 5G and underlying wireless firmware development. Our wireless security course examines recent wireless security data breaches showing that wireless security is still not well understood across the cybersecurity workforce.

Review of Literature and Research Rationale

There are three main domains of relevant literature for this paper. The first domain is industry wireless security trends and wireless communication specifications such as WIFI data- in-motion encryption (e.g. WPA3, WPA2, etc.), Bluetooth security (Haataja 2008), Near Field Communications (NFC) security, Internet of Things (IoT) security, and 3GPP Cellular (3GPP, 2020), among other wireless protocols. Summers and DeJoie (2004) report on early wireless security topics. The second domain is academic wireless security and forensic research (Ghafarian, 2019). Little, if any recent published academic research exists on wireless security technologies in some of the major leading literature databases. A third and most relevant research domain is wireless security education, which entirely suffers from a literature and research gap. Education literature, however, does exist in the larger domain of cybersecurity education. For example, the Joint Task Force on Cybersecurity Education (2018) created a report based on industry surveys for Curriculum Guidelines for Post- Secondary Degree Programs in Cybersecurity. The guidelines note wireless security topics including: implementations of the wireless 'physical' media; wireless issues surrounding biomedical devices [a special subset of embedded systems]; and security awareness, training and education (commonly referred to as SETA). However, we were unable to identify any educational studies incorporating student feedback such as those often found in the field of Mathematics Education (Schmeelk, Krupnik, Nyakoojo, Maher, & Horwitz, 2020). This cybersecurity literature gap on educational skills studies for wireless security warrants new wireless security education research.

II. Research Questions

Our research contributes to curriculum development for Wireless Security courses. We carefully analyze respected wireless security related industry certifications, curriculums, recent textbooks, and best practices from standardizing bodies to identify gaps in the current NIST NICE framework to include in a future update of the framework. Specifically, we ask, what are the

current wireless security topics and skills examined in the current NIST NICE framework and are there potential gaps to fill in a new iteration. We found that an understanding of the creation of wireless embedded systems firmware development and detailed network forensics topics are entirely missing from cybersecurity research education and the current NIST NICE framework.

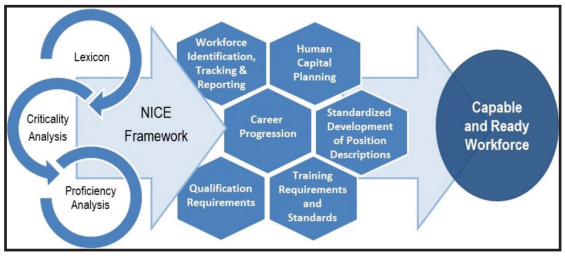
III. Investigative Approach

In order to make recommendations for the next iteration of the NICE framework to answer our first research question, we analyze existing industry best practice certifications, curriculums, and recent books. Specifically, we examined the following entities to gain insights in topic coverage:

- Offensive Wireless Security Professional (OffSec Services Limited, 2020)
- CompTIA Security+ (CompTIA, 2020)
- Certified Information Systems Security Professional (CISSP) ((ISC)² , 2020)
- NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST, 2017)
- National Security Agency (NSA)'s National Centers of Academic Excellence (CAE) (NSA) , 2020)
- Computing Sciences Accreditation Board (CSAB) (CSAB, 2020)
- Accreditation Board for Engineering and Technology (ABET) (ABET, 2020)
- The Association of Computing Machinery (ACM) (Association for Computing Machinery (ACM), 2020)
- Institute of Electrical and Electronics Engineers (IEEE)
- Wireless Hacking Exposed (Wright & Cache, 2015)
- Wireless and Mobile Device Security (Doherty, 2016)
- SANS (SANS, 2020)
- Current iteration of our developed wireless security course.

Our analysis of these entities for wireless security topic coverage is discussed in the following subsections.

Figure 1: Building Blocks for a Capable and Ready Cybersecurity Workforce



NICE Cybersecurity Workforce Framework

The NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) is published in the NIST Special Publication (SP) 800-181 (NIST, 2017). The framework serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization. As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent (Figure 1). The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity workforce development, planning, training, and education.

The NICE Framework SP 800-11 defines their usage of the term's knowledge, skills, abilities, and tasks. Overall, KSAs are attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training. Formally, ***knowledge*** is defined as the "body of information applied directly to the performance of a function." ***Skill*** is defined as "an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual." The ***ability*** keyword is defined as the "competence to perform an observable behavior or a behavior that results in an observable

product." Finally, ***task*** is defined in 800-11 as, "a specific defined piece of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role."

The NICE Framework provides categories for workforce personnel, as seen in Figure 2.

Figure 2: NICE Framework Workforce Categories

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

The NICE Framework provided a list of cybersecurity Specialty Areas for each of the workforce categories listed in Figure 2. The framework lists between two and seven specialty areas for each category. In industry, due to the wide range of cybersecurity team sizes from only one workforce member to numerous team members, these workforce categories may or may not translate directly to each organization. Table 8, found in Appendix A, shows the NICE wireless security components, specialty areas, task ID, descriptive statement and competency.

NIST SP 800-11 provides a listing of all the tasks that have been identified as being part of a cybersecurity work role. Each task involving wireless technology is listed in Table 1.

Table 1: NIST 800-11 Task Mappings

ID	Task Description
T0289	Utilize deployable forensics toolkit to support operations as necessary.
T0608	Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.
T0609	Conduct access enabling of wireless computer and digital networks.
T0610	Conduct collection and processing of wireless computer and digital networks.
T0612	Conduct exploitation of wireless computer and digital networks.
T0697	Facilitate access enabling by physical and/or wireless means.
T0807	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.

KSAs describe the various kinds of information applied directly to the performance of a function. A complete listing of the NIST NICE mappings of KSAs with job workforce categories can be found on the full spreadsheet entitled, Reference Spreadsheet for NIST Special Publication 800-181 (NIST, 2020) Table 2.

As defined above, skill is the observable competence to perform a learned psychomotor act. There are three relevant skills listed for wireless technologies as seen in Table 3.

Table 2: NIST 800-11 Knowledge Mappings

ID	Description
K0108	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
K0133	Knowledge of types of digital forensics data and how to recognize them.
K0134	Knowledge of deployable forensics.
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).
K0274	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.
K0375	Knowledge of wireless applications vulnerabilities
K0388	Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologies, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies.
K0428	Knowledge of encryption algorithms and tools for wireless local area networks (WLANs).
K0438	Knowledge of mobile cellular communications architecture (e.g., LTE, CDMA, GSM/EDGE and UMTS/HSPA).
K0442	Knowledge of how converged technologies impact cyber operations (e.g., digital, telephony, wireless).
K0446	Knowledge of how modern wireless communications systems impact cyber operations.
K0573	Knowledge of the fundamentals of digital forensics to extract actionable intelligence.
K0600	Knowledge of the structure, architecture, and design of modern wireless communications systems.
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.

Table 3: NIST 800-11 Skills Mappings

ID	Description
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).
S0182	Skill in analyzing target communications internals and externals collected from wireless LANs.
S0276	Skill in survey, collection, and analysis of wireless LAN metadata.
S0299	Skill in wireless network target analysis, templating, and geolocation.

Ability, as defined above, is the competence to perform an observable behavior or a behavior that results in an observable product. NIST lists one wireless technology ability, as seen in Table 4.

Table 4: NIST 800-11 Ability Mappings

ID	Description
A0100	Ability to perform wireless collection procedures to include decryption capabilities/tools

NSA's CAE Knowledge Units

The National Security Agency (NSA) sponsors two types of Centers of Academic Excellence (CAE): one in Cyber Defense (CD) and one in Cyber Operations (CO) (National Security Agency, 2020). The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program. CAE centers for cyber defense can either be designated as education or research centers, CAE-CDE and CAE-R respectively. The NSA's CAE in Cyber Operations (CAE-CO) program supports the President's National Initiative for Cybersecurity Education (NICE) and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation. The relevant skills mappings, or knowledge units, is shown in Figure 3.

Figure 3: Relevant NSA CAE KU Mapping Concepts

Relevant CAE KU Mapping Concepts:
- Foundational CDE Knowledge Units
  - Cybersecurity Foundations (CSF)
  - Cybersecurity Principles (CSP)
  - IT Systems Components (ISC)
    - 5. Networks (Internet, LANs, wireless)
- Core Technical CDE Knowledge Units
  - Basic Cryptography (BCY)
  - Basic Networking (BNW)
    - 2. Network media (wired, optical, and wireless)
  - Basic Scripting and Programming (BSP)
  - Network Defense (NDF)
  - Operating Systems Concepts (OSC)
- Core Non-Technical CDE Knowledge Units
  - Cyber Threats (CTH)
    - 3. Types of Attacks (and vulnerabilities that enable)
      - b. Backdoors / trojans / viruses / wireless attacks
  - Cybersecurity Planning and Management (CPM)
  - Policy, Legal, Ethics, and Compliance (PLE)
  - Security Program Management (SPM)
  - Security Risk Analysis (SRA)
- Optional Knowledge Units
  - Wireless Sensor Networks (WSN)
  - Embedded Systems (EBS)
  - Mobile Technologies (MOT)
  - Radio Frequency Principles (RFP)

Offensive Security Wireless Professional (OSWP)

The Offensive Wireless Security Professional (OffSec Services Limited, 2020) is a four-hour exam in which the student seeking certification is required to recover the keys to three wireless (WiFi) networks. A recent certificate awardee blogged that the setup is "quite clever and efficient with SSH access to an Offsec attacking system which has a packet injectable adapter attached and the [three] required networks within range of this" (Budd, 2019). To prepare for the OSWP hands-on exam, the Offensive Security course Wireless Attacks (WiFu) is suggested (Offensive Security, 2020). Topics covered in the Offensive Security WiFU course are shown in Figure 4.

