

2022

A Universal Cybersecurity Competency Framework for Organizational Users

Patricia A. Baker

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Computer Sciences Commons](#), and the [Library and Information Science Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

A Universal Cybersecurity Competency Framework for Organizational Users

by

Patricia Baker

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Computing and Engineering
Nova Southeastern University


2022

We hereby certify that this dissertation, submitted by Patricia Baker conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Yair Levy, Ph.D.
Chairperson of Dissertation Committee

7/19/22
Date



Martha M. Snyder, Ph.D.
Dissertation Committee Member


7/19/22
Date



Ling Wang, Ph.D.
Dissertation Committee Member

7/19/22
Date

Approved:



Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

7/19/22
Date

College of Computing and Engineering
Nova Southeastern University

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of
the Requirements for the Degree of Doctor of Philosophy

A Universal Cybersecurity Competency Framework for Organizational Users

by
Patricia Baker
July 2022

The global reliance on the Internet to facilitate organizational operations necessitates further investments in organizational information security. Such investments hold the potential for protecting information assets from cybercriminals. To assist organizations with their information security, The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) was created. The framework referenced the cybersecurity work, knowledge, and skills required to competently complete the tasks that strengthen their information security. Organizational users' limited cybersecurity competency contributes to the financial and information losses suffered by organizations year after year. While most organizational users may be able to respond positively to a cybersecurity threat, without a measure of their cybersecurity competency they represent a cybersecurity threat to organizations.

The main goal of this research study was to develop a universal Cybersecurity Competency Framework (CCF) to determine the demonstrated cybersecurity Knowledge, Skills, and Tasks (KSTs) through the NCWF (NICE, 2017) as well as identify the cybersecurity competency of organizational users. Limited attention has been given in cybersecurity research to determine organizational users' cybersecurity competency. An expert panel of cybersecurity professionals known as Subject Matter Experts (SMEs) validated the cybersecurity KSTs necessary for the universal CCF. The research study utilized the explanatory sequential mixed-method approach to develop the universal CCF.

This research study included a developmental approach combining quantitative and qualitative data collection in three research phases. In Phase 1, 42 SMEs identified the KSTs needed for the universal CCF. The results of the validated data from Phase 1 were inputted to construct the Phase 2 semi-structured interview. In Phase 2, qualitative data were gathered from 12 SMEs. The integration of the quantitative and qualitative data validated the KSTs. In Phase 3, 20 SMEs validated the KST weights and identified the threshold level. Phase 3 concluded with the SMEs' aggregation of the KST weights into the universal CCF index.

The weights assigned by the SMEs in Phase 3 showed that they considered knowledge as the most important competency, followed by Skills, then Tasks. The qualitative results revealed that training is needed for cybersecurity tasks. Phase 3 data collection and analysis continued with the aggregation of the validated weights into a single universal CCF index score. The SMEs determined that 72% was the threshold level.

Patricia Baker

The findings of this research study significantly contribute to the body of knowledge on information systems and have implications for practitioners and academic researchers. It appears this is the only research study to develop a universal CCF to assess the organizational user's competency and create a threshold level. The findings also offer further insights into what organizations need to provide cybersecurity training to their organizational users to enable them to competently mitigate cyber-attacks.

Acknowledgements

The process of completing a doctoral study cannot be done single-handedly. I am extraordinarily grateful to have received incredible support throughout this amazing scholastic journey. I want to thank several people, especially my mom and my late dad, who are always a constant inspiration to be the best I can be. Mom, you are my living legend! To my mentor, my confidant, and my cousin, Fay Simpson, thanks for supporting me in every step of my life. I am blessed to come from the bloodline of a supportive family who constantly checks on me: "How far are you with this dissertation?!" To all my younger family members namely, Theo, Christopher, Nia, Darren, Zane, Ashley, Allie, Lorenzen, Jaheem, Jahi, and those yet to be born, this quest is an example for you to follow.

I thank profusely all the staff at NSU Writing Center, especially Jane Harrington and Nikki Chasteen, for your kindness and cooperation throughout my study. I also want to thank Krystopher Knight at the NSU OITT department for his creativity and patience.