Figure 4: OSWP Relevant Topics

OSWP Exam Outline:

- 802.11 Standards and Amendments
- Detailed Protocol Descriptions
- Packets and Network Interaction
- Hardware (Antennas, Wireless Cards)
- Linux Wireless Stack and Drivers
- Wireless Operating Modes
- Aircrack-ng Essentials
- Cracking WEP with Connected Clients
- Cracking WEP via a Client
- Cracking Clientless WEP Networks
- Bypassing WEP Shared Key Authentication
- Cracking WPA/WPA2 PSK w/ Aircrack-ng
- Cracking WPA with JTR and Aircrack-ng
- Cracking WPA with coWPAtty
- Cracking WPA with Pyrit
- Wireless Reconnaissance
- Rogue Access Points
- ARP Amplification

CompTIA Security+

The CompTIA Security+ (CompTIA, 2020) is a global certification that validates the baseline skills needed to perform core security functions and pursue an IT security career. Many employers look for this certification among candidates. Relevant wireless security and forensics concepts in the CompTIA Security+ SY0-501 and SY0-601 exams are shown in Figure 24 (Appendix B), with many relevant topics.

Certified Information Systems Security Professional

The Certified Information Systems Security Professional (CISSP) is an independent information security certification granted by the International Information System Security Certification Consortium, (ISC)² ((ISC)² , 2020). According to the (ISC)² member portal ((ISC)², 2020), as of July 22, 2020, there are 141,607 members holding the CISSP certification worldwide. The CISSP has eight domains of questions, based on the outline ((ISC)², 2020). According to the (ISC)² CISSP exam outline, there is only one instance where wireless security is discussed as a domain on the exam. CISSP does not mention any specific wireless technologies. Instead, they specify to implement secure design principles, as shown in Figure 5.

Figure 5: CISSP Relevant Wireless Topics

CISSP Exam Outline:

- Domain 4: Communication and Network Security
  - 4.1 Implement secure design principles in network architectures
    - Wireless networks
- Domain 7 - Security Operations
  - 7.1 Understand and support investigations
    - Digital forensics tools, tactics, and procedures

Accreditation Boards: CSAB, ABET, ACM, IEEE

Computing Sciences Accreditation Board (CSAB) is the lead Accreditation Board for Engineering and Technology (ABET) (ABET, 2020) member society for accreditation of degree programs in Computer Science, Cybersecurity, Data Science, Information Systems, Information Technology, and Software Engineering (CSAB, 2020). The Association for Computing Machinery (ACM) and the IEEE Computer Society (IEEE-CS) are the member societies of CSAB.

The ACM recommends curriculum development for Computer Engineering, Computer Science, Cybersecurity, Information Systems, Information Technology, and Software Engineering. (Association for Computing Machinery (ACM), 2020). Specifically, for Cybersecurity, the ACM published the Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, 2017).

The ACM/IEEE CS2013 Body of Knowledge (BoK) serves as the foundational curricular framework for the ACM associate-degree transfer guidelines in computer science. The CS2013 BoK is organized into a set of 18 Knowledge Areas (KA) that correspond to topical areas of study in computing for undergraduate, baccalaureate degree programs in computer science. A KA may not necessarily equate to a course, and are listed in Figure 6.

Figure 6: ACM's KAs of the Computer Science Transfer Curriculum

Cybersecurity KA Knowledge Units
Foundational Concepts in Security
Principles of Secure Design
Defensive Programming
Threats and Attacks
Cryptography
Web Security

In the ACM latest curriculum guidelines, the ACM only explicitly discuss Wireless Security in the Networking and Communications (NC) KA, Figure 7. Implicitly, however, their overarching Cybersecurity KAs listed in Figure 7 are all relevant to the wireless security domain.

Figure 7: ACM Relevant Topics (Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, 2017)

NC/Networked Applications Knowledge Unit Assessment:
- Emerging - NC-06. Describe security concerns in designing applications for use over wireless networks. [Understanding]
- Developed - Recognize security concerns in designing applications for use over wireless networks. [Remembering]
- Highly Developed - Illustrate security concerns in designing applications for use over wireless networks. [Applying]

Wireless Hacking Exposed

The book Wireless Hacking Exposed (WHE) (Wright & Cache, 2015) is a popular educational wireless security book. Wright has been a senior instructor and author for SANS Institute as well as holding senior technical roles at organizations including Counter Hack. Cache, Chache Heavy Industries. He has been a speaker at BlackHat, BlueHat, and ToorCon. He has also written papers and tools on/for the security of 802.11. The technical book shows many types of wireless attacks and occasionally discusses mitigations. Interestingly, the book introduces many tools and gives all the tools the authors decided risk rating based on perceived popularity, simplicity, and impact. The relevant WHE topics are shown in Figure 8. The book provides a few resources for hands-on exercises for learners.

Figure 8: WHE Relevant Topics (Wright & Cache, 2015)

Wireless Hacking Exposed Topic Coverage:
- Introduction to 802.11 Hacking
- Scanning and Enumerating 802.11 Networks
- Attacking 802.11 Wireless Networks
- Attacking 802.11 Wireless Clients
- Bridging the Air-Gap from Windows 8
- Bluetooth Classing Scanning and Reconnaissance
- Bluetooth Low Energy Scanning and Recon
- Bluetooth Eavesdropping
- Attacking and Exploiting Bluetooth
- Software-Defined Radios
- Hacking Cellular Networks
- Hacking ZigBee
- Hacking ZWave Smart Homes

Wireless and Mobile Device Security

The book *Wireless and Mobile Device Security (WMDS)* (Doherty, 2016) is part of the Jones & Bartlett Learning's Information Systems Security & Assurance Series. The book approaches security through risk mitigation and assurance mechanisms. Jim Doherty, the book's author, has held leadership positions in organizations including Ixia, Cisco Systems, Certes Networks, and Ericsson Mobile. The book's relevant topics are shown in Figure 9.

Figure 9: WMDS Relevant Topics (Doherty, 2016)

Wireless and Mobile Device Security Topic Coverage:
- Evolution of Data Networks
- Evolution from Wired to Wireless
- Mobile Revolution
- Security Threats: Wired, Wireless, Mobile
- WLAN Architecture
- WLAN Vulnerability Analysis
- Basic WLAN Security Measures
- Advanced WLAN Security Measures
- WLAN Auditing Tools
- WLAN Risk Assessments
- Mobile Communication Security Challenges
- Mobile Device Security Models
- Mobile Wireless Attacks and Remediations
- Fingerprinting Mobile Devices
- Mobile Malware and Application-Based Threats

The book *Wireless and Mobile Device Security (WMDS)* comes with mappings of the book to different standards, curriculums, and certifications. Table 5 and Table 6 show the mappings of the book to two important aspects of the CompTIA Security+ exam. As can be seen, the book provides very few, if any, relevant hands on lab exercises.

Table 5: Security+ Wireless Config Mapping to WMDS

CompTIA Security+ SY0-501	Mobile1e: Wireless and Mobile Device Security		
	Book Chapter	Course Lesson	Hands On Lab
6.3 Given a scenario, install and configure wireless security settings.			
Implementation vs. algorithm selection	1, 6, 7, 8, 9	7	
o WPA	1, 6, 7, 9	7	
o WPA2	1, 6, 7, 8, 9	7	
o CCMP	7, 8		
o TKIP	7		
Authentication protocols	7, 8, 13	8	
o EAP	7, 8		
o PEAP			
o EAP-FAST			
o EAP-TLS	13		
o EAP-TTLS			
o IEEE 802.1x	7, 8	8	
o RADIUS Federation			
Methods	7, 8, 9, 13, 15		
o PSK vs. Enterprise vs. Open	7, 8, 9		
o WPS			
o Captive portals	8, 13, 15		

Table 6: Security+ Wireless Attacks Mapping to WMDS

CompTIA Security+ SY0-501	Mobile1e: Wireless and Mobile Device Security		
	Book Chapter	Course Lesson	Hands On Lab
Wireless attacks	4, 6, 7, 9, 13	4, 6, 9	
o Replay	6		
o IV	7		
o Evil twin	6, 9	6	
o Rogue AP	4, 6, 7, 9, 13	6	
o Jamming	9	9	
o WPS			
o Bluejacking	6	6	
o Bluesnarfing	6	6	
o RFID			
o NFC	4	4	
o Disassociation	6, 13		
Cryptographic attacks	1, 6, 7, 9		
o Birthday			
o Known plain text/cipher text			
o Rainbow tables	9		
o Dictionary	9		
o Brute force	9		
▪ Online vs. offline			
o Collision			
o Downgrade			
o Replay	6		
o Weak implementations	1, 7		

SANS Relevant Trainings

The SANS Institute was established in 1989 as a cooperative research and education organization. A list of their current course offerings can be found on their course list (SANS, 2020). Five relevant courses are shown in Figure 10. The courses either focus on wireless, mobile devices, or include network forensics topics. All three elements are essential to wireless security.

Figure 10: SANS Relevant Course Offerings

Wireless and Mobile Device Courses:

- SEC617: Wireless Penetration Testing and Ethical Hacking. Certification: GIAC Assessing and Auditing Wireless Networks (GAWN)
- SEC575: Mobile Device Security and Ethical Hacking. Certification: GIAC Mobile Device Security Analyst (GMOB)
- FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. Certification: GIAC Network Forensic Analyst (GNFA)
- FOR498: Battlefield Forensics & Data Acquisition. Certification: GIAC Battlefield Forensics and Acquisition (GBFA)
- FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics. Certification: GIAC Certified Forensic Analyst (GCFA)

IV. Results and Contributions

Framework iteration. We also present suggested developed curriculums to address historical industry gaps in learning from more traditional wireless security related courses.

NICE Summary of Topics Coved by Content Domain

From the entities analyzed, there are three important arch- categories of coverage for wireless security. One domain is on the actual wireless technologies covered (Table 7), and the other is of the spread of topics covered within a given analyzed entity (Figure 11). In Table 7, the columns signify the following: **W** – WIFI, **B** – Bluetooth, **I** – IoT, **N** – NFC, **C** – Cellular, **S** – Satellite, **P** – Paging, **E** – Embedded System Communication, **Z** – SCADA, **Y** – IR, **R** – RFID, and **F** – Wirelesses without further protocol specification.

The IoT (**I**) category includes the following technologies: Adaptive Network Topology (ANT), Zigbee, ZWave, and Wireless Sensor Networks (WSN).

Table 7 shows coverage gaps in NICE for current wireless technologies such as NFC (e.g. Apple Pay, Android Pay, Android-NFC), IoT, and embedded systems (e.g. wireless router firmware development, automobiles, printers, etc.). Some embedded systems do however communicate with protocols listed in Table 7.

Table 7: Domain of Wireless Technologies Covered

	W	B	I	N	C	S	P	E	Z	Y	R	F
OSWP	*											
CISSP												*
Sec+	*	*	*	*	*	*		*	*	*		
NICE	*	*			*	*	*		*	*	*	
NSA	*		*		*			*			*	
CSAB												*
SANS	*				*							
WMDS	*	*			*							
WHE	*	*			*		*	*				

As we can see from Table 7, our first finding is that certain wireless domains are covered strongly on some certifications but other domains are entirely missing. The table provides a 'strengths' analysis for which certifications are strong in what domain. As we can see from the table, the next iteration of the NIST NICE framework would benefit from adding skills and tasks related specifically to IoT. Popular protocols in IoT include ZWave and Zigbee. Another area to add to the NIST NICE framework is NFC and other near field payment options such as Apple Pay and Android Pay. NICE NIST also could benefit from embedded device security such as custom firmware development for wireless routers, vehicles, medical devices, among other embedded systems.

Our second finding is shown in Figure 11. The figure presents the best practice topics findings of the research for the coverage with respect to each wireless technology. This domain is essential for a complete security lifecycle understanding from wireless design, risk, to the forensics surrounding an incident or crime.

Our third finding of importance is the coverage of different wireless attacks. Figure 12 presents the current best practice attacks for coverage, however, wireless attacks and mitigations continually evolve due to the dynamic nature of cybersecurity. Currently, NICE has specific KSAs and Tasks on topics listed with the numbered bullets as follows: 1 (operating systems only), 2, 3, 4 (jamming attacks only), and 5 (fidelity Only). NICE should consider adopting the remaining topics listed in Figure 11.

Figure 11: Topic Coverage within Wireless Technology

Topic coverage within a given analyzed entity:

1. Hardware, Software, Operating Systems
2. Design, Architecture, Topology
3. Protocols, Operations
4. Reconnaissance, Attacks, Mitigations
5. Risk and Metadata Analysis
6. Ethics

The attacks listed of in Figure 12 are found throughout the analyzed entities. However, NICE currently keeps these attacks at a high-level with the following: (K0274) jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly; (T0612) Conduct exploitation of wireless computer and digital networks; (S0299) Skill in wireless network target analysis, templating, and geolocation; (A0100) Ability to perform wireless collection procedures to include decryption capabilities/tools.

Figure 12: Specific Wireless Attacks Discussed

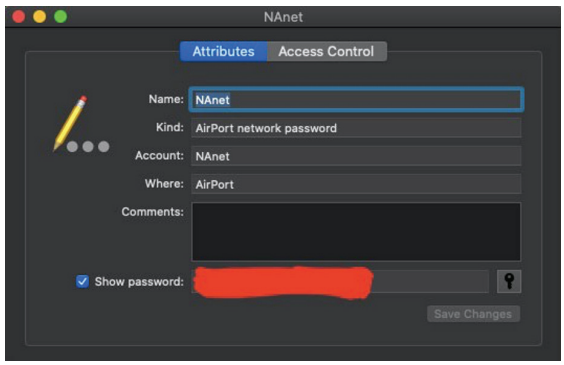
Wireless Attacks:

- Replay
- IV
- Evil twin
- Rogue AP
- Jamming
- Wi-Fi Protected Setup (WPS)
- Bluejacking
- Bluesnarfing
- Disassociation
- Breaking transport encryption (e.g. WEP, WPA, WPA/2, WPA/3)

Lastly, our fourth finding for our first research question is that specialized digital forensics KSAs for wireless network, wireless devices, and wireless metadata are missing entirely from the current NICE Framework.

There is a tremendous amount of WIFI data stored in both mobile devices, laptops, and desktops. Software tools have been written to easily scrape and recover this data and the subject should be included in the bodies of knowledge. For example, both the Microsoft Windows Registry and the Apple OSX Keychain store BSSID names, MAC addresses, and passwords for networks that have been previously accessed, as shown in Figure 13, Figure 14, and Figure 15.

Figure 13: WPA Key Store in OSX Keychain



Forensic tools, such as Cellebrite recover wireless data while analyzing mobile devices such as IOS and Android phones and tablets. Wigle.net, as seen in Figure 16, is a publicly available searchable online database that incorporates geolocation data of WIFI access points based on MAC Addresses and BSSID names.

Figure 14: WPA Keys Recovered from Windows Registry

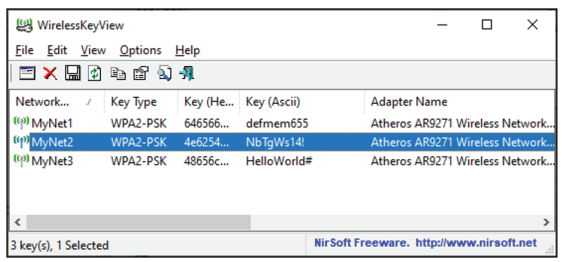


Figure 15: BSSIDs Stored in OSX Keychain

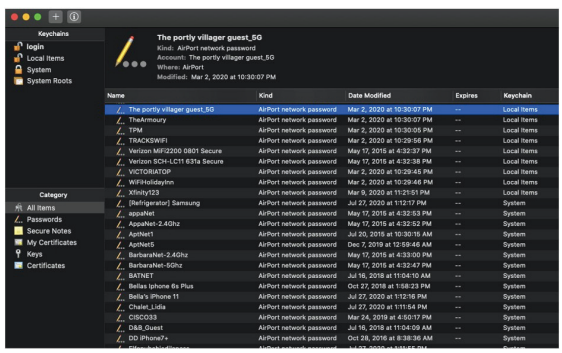
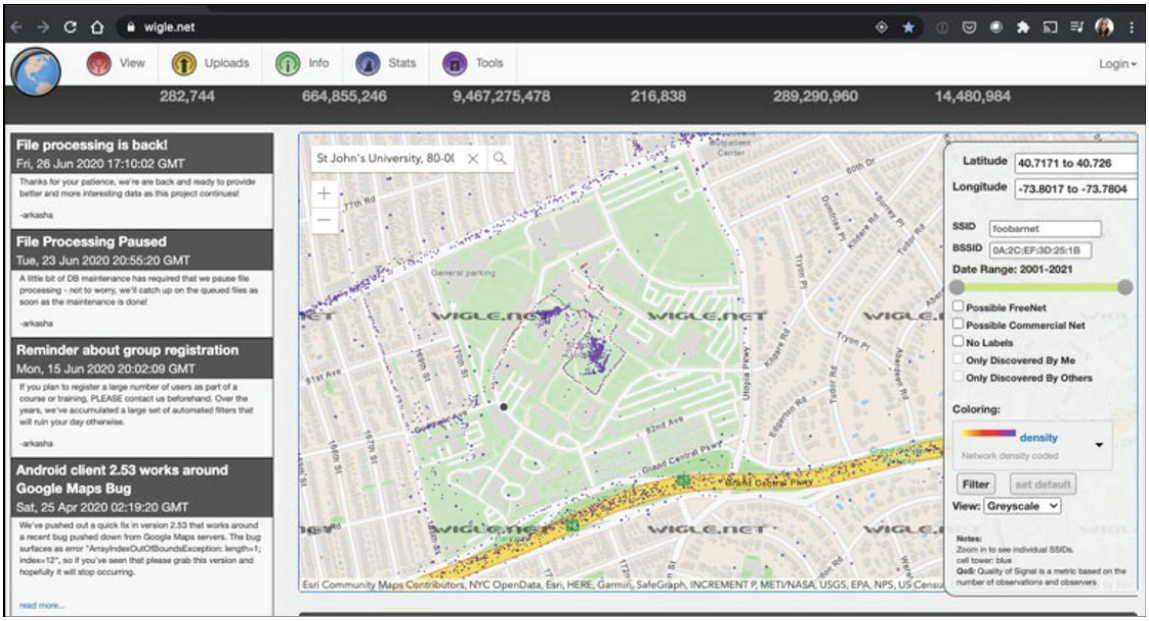


Figure 16: Wigle.net Online Database



Developed Courses to Address Gaps

We have developed two separate courses to address industry gaps in traditional wireless security courses. Specifically, we developed both a Mobile Device Forensics forensic course and expanded an advanced Wireless Security course. We will discuss both in detail.

Mobile Device Forensics Course: The Mobile Device Forensics course is updated each semester offered, as the technology is constantly evolving. Originally, the course included sections covering Palm Pilots, Windows phones, and Blackberry devices, but now centers predominantly on Apple iOS and Android based wireless devices. IoT, wearable, and vehicle based wireless device forensics are also included, as listed in Figure 17.

This forensics-based course sets the groundwork by introducing the iOS and Android mobile operating systems, their structures, and integrated security frameworks. To exemplify the pervasiveness of mobile devices into our everyday life, we have the students forensically examine their own personal cell phones. Students then examine ZTE Prelude Z993 4GB Android phones that each contain an exact pre-built dataset. Students are introduced to and get hands-on experience with (2) industry standard mobile device forensic tools—BlackBag Technologies Mobilyze and Cellebrite Universal Forensic Extraction Device (UFED). The course then pivots into the study of WIFI forensics, wearables (i.e. smart watches, fitness devices, etc.), vehicle forensics (i.e. digital black boxes/ flight recorders) and other IoT devices.