To my loudest cheerleaders, Jada, Chris, and Valerie, thanks for your prayers and constant encouragement. I heard you!

I owe a tremendous debt of gratitude to my dear friends, Donna, Joan, Karen, Nathan, Christine, Jenine, Abdul, Ms. Jean, and Richard S., for your constant encouragement throughout my study.

It is my privilege to thank my friend Tommy Pollack. Tommy, you are my pillar! Every doctoral student will need a Tommy Pollack to get them through this scholastic journey.

To my NSU family, thanks for your kindness, especially Vasilka Chergarova, Mel Tomeo, John McConnell, Bob Jones, Celestine Kemah, Amy Antonucci, Javier Coto, Tyler Pieron, and Ahmed Alattas.

To my employer, thanks for the benefits you provided to the employees to further our education. Your investment played a significant role in this dissertation. To my current and former coworkers, thanks for your continuous encouragement.

Thanks to all of the SMEs who completed my surveys. I am grateful for your participation!

I am extremely thankful to my committee members, Drs. Snyder and Wang, for their remarkable guidance and support from my first day at NSU!. Your scholarly advice and scientific approach have helped me to a great extent to complete my dissertation. I love receiving support from such indomitable women who paved the way for me.

I owe a deep sense of gratitude to my dissertation chair, Dr. Levy, for his extraordinary interest at every stage of this research. Your support and influence on me transcends this dissertation. You believed in me more than I did. Without your assistance, guidance, and expertise, this

dissertation would not have happened. I am indebted to you for the doors you have opened for me. Working with you is a privilege and an honor.

Table of Contents

Abstract ii
List of Tables vii
List of Figures ix

Chapters

1. Introduction	1
Background	1
Problem Statement	2
Research Goals	7
Research Questions	10
Relevance and Significance	11
Relevance	11
Significance	12
Barriers and Issues	12
Limitations and Delimitations	13
Limitations	13
Delimitations	14
Definition of Terms	14
Summary	16
2. Review of the Literature	18
Introduction	18
Cybersecurity Workforce	18
Cybersecurity Knowledge	28
Definition of Knowledge	28
Cybersecurity Knowledge Units	31
Cybersecurity Skills	44
Skills Defined	44
Organizational Users' Cybersecurity Skills	46
Cybersecurity Abilities	61
Abilities Defined	61
Organizational Users' Cybersecurity Abilities	63
Cybersecurity Tasks	71
Activity Theory	71
NCWF Tasks	72
National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) Literature	79
Competency	81
Competency Defined	81
NIH Competency Framework	84

Cybersecurity Competency	85	
Summary of What is Known and Unknown	88	
3. Methodology	90	
Overview of Research Design	90	
Research Method	90	
Research Design	92	
Phase 1 – Survey Instrument and Measures		94
Survey Instrument Development	94	
Selection of the SMEs	95	
Reduction of the KSTs	96	
Instrument to Validate KSTs	96	
Main Data Collection – Quantitative Data	96	
Main Data Analysis – Quantitative Data	97	
Phase 2 – Qualitative Data	98	
Qualitative Data Collection	99	
Qualitative Data Analysis	100	
Reliability and Validity of the Qualitative Data Analysis	101	
Integration of Quantitative and Qualitative Data	102	
Phase 3 – Identification of KST Weights and Threshold Level	103	
KST Weights	103	
Threshold Level	104	
Validity and Reliability	105	
Validity	105	
Reliability	106	
Sample Size	107	
Pre-Analysis Data Screening	110	
Resources	111	
Summary	112	
4. Results	114	
Overview	114	
Phase 1 – Instrument Development Findings		114
Quantitative Data Analysis	117	
Knowledge Units	117	
Skills	120	
Tasks	122	
Phase 2 – Qualitative Data Results		124
Knowledge Units	127	
Skills	129	
Tasks	130	
Integration of Quantitative and Qualitative Data Analysis		132
Knowledge Units	132	
Skills	133	