Figure 17: Developed Mobile Device Forensics Course

Topic Coverage in a Mobile Device Forensics Course:
- Introduction to Mobile Forensics
- Understanding iOS Device Internals & Data Acquisition from iOS Devices
- Data Acquisition from iOS Backups, Data Analysis & Recovery
- iOS Forensic Tools
- Understanding Android, setup and Pre-Data Extraction
- Android Data Extraction Techniques
- Android Data Analysis & Recovery
- BlackBag Forensics Mobilyze Operator Instruction
- Certified CelleBrite Operator Certification Instruction
- Certified CelleBrite Operator Exam
- Investigating Wireless Attacks
- IoT, Wearable, and Vehicle Forensics

These topics have applicability across all the NICE workforce categories (Figure 2) and the NIST 800-11 Task Mappings (Table 1), Knowledge Mappings (Table 2), Skills Mappings (Table 3), and Ability Mappings (Table 4).

Wireless Security Course: Each iteration of our developed advanced wireless security course incorporates continual improvement in accordance with ABET (re)accreditation. Recently, we structured the course to be focused on WIFI, but incorporate other wireless technologies in keeping with industry trends on IoT, Bluetooth, and other radio frequency protocols. Our last iteration of the course included the topics listed in Figure 18.

Figure 18: Developed Wireless Security Course

Topic Coverage in a Wireless Security Courses:

- Wireless Technologies and Security: Where have we been (historical context), where we are now (radio frequency spectrum), and managing future wireless risks (risk management).
- WIFI: Architecture and Media Access Control (MAC) Part I - Examining topology, packet structure, packet flow, hardware, drivers
- WIFI: Network Scanning & Enumeration with Kali Linux tools
- WIFI: Network Attacks and Mitigations
- WIFI: Attacks on Clients and Mitigations
- WIFI: Data-In-Motion - Attacks and Mitigations on Encryption
- WIFI: Architecture and MAC Part II – Examining Wireless Router Source Code with focus on Security – Building Custom Firmware
- Cellular Networks: Architecture, Topology, Attacks and Mitigations
- Cellular Networks: Mobile Device Application Security - Attacks and Mitigations
- Bluetooth (IEEE 802.15.1) and other radio frequencies (NFC, RFID, IR, etc.) Security.
- Wireless IoT Security (Zigbee, IEEE 802.15, and ZWave)
- [All Semester] Student presentation on wireless security breaches involving wireless communications

The course spends the majority of the semester on WIFI security, and the remainder of the course focuses on other wireless protocols. The design is for students to understand the different wireless protocols and to learn to research security concerns among all wireless protocols. The course ends with the students building their own custom wireless router firmware. The OpenWrt project is a Linux operating system targeting embedded devices; it provides a fully writable filesystem with package management (OpenWrt, 2020). OpenWrt is a framework to build an application without having to build a complete firmware around it. Figure 19 shows the mini smart router, which is specifically designed through the product business model, to support the installation of custom firmware. Once the firmware is customized as needed, Figure 20 shows the configuration for the firmware build.

Custom firmware is extremely important for wireless security for many reasons. As security risks, attacks, mitigations, and tools change frequently, a longer-lasting learning experience revolves around a hands-on activity to build custom firmware. Top security benefits from building custom embedded system firmware include at least the following: (1) transparency by knowing what the system actually does, (2) transparency by scanning the code for issues and vulnerabilities, (3) implementing overall additional system hardening, (4) implementing new security features, (5) facilitating additional security research, and (6) faster patch deployment as system administrators and users can install custom patches without waiting for the original equipment manufacturer (OEM) to release patches. The students are required to emphasize the ethics around building a system and having super privileges (i.e. root) of the system. Custom firmware development strongly fosters research for newer security mitigating controls to be implemented.

Figure 21 then shows building the actual firmware. Figure 22 shows the output firmware image. Specifically, the figure shows both a fresh custom OpenWrt install image and a custom OpenWrt upgrade image. Lastly, the project computes an integrity check on the files and stores the integrity hashes in the file sha256sums on all the firmware images. Figure 23 shows an image for installing the fresh build in a router under the router configuration graphical user interface (GUI). Many routers enable the download of the current firmware prior to the upgrade. It is also possible to perform a command-line install through ssh-ing into the router and performing the steps via the command-line instead of the GUI.

Figure 19: GliNet Mini Smart Router (OpenWrt, 2020)

Figure 20: Customizing OpenWrt Configuration

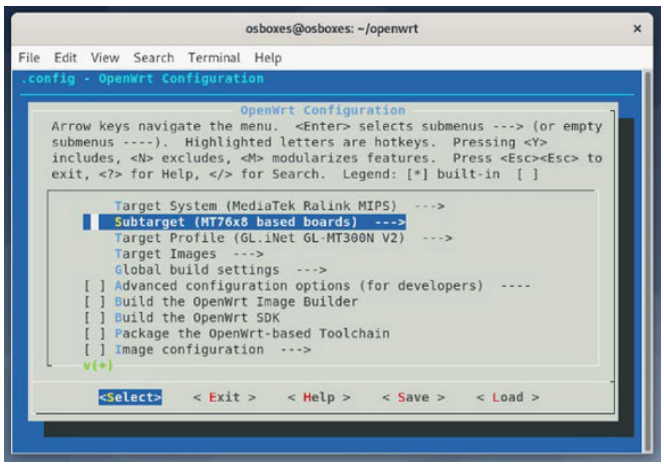


Figure 21: Building Custom OpenWrt Firmware

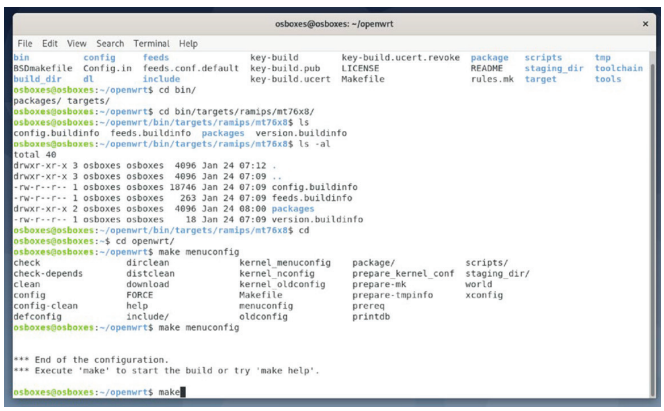


Figure 22: Custom OpenWrt Firmware Images

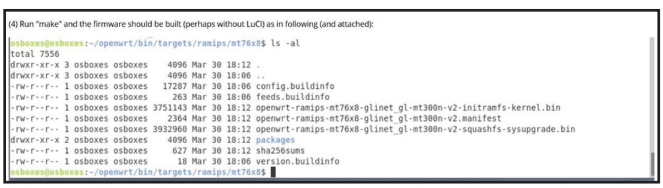
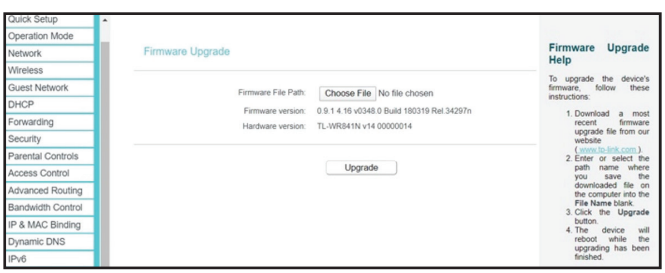


Figure 23: Installing OpenWrt on a Wireless Router



V. Lessons Learned and Future Work

There remains a wireless security educational literature gap. Understanding the limitations and benefits for current frameworks and certifications on wireless security raises fundamental cybersecurity education questions. First, future investigations can improve on the quantity and quality of topics, developing working hands-on labs and understanding key security engineering tasks such as wireless firmware development. Second, future research should test findings from this research through IRB- approved surveys with both industry alumni and local area employers to gain more insights into wireless security educational gaps. Third, while the course covers breaches involving wireless security, future research could comprehensively examine breaches to determine where the gaps in mitigations occurred. Fourth, we are currently developing a Network Forensics course that will include wireless networks. Fifth, future investigations could examine industry-leading conferences such as DefCon, Blackhat and HOPE for gaps in wireless mitigations. These conferences do not include paper publications, so analysis methods for the talks and workshops would need to be developed. As IoT (e.g. ANT, BLE, Zigbee, ZWave, Wireless Sensors, etc.), NFC (e.g. ApplePay, Android NFC, etc.), Bluetooth, Cellular (Mobile Device Security, CDMA, GSM/ EDGE and UMTS/HSPA UMTS, LTE, 5G, etc.), and other wireless securities expand, consumers need a cybersecurity workforce competent in lower risks to the communications and data processed by these wireless technologies.

VI. Implications for Practice

Our findings present implications for practice such as which topics are covered by certification. CISSPs, for example, have very little, if any, specific protocol training. Similarly, the OWSP certification is really geared towards WIFI. Overall, the topic coverage informs the educational background and skills brought into a workplace. As we move more-and-more to IoT, we can clearly see which, if any, topics cover IoT security needs.

VII. Conclusion

This research makes two contributions. First, we examine leading industry certifications with respect to wireless security to gain insights into gaps for the next generation of the NIST NICE framework. We found that certain wireless protocols such as IoT, Apple Pay, Android Pay, NFC, and customer wireless firmware development for embedded systems such as wireless routers, medical devices, and automobiles are currently missing. In addition, we found that certain WIFI attacks and mitigations are missing from the current NICE Framework. Lastly, we found that most industry certifications and the current NICE Framework is missing wireless specific guidance for forensic applications. Second, we found that building wireless security into custom firmware is entirely missing from literature. As such, we integrated the topics into our semester-long wireless course. Overall, this research explores top industry certifications, frameworks, and curriculums to gain insights into the next iteration of the NICE Framework. All organization accept wireless security risks, it is now fundamental that the cybersecurity workforce understands these implicit and explicit risks.

References

3GPP. (2020). *SA3 - Security*. Retrieved from 3GPP: The Mobile Broadband Standard: https://www.3gpp.org/specifications-groups/sa- plenary/sa3-security

ABET. (2020). *ABET Portal.* Retrieved from ABET: https://www.abet.org/

Association for Computing Machinery (ACM). (2020). *Curricula Recommendations.* Retrieved from ACM Portal: https://www.acm.org/education/curricula-recommendations

Budd, I. (2019, December 2). *Offensive Security Wireless Professional (OSWP) review.* Retrieved from Nethemba: https://nethemba.com/offensive-security-wireless-professional-oswp-review/

CompTIA. (2020). *CompTIA Security+ Certification Exam Objectives EXAM NUMBER: SY0-501.* Retrieved from CompTIA: https://www.comptia.jp/pdf/Security%2B%20SY0- 501%20Exam%20Objectives.pdf

CSAB. (2020). *About Us.* Retrieved from CSAB Portal: https://csab.org/about-us/

CSAB. (2020). *CSAB: Leading Computing Education.* Retrieved from CSAB: https://csab.org/

Cybersecurity Curricula 2017: *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.* (2017, December 31). Retrieved from ACM Portal: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Doherty, J. (2016). *Wireless and Mobile Device Security.* Boston, MA: Jones & Bartlett Learning.

Freeman, I. Haigler, A., Schmeelk, S. Ellrodt, L. and Fields, T. (2018) "What are they Researching? Examining Industry-Based Doctoral Dissertation Research through the Lens of Machine Learning," in the 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 1338–1340.

Haataja, K. M. J. (2008). New efficient intrusion detection and prevention system for Bluetooth networks. Proceedings of the 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications. Innsbruck, Austria, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Article 16.

(ISC)² . (2020). Portal. Retrieved from International Information System Security Certification Consortium (ISC)² : https://www.isc2.org/

(ISC)². (2020). *(ISC)² Member Counts*. Retrieved from (ISC)² Portal: https://www.isc2.org/About/Member-Counts

(ISC)². (2020). *Get Familiar with the Exam.* Retrieved from (ISC)² Portal: https://www.isc2.org/exam-outlines

Joint Task Force on Cybersecurity Education (2018) Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, New York, NY, USA.

National Security Agency (NSA). (2020). *National Centers of Academic Excellence.* Retrieved from National Security Agency (NSA) portal: https://www.nsa.gov/resources/students- educators/centers-academic-excellence/

NIST. (2017, August). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework SP 800-181.* Retrieved from NIST Computer Security Resource Center: https://csrc.nist.gov/publications/detail/sp/800- 181/final

NIST. (2020). *Reference Spreadsheet for NIST Special Publication 800-181.* Retrieved from NIST NICE Framework: https://www.nist.gov/file/372581

Offensive Security. (2020). W*iFu Offensive Security Wireless Attacks The Official OSWP Certification Course.* Retrieved from Offensive Security: https://www.offensive-security.com/wifu-oswp/

OffSec Services Limited. (2020). *WIFU: Offensive Security Wireless Attacks - The Official OSWP Certification Course.* Retrieved from Offensive Security: https://www.offensive-security.com/wifu-oswp/

OpenWrt. (2020). *GL.iNet GL-MT300N V2.* Retrieved from OpenWrt Wireless Freedom: https://openwrt.org/toh/gl.inet/gl.inet_gl-mt300n_v2

OpenWrt. (2020). *OpenWrt Wirless Freedom Hompage.* Retrieved from OpenWrt: https://openwrt.org

OWASP. (2020). *M3: Insecure Communication.* Retrieved from Open Web Application Security Project: https://owasp.org/www-project-mobile-top-10/2016- risks/m3-insecure-communication

SANS. (2020). *Cybersecurity Courses & Certifications.* Retrieved from SANS Portal: https://www.sans.org/cyber-security-courses/

Summers, W. C. and A. DeJoie (2004). Wireless security techniques: an overview. Proceedings of the 1st annual conference on Information security curriculum development. Kennesaw, Georgia, Association for Computing Machinery Bhagyavati: 82–87.

Wright, J., & Cache, J. (2015). *Wireless Hacking Exposed: Thrid Edition.* McGraw-Hill Education.

Research Note

Cybersecurity Intelligence: A Novel Information Security Threat Mitigation Approach

Patrick Offor
City University of Seattle, United States

I. Problem Statement

Despite technology and countermeasure investments worldwide, mandatory training and its repeated iterations in organizations, awareness, and education of the threats posed to critical information systems by trusted insiders globally, the exploits and havocs have continued to increase exponentially, rather than diminish. Trusted insiders have continued to threaten our networks and communication infrastructures, in spite of the availability of more capabilities for identifying the culprits, and the incessant prosecution and conviction of malicious actors. In addition, even with the exposure of non-malicious actors in organizations, training and education of employers and employees alike, analysis of costs to individuals and organizations due to cybersecurity losses, and the ubiquitous or plethora of defensive and offensive cybersecurity investments by governments and organizations in technical and non-technical measures, the issue of trusted insiders has continued to increase.

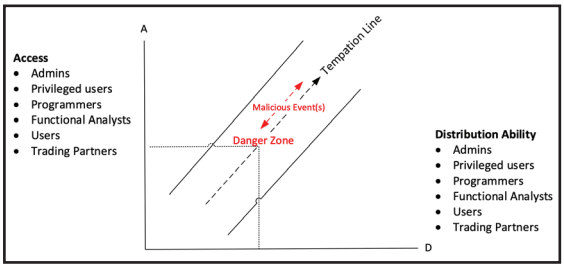
The main reason for such an unavoidable risk emanating from trusted insiders is not farfetched. Although anyone in an organization poses a risk to the organization's critical information, the cost is greater when it happen from those with authorized and privileged access. Organizations have personnel who have physical access to the organization's information systems, technical knowledge of the systems, undetectable distribution capacity of a stolen artifact (data, information, objects, intellectual property), and who understands the organization's cybersecurity mitigation strategy and plan. Therefore, having personnel in organization with such inevitable capacities pose even more significant risks and threats to the organization.

The practicality of insider threats is such that, at any given time, select employees would always have physical access and technical expertise of an organization's critical information systems or infrastructure, and non-suspecting distribution capacity of the compromised artifact as depicted in Figure 1. It is a known fact that information system professionals, depending on their positions, usually would have both the physical access to the systems and the systems' technical knowhow, including the systems' known vulnerabilities and the organization's risk management framework. Crossing the danger zone notation in Figure 1 indicates the point at which an employee, affected by one or more of the cybersecurity trigger indicators, has decided to become an insider malicious attacker, in part, because the opportunity of having access and distribution capacities had presented.

An insider attack originates from a trusted insider, regardless of whether the attack is malicious or non-malicious. Insider threats to organizations can generally be categorized as malicious (an attack by a criminal or malicious insider) or non-malicious (a careless, mistaken, negligent, or intentional but non-malicious attack by an employee, contractor, or otherwise) (Ponemon, 2018). People rather than technology or process, has shown to pose the greatest threat to organizations' critical information systems (IS), information security, or cybersecurity (Gelles & Mitchell, 2015; Greitzer & Hohimer, 2011) because they possess the two perilous elements to cybersecurity vulnerabilities, which are accessibility of the physical systems and technical knowledge of the systems (Archuleta, 2009). As such, the proposed study will conduct a theoretical evaluation of the phenomenon based human behavior theory underpinnings. In this context, people represent employees, contractors, and employers of a company who could otherwise be referred to as trusted insiders or actors

.

Figure 1: A Trusted Insider Becoming an Attacker (adapted from The Insider Threat, 2015)



The difficulty this problem poses to businesses, governments, institutions, and other entities is currently manifested in real-time and in the extant literature. In recent years, attacks by the trusted insiders have been very costly. In 2015, each incident's cost to organizations is estimated at over $144,000, and the resolution of the issues of insider actors cost organizations about $21,000 a day (Securonix, 2015). Out of the 3269 insider incidents in 2017 from 159 organizations in North America, Europe, Middle East and Africa, and Asia-Pacific, 64% were due to negligence by employees and contractors, 23% were from malicious or criminal insiders, and 13% were relating to user credential theft. On average, the total average cost of insider attack for the organizations was $8.76 million in 2017 (Ponemon, 2018). Ron Rockwell Hansen, a former Defense Intelligence Agency (DIA) officer, pleaded guilty to attempted espionage in March 2019 (Cyber Awareness Challenge, 2021).

The issue is that most study on insider attack have if-x-then-y perspectives. They focused heavily on indicators, triggers, activity monitoring, and workplace reporting. They also focused on the attackers' character exhibitions, i.e., whether an attacker exhibits signs of having personality problem, mental disorder, ethical issue, personal or work-related issues, emotional issue, or overdependence (Liang et al., 2016). They also focus on whether the insider attacker has financial problem, is not rational, disgruntled or is socially isolated (Liang et al., 2016). Hence, we argue that although these factors play important roles in the characteristics of insider attacker, the choice of an attacker is more important because it consummates to an attack, as such, the second most critical part of the act other than the act. For that reason, the proposed study will focus more on the decisions or choices of insider attackers.

As the Chief Information Security Officer (CISO) of an organization, an Information Security or Cybersecurity Consultant, or Educator, imagine that you have the capacity to categorize the employees in your organization distinctively into four, based on a predetermine elements of data collected from the employees. And that you have the capacity to assess, identify, and determine the probability of employees' leanings or propensity to becoming insider attackers when affected by any of the already identified insider threat indicators based on the data. That is the kind of intelligence the proposed study could bring to bear. The presupposition is that such a study will support the operationalization of such capacity and would be a gold mine for cybersecurity professionals.