Tasks	134	
Phase 3 – Identification of KST Weights and Threshold Level Analysis		134
Data Screening	134	
KST Weights	135	
Threshold Level	138	
Summary	141	
5. Conclusions, Implications, Recommendations, and Summary		143
Conclusion	143	
Discussion	144	
Implications for Practice	145	
Implications for Research	145	
Limitations	146	
Recommendations and Future Research		146
Summary	147	
Appendices		
A. Phase 1 Proposed Checklist of KSTs for the CCF	149	
B. Phase 1 Proposed CCF – Competency Instrument	155	
C. Phase 2 Qualitative Data Collection Participant Letter	163	
D. Phase 2 Structured Interview Protocol	170	
E. Phase 2 Invitation Letter to Participate in Semi-Structured Interview	172	
F. Phase 3 Proposed CCF – Aggregated Score Development Instrument	173	
G. Institutional Review Board (IRB) Approval Letter	175	
References	177	

List of Tables

Tables

1. Summary of Cybersecurity Workforce	26
2. Summary of Knowledge Defined Literature	30
3. Summary of Cybersecurity Knowledge Units Literature	41
4. Summary of Skills Definition Literature	45
5. Summary of Cybersecurity Skills Literature	59
6. Summary of Abilities Defined Literature	62
7. Summary of Organizational Users' Cybersecurity Abilities Literature	69
8. Summary of Cybersecurity Tasks Literature	78
9. Summary of Competency Defined Literature	83
10. Summary of NIH Competency Framework Literature	87
11. Summary of the NCWF (NICE, 2017) Spreadsheet with KSTs	95
12. Summary of the Total Technical KSTs	115
13. Summary of the Total Non-Technical Approved KSTs from the SMEs	115
14. Summary of the Accepted Non-Technical KSTs Adapted from the NCWF (NICE, 2017) for the Survey Instrument	116
15. Quantitative Demographics of SMEs	116
16. Results of the SMEs' Assessments of the Knowledge Units	118
17. Results of the SMEs' Assessments of the Skills	120
18. Results of the SMEs' Assessments of the Tasks	122
19. Qualitative Demographics of SMEs	125

20. Summary Scores Weighted Average and Standard Deviation	135
21. Summary Average Threshold Level	139
22. Summary of Entry Level Cybersecurity Certification Programs	141

List of Figures

Figures

1. Cyber Domain System 24
2. Knowledge Creation Nodes 29
3. The Stages of Skill Acquisition 45
4. Cybersecurity Mitigation Activity 71
5. Research Design Process for Development of a Universal CCF 94
6. Summary Scores Weighted Average 136
7. Summary of the Competency Threshold Level 140

Chapter 1

Introduction

Background

Cybersecurity is now the core of organizational infrastructure that academic institutions, organizations, and public and private sectors can no longer ignore (Solms & Solms, 2018). Cybersecurity incidents to organizations and institutions resulting from data breach involve more than stolen data, financial damage, and regulatory fines (James, 2018). According to James (2018), the hidden cost, such as negative publicity and loss of intellectual property useful to competitors, holds the potential to jeopardize an organization's competitive advantage. A plethora of research on cybersecurity, as well as organizational initiatives, have been conducted, and the argument can be made that much more must be done to mitigate cyber-attacks (Conti & Fanelli, 2019). Organizations' capabilities to safeguard their information assets significantly relate to organizational users' readiness and competency (Alonge et al., 2019; Brillingaite et al., 2020). This research study addressed the need for further empirical research and provided a competency framework for organizational users' cybersecurity Knowledge, Skills, and Tasks (KSTs). The research findings from this study are significance to the cybersecurity body of knowledge while providing researchers and practitioners an understanding of organizational users' cybersecurity readiness and competency.

Although research has been conducted utilizing the NIH competency framework in the medical field and other disciplines, a paucity of research was available to determine the competency of the organizational users referencing the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF). Furthermore, scant research

was available on the validity and instrument development for such measurement. The instrument development consisted of consensus from Subject Matter Experts (SMEs) using the explanatory sequential mixed-method.