Therefore, the concept espoused in this note aims to provide a novel cybersecurity intelligence capability that can predictively and prescriptively help organizations to identify employees who may have the propensity to cross the danger zone on the temptation line, as illustrated in Figure 1, and become insider attackers or malicious actors when any one or more of the following insider threat indicators manifest itself: divided loyalties, identification, ideologies, revenge, anger tendencies, destructive behavior, adventure, thrilling tendencies, ego, self-image, ingratiation, compulsiveness and/or family problems (U.S. Department of Justice, 2014). It also aims to alert cybersecurity manager earlier for better deployment of mitigation measures and broaden cybersecurity skills and education.

II. Research Questions

The conceptual propositions for this proposed study is based on choice theory. The choice theory underlying principles would be adopted in the study because of its potential ability to illustrate the powerfulness of a substantive and reflective insight of proactiveness, prescriptiveness, and purposefulness in advancing cybersecurity intelligence. In assessing the reasonableness of using choice theory in examining the threat of trusted insiders to cybersecurity, we conducted a search of the relevancy of the theory in the extant literature and in other disciplines using "choice theory" as keyword since this is the first attempt to use it in a cybersecurity setting, at least, to the best of our knowledge. Therefore, the following is a delineation of the theory and a description of the expansiveness and usefulness of the theory to research and practice.

Choice theory "is an internal control psychology; it explains why and how we make the choices that determine the course of our lives" (Glasser, 1998, p. 7). It also explains that human beings are internally motivated to behave; although external stimuli (motivations) inform us, they do not control the specific choices we make or our responses to stimuli. Inherent in choice theory is the argument that all we do, from the beginning of our lives to the end, is to behave and relate (Glasser, 1998). Choice theory "is about making better choices, but we have to understand the reason for the bad choices before we can make good ones" (Glasser, 1998, p. 157).

In describing human behavior, Glasser suggested four inseparable components of each human behavior, i.e., activity, thinking, feeling, and physiology. Since these four components of each behavior work together simultaneously, he referred to it as a total behavior. In other words, Glasser further explained that when we are doing something, we are acting and thinking; that we are feeling something; and that we are breathing, our heart is beating, and our brain is working. Finally, he added that although the inner workings of these components are intertwined, (1) that we have direct control over our actions and thoughts, and (2) that we have indirect control over our feelings and physiology (Glasser, 1998). Therefore, the conceptual framework for the proposed study will anchor in the total behavior. Total behavior hinges on the idea that all behaviors are purposeful, and involve physiology, feeling, thought, and culminate in an act (Glasser, 1998).

Furthermore, choice theory is about human decisions; and how we relate to and gather information from one another, how we relate to or gather information from our organizations, and vice versa. This conception of choice theory is also relevant and suitable because people are the most significant cybersecurity threat. Choice theory will be relevant to gathering cybersecurity intelligence because behaving is relating and because of the need to understand the two relationships in an employer-employee relationship; how an employer behaves toward an employee and how an employee behaves and relates to the employer (Butorac, 2020).

Although choice theory or total behavior has not been used in cybersecurity intelligence literature—to our knowledge, it has been used in many other areas, including reality therapy, economics, sports, and education.

A Google Scholar search for "Choice Theory" indicates that Glasser (1998) has been cited 2,137 times since its publication. There were 724 citations of the theory from 1998 to 2010, and there were 1340 citations from 2011-2020, indicative of a trending interest on it. Equally important is that some of the books and articles that cited the choice theory have over 300-1,700 citations of their own.

Additionally, using "Choice Theory" as a keyword/phrase and selecting "Peer-reviewed (scholarly) journals," "Full Text," and "2015-2020" as limiters or criteria in the Academic Search Premier database, we found 10,069 articles relating to the theory, indicative of the relevancy and the amount of interest in the theory in recent times. Minimizing the criteria will provide greater number of academic journals with choice theory as well.

III. Contribution

First, the outcome of the proposed study will add to the body of knowledge because it will help in answering the question of whether a predictive or prescriptive analysis could foretell an employee's cybersecurity tendencies or behaviors? An information security manager that is armed with employees' cybersecurity tendency intelligence will be better prepared in instituting surgical and appropriate countermeasures to insider threats, risks, and vulnerabilities.

Secondly, the outcome of the proposed study will help in answering the question of the degree to which a predictive or prescriptive analysis would foretell an employee's cybersecurity tendencies or behaviors? Here, the question is whether the juice is worth the squeeze—the proposed study will provide the magnitude of or the significance of such employee's cybersecurity tendencies.

Thirdly, the outcome of the proposed study will assess whether an organization could reasonably minimize its cybersecurity risk and threat exposures when the findings are operationalized. In order words, it will demonstrate that the development of such proposed cybersecurity intelligence is not only theoretical but has applicability and generalization.

Furthermore, if the findings in the proposed study were to come to fruition, it will usher a new dimension to applied research because of its rich real-world application potentials and will further academic inquiry in cybersecurity because

of its social science implications. The potential contribution to the body of knowledge would be (1) to confirm or disconfirm the essence of total behavior or the falsifiability of the concept of total behavior, (2) would help in determining whether personnel in organizations could be categorized such that their cybersecurity leanings when faced with insider threat triggers could be determined, and (3) provide statistical answers to insider threat research problem or the phenomenon of interest.

Typically, some middle to large organizations have over 1,000 employees, as such it is not logical, in fact, it will not be reasonable to individualize each person's total behavior. Hence, the first iteration of the study will categorize the sample subjects in four so that it can be manageable. Each category will be measured against each of the insider threat indicator or triggers in order to extrapolate cybersecurity intelligence. The categorization would be exploratory in nature and will be based on the data collected using a survey instrument.

IV. Rationale

The rationale for this concept is to provide researchers and practitioners with an essential and actionable cybersecurity intelligence since the issue of insider threat has not diminished despite current technical and non-technical solutions available in the market. Secondly, the importance of advancing this concept is because in spite of the rapidity of technology innovation and creativity, and despite the technological capabilities available to organizations, government, and institutions of learning, the issues of trusted insiders have continued to ravage industries around the world.

Additionally, the provision of such intelligence is in line with the Cybersecurity Workforce Framework stipulated in the National Initiative for Cybersecurity Education (NICE). Although the concept that effective cybersecurity or information security risk management (RSK), data administration (DTA), and knowledge management (KMG) are complex schemes, especially in the middle to large organizations, is not novel, there is a need for the establishment of a continuum of efforts toward a better cybersecurity mitigation approach. Moreover, an organization's ability to manage cybersecurity threat and risk largely depends on its capacity to formulate, articulate, and enforce the provisions stipulated in the NICE Framework categories relating, but not limited to Secure Provision (SP), Oversee and Govern (OV), Protect and Defend (PR), and Investigate (IN), among others (NIST SP 800-181).

V. Investigative Approach

We will use exploratory and quantitative research approaches for the study—see research contribution. Discernment and categorization of personnel based on the total behavior can only be achieved based on exploratory inquiry because will be the first of its kind. Furthermore, quantitative approach will be used because of its capacity to determine relationships among variables or constructs and the phenomenon of interest, and because it is predictive in nature. A survey instrument will be used to gather data from subjects among the working population in the U.S. The development of variables or constructs for the study will be based on the total behavior's core principles. Following the initial theoretical investigation, depending on the result, a longitudinal examination may ensue for generalization and further affirmation of the result.

In addition, quantitative analysis tends to explore attitudes and behaviors (Offor, 2016). The first iteration of this study would test the falsifiability of the theory. In other words, the initial objective is to establish that all actions/activities are based on total behavior. In identifying our total behavior categories, we will assess their correlations to provide cybersecurity intelligence. We will then assess how insider threat triggers moderate each total behavior category in relation to insider threat behaviors.

VI. Lesson Learned

The currency of the following observations or lessons learned is one of the motivations for this conceptualization and proposal for a new innovative and creative examination of the phenomenon:

- Cybersecurity education is still evolving because cybersecurity threats are still evolving.
- As our cyber presence increases, governments and organizations alike must advance cybersecurity technical and non-technical solutions and be zealous in crafting the right mix of regulation.
- That our cyber environment will outgrow our physical environment because the

Internet has no boundaries; as such, the need for a safer cyber environment cannot be overstated.

VII. Implication for Practice

The results of the study will indicate that organizations can be better served when they could make reasonable assessments and judgments or have reasonable sets of expectations of their employees' information security or cybersecurity propensities or postures in order to take appropriate mitigation countermeasures. It will help organizations in taking preventative measures to cybersecurity rather than relying on reactive measures.

A successful result will advance cybersecurity intelligence capabilities and provide cybersecurity managers, across the globe, with predictability in their mitigation strategies, plans, and efforts. In addition, a successful result will advance interests in the psychology community, especially for practitioners in the reality therapy.

VIII. Implication for Research

The result of the study will ignite a new frontier in theoretical examinations of the phenomenon of an insider threat since "a theoretical framework is a set of related concepts or constructs formulated based on a given theory to analyze, explain, predict, prescribe, and understand a phenomenon" (Offor, 2016). In addition, a theoretical examination of a trusted insider's issue requires the formulation of a translatable, observable, and empirically testable theory (Offor, 2016). The benefits of a successful outcome from the proposed study will enrich academic research cybersecurity, psychology, and other academic domains because understanding human behaviors is the core to understanding cybersecurity issues emanating from trusted insiders.

IX. Call for Action

We are open to and are looking for research partners, sponsors, and/or participating organizations in order to advance this proposed study.

References

Aldhizer III, G. R. (2008). The Insider threat. *Internal Auditor,* 65(2), 71–73.

Butorac, D. (2020). Choice theory vs. common sense: Relationships. *International Journal of Choice Theory & Reality Therapy, 39*(2), 17–21.