Problem Statement

The research problem that this study addressed was the exploitation of organizational information security caused by limited cybersecurity competency of users that causes significant financial losses, data breaches, and negative publicity to organizations (Hanus & Wu, 2016; James et al., 2013; Torten et al., 2018). The following definitions assisted in explaining the research problem. *Cybersecurity* is defined as a “computing-based discipline involving technology, people, information and processes to enable assured operations in the context of adversaries” (Joint Task Force on Cybersecurity Education (JTFCB); 2017, p. 16).

Organizational users’ cybersecurity competency is dependent upon their KSTs that can be demonstrated tasks, which prior literature has reported to be inadequate (Ani et al., 2019; Carlton & Levy, 2017; Ikeda et al., 2019). *Organizational users* are any employees who utilize computers in their day-to-day jobs (Yang et al., 2015). Nonaka (1994) noted that knowledge can be classified as explicit and tacit. *Explicit knowledge* is easily transferred, reproduced, and codified (Nonaka, 1994). *Tacit knowledge* is a body of facts or information that organizational users know from within and is very difficult to codify or translate into an explicit documentation (Nonaka, 1994). A social engineer or hacker uses their tacit knowledge to manipulate organizational users into divulging information until their desired results are achieved (Hatfield, 2018). *Skill* is described as the ability to do something well (Levy & Ramim, 2015). Specifically, Carlton and Levy (2017) noted that cybersecurity skill “is an individual’s technical ability,

knowledge, and experience surrounding the hardware and software required to implement IS security for mitigating a cyber-attack” (p. 18). *Tasks* are defined as “a specific defined piece of work that, combined with other identified tasks, composes the work in a specific specialty area or work role” (NICE, 2017, p. 6). *Competency* is defined as “the capability of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position” (NICE, 2017, p. 10). Dodel and Mesch (2019) maintained that cyber-attacks present a threat to organizations, and even the most knowledgeable as well as skilled organizational users fall prey to cyber-attacks, let alone organizational users with limited cybersecurity knowledge and skills. Additionally, Contech and Schmick (2016) reported that cyber-attacks dominate the United States news headlines; former Federal Bureau of Investigation (FBI) Director, James Comey, confirmed that cyber-attacks surpassed physical terrorists’ attacks on the United States; and cyber-attacks are increasing exponentially.

Limited cybersecurity skills of organizational users are a common problem, according to several researchers (Blackwood-Brown et al., 2019; Carlton et al., 2019; Nilsen et al., 2017). Within the healthcare industry, the elderly population is among the most susceptible for cyber-attacks because of their limited cybersecurity knowledge and skills (Blackwood-Brown et al., 2019). Likewise, Nilsen et al. (2017) noted that organizational information systems users lack cybersecurity knowledge and skills, a vital component to mitigate cybersecurity threats. Carlton et al. (2019) noted that cybersecurity threats to organizations are a result of human errors owing to poor cybersecurity skills. Contech and Schmick (2016) concluded that new employees commit the majority of human errors in organizations, followed by clients and customers with hackers

aiming at their vulnerabilities. Organizational users with limited or no cybersecurity skills are naïve and more likely to fall prey to social engineering. Social engineering is email related scams to trick organizational users into divulging personal information, intentionally harming computers by downloading malicious files, and are a serious threat to cybersecurity (Contech & Schmick, 2016; Molinaro & Bolton, 2018). Additionally, Junger et al. (2017) pointed out a vulnerability in organizational users in their inability to prevent social engineering because of a lack of knowledge. In most cases, organizational users do not know of the types of information that are useful for attackers. Unfortunately, the most significant impact of organizational users' lack of cybersecurity knowledge and skills results in major financial losses to companies (FBI, 2018). The FBI (2018) reported that the losses from Business Email Compromise (BEC) have increased from \$5 billion in 2017 to \$12 billion in 2018, and from \$37 billion in 2019 to \$43 billion in 2022 (FBI's Internet Crime Complaint Center (IC3), 2022). Furthermore, according to the FBI's IC3 (2018), historical data revealed in 2018 that \$2.71 billion in identifiable victim losses were the result of limited cybersecurity knowledge and skills. The increase in financial losses owing to cybersecurity attacks can disrupt the viability of an organization, for example, as in the collapse of Ashley Madison (Sallos et al., 2019).

Cybersecurity threat has grown significantly and is a major challenge for organizational users (Yang et al., 2015), online retail organizations (Shah et al., 2019), and the financial market (Renaud et al., 2018). The common denominator among the researchers is that organizational users lack the knowledge or "know how" to mitigate cybersecurity threats (Mamonov & Benbunan-Fich, 2018; Shah et al., 2019). Renaud et al. (2018) noted that organizational users' limited cybersecurity competency compromises security because of their dismissal of

cybersecurity protocols. Subsequently, historic records provide solid evidence that limited cybersecurity competency causes data breaches in organizations, which is part of the human factor in cybersecurity (Ani et al., 2019).

The IC3 (2018) defined a data breach as “when sensitive, protected or confidential data belonging to a well-known or established organization is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so” (p. 15). Smith et al. (2018) pointed out that hospitality, retail, and health industries are major targets of data breaches given the volume of personal data collected from these industries that are operating across multiple channels, and organizational users are lacking cybersecurity competency to manage the large volume of personal data across multiple channels. Often, personal data are stored on old computer systems lacking cybersecurity control, thereby creating a passage for hackers to take advantage of organizational users’ limited cybersecurity competency (Smith et al., 2018). For example, Zhang et al. (2019), as well as Chen and Fiscus (2018) noted that data breaches in the hospitality industry are a severe concern affecting major corporations to single properties because of malicious software installed on front desk processing systems that compromise customers’ personal data and cause business e-mail compromise. Repeat customers are no longer booking hotel reservations where data breaches occurred but are instead booking hotels that have more effective cybersecurity practices, thus, negatively impacting revenues as well as organizations’ reputations (Zhang et al., 2019).

Numerous researchers contended that organizational users are the weakest link when protecting companies’ information assets (Alshare et al., 2018; Carlton & Levy, 2015; Connolly et al., 2017; Merhia & Ahluwalia, 2019; Shropshire et al., 2015). Furthermore, Connolly et al.

(2017) noted that organizations have invested in technologies to mitigate cybersecurity malpractice, but the fundamental cause of the security problems is the organizational users' limited cybersecurity competency. Organizations have invested in Security Education, Training, and Awareness (SETA) programs to bring their users up to speed on appropriate cybersecurity practices (D'Arcy et al., 2009). However, Sabillon et al. (2019) contended that SETA programs have been failing to educate the organizational users to recognize, block, or report cybersecurity threats within the organization. As a result, additional empirical research on organizational users' cybersecurity knowledge, skills, and competently completing tasks is warranted.

The Center for Strategic and International Studies (CSIS; 2011) noted the slowness with which the United States Government (USG) developed safety measures for steamboats, automobiles, and air travel. The CSIS (2011) reported that automobile safety rules were implemented after half a century of strong opposition. Unfortunately, cybersecurity cannot wait decades for the government to develop safety rules due to the massive increases of loss of revenue and intellectual property that organizations suffer year after year (FBI, 2018). Similarly, Vogel (2016) explained that U.S. President Barack Obama, described cybersecurity as a "human capital crisis," and the expansion of cyber KSTs is of paramount importance (p. 34). In much the same way as lawmakers introduced safety measures for airlines and automobiles through KSTs (Hemenway, 2001), the development of a cybersecurity competency framework can be approached through KSTs to mitigate cyber-attacks. Additionally, the National Institute of Health (NIH; 2019) noted that competencies should include KSTs, which are a requirement for organizational users to be successful on the job and should use a competency framework to universally quantify organizational users' competencies.