Center for Development of Security Excellence. (2019). Insider threat: Potential risk indicators. Retrieved from https://www.cdse.edu/documents/toolkits-insider/INTJ0181-insider-threat-indicators-job-aid.pdf

Cyber Awareness Challenge. (2021). Retrieved from https://public.cyber.mil/training/cyber-awareness-challenge/

Gelles, M. G., & Mitchell, K. (2015). Top 10 considerations for building an insider threat mitigation program. *Journal of Threat Assessment and Management, 2*(3-4), 255-257.

Glasser, M. D. (1998). Choice theory: A new psychology of personal freedom. New York, NY: HarperCollins.

Greitzer, F.L., & Hohimer, R. E. (2011). Modelling human behavior to anticipate insider attacks. *Journal of Strategic Security, 4*(2), 25-48.

Haystax. (2019). Insider threat report. Retrieved from https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

InfoSecurity. (2018). Top ten cases of insider threat. https://www.infosecurity-magazine.com/magazine-features/top-ten-insider-threat/

Moghaddam, F. M., & Studer, C. (1998). Illusions of control: Striving for control in our personal and professional lives. WestPoint, CT: Praeger.

Liang, N., Biros, D. P., & Luse, A. (2016). An Empirical Validation of Malicious Insider Characteristics. *Journal of Management Information Systems, 33*(2), 361–392.

Offor, P. I. (2016). Examining consumers' selective information privacy disclosure behaviors in an organization's secure e-commerce systems (Doctoral dissertation, Nova Southeastern University).

Ponemon Institute. (2018). 2018 cost of insider threats: Global. Retrieved from https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/ObserveIT-Insider-Threat-Global-Report-FINAL.pdf

Puhakainen, P., & Siponen, M.T. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly,* 34, 757-778.

The Insider Threat—The human aspect: It's emotional. (2015). Retrieved from https://youtu.be/XT1TmxE5NfY

U.S. Department of Homeland Security (DHS). (n.d). Insider threat. Retrieved from https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat

U.S. Department of Justice Security Federal Bureau of Investigation (FBI). (2014). The insider threat. Retrieved from https://web.archive.org/web/20140803163734/http://www.fbi.gov/ about-us/investigate/counterintelligence/insider_threat_brochure

Teaching Note

Does Cybersecurity Education Focus on the Right Things? A Professions Based Approach to Cybersecurity Education and the NICE Framework

Nainika Patnayakuni
Calhoun Community College, United States

Ravi Patnayakuni
University of Alabama in Huntsville, United States

I. Introduction

There exists a continuous shortage of cybersecurity workforce in the country and numerous education and training programs are trying hard to fill the gap between demand and supply of cybersecurity professionals. While organizations continue to spend more on cybersecurity and hire more personnel, at the same time the number of cybersecurity incidents and attacks continues to rise. We need skilled cybersecurity professionals to fill the role of specialists in large organizations, as well as generalists in small to medium size organizations. The primary and urgent problem is to then understand how to structure the training and education of cybersecurity workers so that we produce both the volume and quality of workforce that fills the available cybersecurity roles as well as those that possess the core skills required of a generalist cybersecurity professional that can protect the organizations computing systems and networks. Further such training and education should be able to be used as a scaffolding for developing specialized skills over a period of career or advanced education. To understand what is the core body of knowledge that all cybersecurity professionals must hold, we seek to understand the nature of cybersecurity work. The NICE framework and its revised draft in 2020 (Newhouse et. al 2017, Petersen et. al 2020) provide the foundational elements in describing the nature of cybersecurity work. While there have been previous attempts to formalize cybersecurity education (Burley et al 2017), we look at the nature of work of a cybersecurity professional and use that as the basis of identifying the core body of knowledge and skills that are relevant to the cybersecurity workforce. We then compare these to the specialty areas described in the NICE framework and advance insights for practitioners.

II. Background Research

There is considerable debate on the question of what constitutes a profession and the professionalization of an occupation The developmental and structural models of professionalization are based on how the progression of profession follows a series of predefined steps that include trade associations, university curricula, licensure and a code of ethics. The Computer Science and Telecommunications Board has recommended that the cybersecurity workforce is not ready for professionalization and has come up with a set of guidelines for when professionalizing of the nation's cybersecurity workforce would be appropriate (NRC 2013).

Professions, however, can be defined in other ways besides a structure, form-based definition based on curricula, regulation and licensure. They do not exist in isolation, but each profession has a set of tasks that it performs to fulfill what the society needs, a body of knowledge on which it is based and jurisdictional relationships with other similar or related professions that satisfy similar societal needs. This definition of professions was conceptualized by Andrew Abbott in his 1988 sociological treatise on the system of professions which dealt with the division of expert labor, how professions came into being and the nature of their jurisdictional battles with other professions. Abbott was one of the first to study the role of actual work tasks in defining a profession, the use of abstract knowledge as a basis of professional work, the role of context and client in the legitimization of the profession and the relationship between professions as they wax and wane in power over time. Abbott's definition of professions is that professions are occupational groups that apply abstract knowledge to solve problems. We use this definition of professions to analyze the work of cybersecurity professionals (as defined by the NICE specialty areas) and then use

that as the basis for providing curricular guidance. We recognize that the NICE framework itself is based on a study of cybersecurity work and practice, but we apply a higher order analysis by situating the concept of cybersecurity profession in the context of other professions such as law, medicine, accounting and nursing over time.

Similar to the attempts to identify the need for professionalization of the cybersecurity workforce, there have also been attempts to identify the knowledge, skills and capabilities required for cybersecurity workers. A joint task force of several organizations (ACM, IEEE-CS, IFIP WG 11.8, IS SIGSEC) has identified essential curricular knowledge in various knowledge areas in cybersecurity including data essentials, software essentials, component essentials, connection essentials, system essentials and human, organizational and societal essentials. The coverage of these knowledge areas is based on a thought model that includes cross cutting concepts, and disciplinary lenses. Our conceptual approach is different. What we seek to do is develop a grounded understanding of the work done by cybersecurity professionals based on Abbott's theory of professions, we then compare our understanding of the specialty areas in the NICE workforce framework to see if we can gain new insights that can guide cybersecurity education in the future.

If we examine the history of cybersecurity as a profession, we find its basis in technological change, the use of computers, networks and the Internet. Cybersecurity work is work that objectively did not exist before the advent of computing and the Internet and in that sense may be different from say medicine where the body as an entity has always existed and people have always been getting sick. Further, one can argue that since computers and networks were first used by governments and large corporations, the task itself and its major clients were large companies and agencies. As computing and networking spread to small businesses and individuals the demand for cybersecurity tasks are also exploding in these arenas.

According to Abbots essay on the division of expert labor (1988), professions are occupations based on the application of expert knowledge to tasks and do not exist in isolation, but systems of professions are related to each other. Professional work has three components, diagnosis, treatment and inference. Diagnosis is the process of getting information about reality, while treatment is the process of suggesting recommended solutions. Inference in contrast, is concerned with taking the information from the diagnosis and finding the matching treatment. The work of diagnosis, inference and treatment may be performed by different work roles(specialist) or the same work roles (generalist) in a given profession or organization.

Abbot's work on the development of professional expertise (1988) has been applied to medicine, law as well as information and computer science-based professions. In applying the model of diagnosis, treatment and inference to the cybersecurity profession, we develop an abstract representation of cybersecurity work. Instead of asking the question what cybersecurity work is, as defined in the NICE framework, we ask the question, what does a professional do, based on our understanding of a variety of professions over time. We then apply this bottom up understanding of professional work to NICE categories and specialty areas to advance an analysis of the key skills, and knowledge areas that need to be given primacy for cybersecurity professionals. By looking at cybersecurity work from the outside-in lens of professional work across time, rather than an inside out analysis of cybersecurity categories and specialty areas in the NICE framework we attempt to understand how cybersecurity work is situated in context, in terms of the problems that it solves for users, organizations and society.

III. Towards the Development of a Conceptual Model

Diagnosis is the process of collecting specific information about the problem, information that has been previously defined as important by the corpus of abstract knowledge of the profession. For example, a vulnerability scan would collect information about the vulnerabilities in the software applications but ignore the IT strategy and CISO work role in the data collection process. Abbott calls these processes colligation and classification, where colligation, for example, could be an incident response specialist collecting data about the issues with website availability that a client is having, and this would then paint a picture for the identification of treatment. Classification would be matching this picture with the list of problems that the profession concerns as legitimate problems. This classification

system is then the abstract knowledge that defines the profession. So, classification of the data collected may result in its identification as a denial of service attack. This process of colligation and classification requires a fair amount of judgement, because if there was a direct match between finding the vulnerabilities and recommending appropriate countermeasures, it could be codified so that a lay person could do it and we would not need experts, or it could be easily automated.

The classification system is thus organized not as a logical but a probabilistic hierarchy. A key part of diagnosis is the treatment system, you diagnose only problems which you can fix and lump problems that have a common treatment together. The viability of treatment impacts the diagnosis. So, for example, hardening network perimeter security and implementing strict account management policies are treatments to a wide variety of security threats, and vulnerabilities. Further the classification system does not have a one on one key with colligation and there are various residual problems. No amount of firewalls and defense in depth approaches can solve all security problems. Diagnosis need not be as complex as it seems, because most steps in diagnosis can be skipped as most clients have similar problems. Most pen testers, for example, would run a vulnerability scan because that has the highest probability of identifying common problems. The more complex diagnosis of social engineering risks requires more sophisticated diagnosis that cannot be performed by high probability tools such as a Nessus Vulnerability scanner.

While the diagnosis system collects parsimonious data, the treatment system brings all the complexities of the target system, user or organization, back into the picture. Who the client is, for instance a large company versus a small business, can also determine what treatment is recommended. Treatment can be delegated to lower levels of the hierarchy if it is routine, see for example paralegals and nurses. However, the prestige of the client can also come into play when delegating treatment. So, help desk and tech support specialists can routinely answer lowest level issues, but highly paid consultants are hired to deal with large scale data leakage and fraud.