To address cybersecurity threats, Obama issued an Executive Order to improve the critical infrastructure of cybersecurity (Executive Order No. 13,636, 2013). Executive Order No. 13,636 (2013) called for the development of a risk-based cybersecurity framework detailing a set of best practices and industry standards to assist organizations in mitigating cybersecurity risk (National Institute of Standards and Technology [NIST], 2014). NICE (2014) expanded its publication NCWF, thus, developing an interdisciplinary reference list outlining the nature of cybersecurity work, including KSTs. KSTs are the driving forces that strengthen cybersecurity posture in organizations (NICE, 2017). One major drawback of the NCWF (NICE, 2017) is a lack of structured guidelines to validate the competency that assess the knowledge, skills, and competently completing tasks of organizational users to bring significant cybersecurity threat mitigation benefits to organizations (Carlton & Levy, 2017; Dodel & Mesch, 2019; Shah et al., 2019). Furthermore, Sallos et al. (2019) contended that to manage cybersecurity threat mitigation among organizational users, one must effectively manage knowledge limitations and reduce the dependency on intuition by creating a way to measure organizational users' cybersecurity competency. Therefore, it appears that the introduction of a universal cybersecurity competency framework to provide structured guidelines to determine the competency that assess the KSTs of organizational users was warranted. Such a framework has the benefit of strengthening the cybersecurity posture in the public and private sectors.

Research Goals

The main goal of this research study was to design, develop, and validate a universal Cybersecurity Competency Framework (CCF) that included a measure to determine the demonstrated cybersecurity knowledge and skills through the NCWF (NICE, 2017) as well as

tasks of organizational users to identify their competency. Ben-Asher and Gonzalez (2015), Furnell et al. (2017), Kouttis (2016), and Lin et al. (2017) demonstrated the need for such a competency framework. Ben-Asher and Gonzalez (2015) found that novice organizational users lacked the technical knowledge to detect cyber-attacks. Furnell et al. (2017) noted a skill shortage in cybersecurity and stated that even organizational users with professional as well as advanced degrees needed to hone their cybersecurity skills. Additionally, Kouttis (2016) recognized a dearth of knowledge and skills in cybersecurity, suggesting the government should act upon the shortage at the early stages of education and continue throughout college. Thus, building organizational users' cybersecurity knowledge and honed skills at an early age prepare them for future employment. Lin et al. (2017) noted that as technology advances, access to knowledge is readily available, and organizational users have to be open-minded as well as solution oriented. Mora et al. (2018) stated that organizational users should be encouraged to utilize more knowledge-building principles by taking the initiative to improve their knowledge and skills. However, it appears that currently no precise competency measure exists in cybersecurity, which is the key outcome of this research study. Competency is not a new concept because it has been adopted in other fields, such as employee management (Soundaram & Pon-Reka, 2018), organizational management (Vargas-Halabi et al., 2017), and social justice (Lane, 2019). NIH (2019) defined a competency as "as one's ability to demonstrate a competency on the job" (para. 1).

The competency was adjusted and validated in the context of cybersecurity based on the feedback from a panel of SMEs. SMEs are individuals knowledgeable and skilled in a particular area (Guzys et al., 2015). The competency was needed to help organizational users compare their

current cybersecurity level to that of higher-level cybersecurity performers (NIH, 2019; Nilsen et al., 2017; Soundaram & Pon-Reka, 2018). The validation of the competency framework helped organizations leverage the cybersecurity KSTs of organizational users because the competency required differs (NIH, 2019; Podmetina et al., 2018; Soundaram & Pon-Reka, 2018).

The first goal of this research study was to identify the *knowledge units* (KUs) for the cybersecurity competency of the organizational users as validated by SMEs. KUs are the fundamental ways to measure knowledge (Nilsen et al., 2017). The identification of KUs for the CCF was needed to help execute the tasks required for cybersecurity mitigation from all organizational users (NICE, 2017). The strengths and weaknesses in KUs were identified so that organizations could better prepare for training and to assess cybersecurity competency of their employees (NICE, 2017; Nilsen et al., 2017; Soundaram & Pon-Rek, 2018).