Another issue is how we measure the outcome of a treatment. Success can be measured with positive outcomes or avoidance of failure and the outcome of cybersecurity is usually measured in terms of avoidance of failure, many of which have a low probability of occurrence. If the outcome of treatment is very easily measurable then a sysadmin could apply all the patches and configure the firewall and you would end up with a secure system. The more complicated and detailed the treatment, the more difficult it is to measure whether the treatment resulted in the avoidance of failure, the more a profession can maintain a jurisdictional stronghold through ambiguity.

Inference is done when there is no direct connection between diagnosis and treatment. Inference works by exclusion or by construction. An incident response specialist that disconnects the infected system from the network while the forensics investigator finds the source of the attacks is working by exclusion. The risk management specialist who completes an assessment of the physical, technical and administrative controls is doing inference by construction. When inference is done over a long period of many time intervals, and there are decisions about controls, configurations and policies made in each time interval with varying probability of success, it results in a long inference chain with compounding probabilities. And the longer the inference chain, the greater the chance that any successful outcome is now based on interference from a variety of constituents and goals of stakeholders such as users, managers, fiduciary agents, public opinion, costs and profitability.

One area where inference is of special significance is in the identification of zero-day vulnerabilities. While several other professions require the practitioner to address cutting edge problems, the cybersecurity profession is unique with regard to its emphasis of trying to maintain a direct connection between security operations and new threats, so as to say ahead of Advanced Persistent Threats and attacker groups. In situations like this, inference is tightly integrated with diagnosis and treatment as once the new vulnerabilities are identified they need to be shared with researchers, vendors and disseminated to users and organizations. In the field of cybersecurity, where there is such a direct and rapid relationship between operations and new research, we believe that the work of inference requires tighter connections between multiple stakeholders and shorter inference chains.

We mapped the categories and specialty areas in the NICE framework to diagnosis, treatment

and inference, which according to Abbott, is what defines professional work. We know that the revised NICE framework draft is removing the hierarchical role of categories and specialty areas, but we decided to define the framework in terms of category areas because it provides an economical model of the types of work that is done in the field of cybersecurity. An overall analysis of categories in the NICE framework indicates that the very roles that are in direct contact with users and clients, such as systems administration, vulnerability assessment and customer service need skills both in diagnosis and treatment. Since the clients are users and business organizations, cybersecurity professional also needs to have an understanding of user psychology and business needs. In other areas too, knowledge of risk, management, workflows, systems thinking, and information assimilation, summarization and presentation would play a key role in defending the organizations computers, networks and information. To that end, it is our counterintuitive argument that the core body of foundational knowledge in cybersecurity should pay equal, if not greater emphasis to interdisciplinary foundational skills in design, information management, presentation, human psychology, politics of goals setting, strategy implementation and change management. We argue that any skills in foundational computing disciplines that do not require judgement and interpretation can easily be acquired in a short period of time and may also be delegated and automated in the future as soon as they can be routinized.

When we analyze the NICE framework categories and specialty areas on the basis of diagnosis, inference and treatment of cybersecurity problems that need to be solved in organizations, we arrive at the classification shown in Figure 1. What this analysis reveals to us is that the majority of work in Cybersecurity is performed at the interface between users, and organizations. For example, performing a threat analysis of foreign intelligence is inferential in nature and tries to develop and deal with abstract knowledge that explains the gaps between diagnosis and treatment. Cybersecurity work such as system administration, secure software development, data administration is treatment that is based on existing models of diagnosis (what is wrong) and treatment classifications (how do we fix it). Treatment is not necessarily routine work or work that requires low levels of judgement. Some treatment work like installing patches or incident response might have a clear playbook and might be routinized while others such as data and knowledge management might require various trials and evaluations to identify the right treatment option.

Many specialty areas require diagnosis and treatment which requires interaction with the client, the user and the business unit. For some work roles, the colligation and classification system for diagnosis and treatment are already established by abstract knowledge. For example, the customer service tech knows the various common ways to solve the problem, while the Cyber investigation and digital forensics expert might require more sophisticated diagnosis of the context before arriving at any conclusions.

The number of cybersecurity specialty areas that require business and user knowledge, along with knowledge in other core areas, for treatment and diagnosis is significant. The question then arises, by training our students for the core knowledge areas in cybersecurity at the expense of business and communication skills, are we hampering the very success of these students in their careers and hindering the effective protection of an organization's information and computing resources?

A case in point is social engineering risks and countermeasures. Phishing is becoming a more and more popular attack vector because organizations are able to implement sophisticated security controls, thus somewhat reducing well known security risks. The training and controls required to mitigate social engineering attacks requires large scale collaboration between users, division heads and top management. Other significant human elements of risk such as insider threats also involve a combination of administrative, technical and physical controls. The success of security professionals in the diagnosis, treatment and inference related to the human element of security is likely to be heavily reliant on their business, communication and emotional intelligence capabilities.

Figure 1: NICE Categories and Professional Work Conceptual Model

Analyze: All-Source Analysis, Exploitation Analysis, Language Analysis, Targets, Threat Analysis	Inference
Collect and Operate: Collection Operations and Cyber Operations	Diagnosis
Collect and Operate: Cyber Operational Planning	Diagnosis and Inference
Investigate: Cyber Investigation and Digital Forensics	Diagnosis and Inference
Operate and Maintain: Customer Service and technical support, Network Services, Data Administration and Knowledge Management, System Administration	Treatment
Operate and Maintain: Systems Analysis	Inference
Oversee and Govern: Cybersecurity Management, Program/Project Management and Acquisition	Diagnosis, Treatment and Inference
Oversee and Govern: Legal Advice and Advocacy, Executive Cyber Leadership, Strategic Planning and Policy	Inference
Oversee and Govern: Training, Education, and Awareness	Diagnosis, Treatment
Protect and Defend: Cyber Defense Analysis	Inference
Protect and Defend: Cyber Defense Infrastructure Support, Incident Response	Treatment
Protect and Defend: Vulnerability Assessment and Management	Diagnosis and Inference
Securely Provision: Systems Architecture, Technology R&D	Inference
Securely Provision: Risk Management, Systems Requirements Planning	Diagnosis and Inference
Securely Provision: Software Development	Treatment
Securely Provision: Systems Development, Test and Evaluation	Diagnosis and Treatment

IV. Conclusion

Cybersecurity curriculum, certification and NICE standards evolved from an analysis of cybersecurity professional work. However, in this note we have put forth the argument that business and user skills are equally, if not more important than cybersecurity knowledge for cybersecurity professionals. This analysis of the extent of diagnosis, treatment and inference in cybersecurity specialty areas is purely conceptual. Future research should identify which part of these specialty areas work roles is involved in diagnosis, inference and treatment. Finally, and most importantly, it would be useful to study successful workers in each of these work roles and correlate that with the proportion of their skills and training in communication, and business as compared to their depth and breadth of knowledge in cybersecurity.

It goes without saying that at the higher level in cybersecurity leadership positions, knowledge of business, communication skills, political landscape, dealing with unstructured information and change management are crucial. However, our analysis of cybersecurity specialty areas identified in the NICE framework based on the theory of professions reveals that even for systems administration, training and development, risk management and customer support an understanding of the client, the user, the business, is absolutely essential for diagnosis, treatment as well as inference. In the case of cybersecurity work, the client whether it is the user, the business unit or an organization requires the sysadmin, the tech support specialist and incident responder to have a deeper level of understanding. Without such understanding, for example, the user may not follow the recommended treatment and practice poor information hygiene thus unwittingly clicking on phishing emails. Without such an understanding, for example, the incident responder and cyber operator would find it difficult to convince the threat actor and the script kiddie to reveal sensitive information.

The implications for small to medium size businesses that do not have a Chief Information Security Officer (CISO) and Security Operations Center (SOC) are even more far reaching. In these organizations there is not a diversity of employees and work roles to specifically fulfil the needs of diagnosis, inference and treatment. When it is left up to a single employee or a small IT department to perform the work of diagnosis, inference and treatment, the importance of understanding the context and the business cannot be underestimated.

One might even argue that we do not need undergraduates with four years of core knowledge in cybersecurity to perform much of diagnosis and treatment. Much of our problems of cybersecurity skills shortage may have the potential to be resolved if we took students well versed in user, communication and business skills and put them through short intense courses in core cybersecurity knowledge areas, similar to the example set by coding boot camps. We might then end up with a cybersecurity professional with high efficacy and might be more rapidly able to meet the shortfall in the cybersecurity workforce.

We know that this is a controversial conclusion based on a conceptual analysis of the nature of cybersecurity work, but we believe that it would behoove us to emulate another profession that is dealing with workforce shortages, namely software development, and its ability to rapidly recruit and onramp workers without degrees by relying on their problem solving skills, coding boot camps and performance based interviews.

References

Abbott, A. (1988). *The system of professions: An essay on the division of expert labor.* University of Chicago press.

Burley, D. L., Bishop, M., Buck, S., Ekstrom, J. J., Futcher, L., Gibson, D., ... & Parrish, A. (2017). Cybersecurity curricula 2017. *Version 0.75 Report*, 12.

Curricula, C. (2017). Curriculum guidelines for post-secondary degree programs in cybersecurity. *A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education.* URL: https://www. slideshare. net/MatthewRosenquist/cybersecurity-curricula-guidelines-for-postsecondary degree-programs (accessed 09.03. 2020).

National Research Council. (2013). *Professionalizing the nation's cybersecurity workforce? Criteria for decision-making.* National Academies Press

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *Nist special publication 800-181, the nice cybersecurity workforce framework.* Technical Report. National Institute of Standards and Technology.

Petersen, R., Santos, D., Smith, M., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework)* (No. NIST Special Publication (SP) 800-181 Rev. 1 (Draft)). National Institute of Standards and Technology.

CYBERSECURITY EDUCATION
SOLUTIONS FOR THE NATION

National CyberWatch Center™
Prince George's Community College
Room 129B
301 Largo Road
Largo, MD 20774

csj.nationalcyberwatch.org