The NCWF (NICE, 2017) appears to be significant to organizations, as it helps with inventory management of their cybersecurity workforce, identifying the training needed to develop KSTs, and developing the necessary talent for cybersecurity work roles. Additionally, the NCWF (NICE, 2017) covered all the salient specialty areas relating to cybersecurity work and grouping them into specific categories to aid in communication about cybersecurity responsibilities. Even though the NCWF (NICE, 2017) covered all specialties areas, organizational user's cybersecurity skills needed to be categorized for the universal CCF. Thus, the second goal of this research study was to identify the NCWF (NICE, 2017) *skills* for cybersecurity competency of the organizational users relevant to the universal CCF and validated by SMEs. The identification of the skills for the universal CCF was needed to help organizational users to perform tasks well, help organizations with communication about cybersecurity responsibilities, and support

organizations in mitigating cyber-attacks (NICE, 2017; Nilsen et al., 2017; Podmetina, et al., 2018).

The third goal of this research study was to identify the *tasks* from the NCWF (NICE, 2017) applicable to the cybersecurity competency of the organizational users relevant to the universal CCF and validated by SMEs. Identifying the KSTs for the universal CCF was necessary given that identification of KSTs helped organizations manage the cybersecurity competency (Dimov, 2017; Lane, 2019; Telha et al., 2016). The fourth specific goal of this research study was to determine the weights of the previously validated NCWF (NICE, 2017) KSTs for the development of an aggregated score for the universal CCF. The final specific goal of this research study was to determine the threshold levels for the aggregated score of the universal CCF and validated by SMEs. The threshold levels was necessary to quantify the minimum percentage point for an organizational user to be considered cybersecurity competent.

Research Questions

The main research question that this study addressed was: What are the organizational user's competency and KSTs needed for the validated universal CCF? Furthermore, the research questions that this study addressed were as follows:

RQ1: What are the specific NCWF *KUs* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ2: What are the specific NCWF *skills* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ3: What are the specific NCWF *tasks* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ4: What are the SMEs' identified NCWF KSTs weights for the development of an aggregated score for the proposed universal CCF?

RQ5: What are the SMEs identified threshold levels for the aggregated score of the proposed universal CCF?

Relevance and Significance

Relevance

The purpose of this research study was to utilize a unique way to address the exploitation of organizational information security owing to limited cybersecurity competency from organizational users. Several studies provided novel ways, such as a socio-technical system (Malatji et al., 2019) to address the problem, yet in 2019 the FBI reported a loss of \$37 billion in the exploitation of limited cybersecurity resulting from financial losses, data breaches, and negative publicity. Jajodia et al. (2017) pointed out that technological advances allow cybercriminals to explore networks to identify vulnerabilities among organizational users. These vulnerabilities are a potential challenge to organizational users already limited cybersecurity competency, thus, requiring a continuous need to assess and improve organizational users' cybersecurity competency. Cybersecurity is far-reaching, and as a result, the European Committee for Standardization (CEN, 2019) created an e-competence framework "using a common language for competences, skills, and knowledge that can be understood across Europe" (para. 1) for overarching policies for training and development to help higher level professionals with information communication technology. Currently, the European e-commerce model demonstrates limited applicability to address specific everyday cybersecurity threats outlined in NCWF (2017) for organizational users. The creation of a universal CCF helped to categorize

organizational users' cybersecurity competency to create cybersecurity structures and training for organizations, thus warding off cyber-criminals' malicious attacks (Jajodia et al., 2017).

Significance

This research study is of significance because previous studies, particularly in the nursing profession, have used a competency to meet organizational requirements (Cunningham et al., 2007; Dimov, 2017; Podmetina et al., 2018). Franklin and Melville (2015) noted that competency has been used in the nursing profession, and demonstration of competency is a necessity in healthcare organizations. Similarly, a demonstration of the cybersecurity competency was used as a necessity to identify gaps in organizational users' cybersecurity competency (Cunningham et al., 2007). Also, organizations are able to use the universal CCF to effectively manage organizational users' cybersecurity KSTs to align with the organization's cybersecurity policy to reduce cybersecurity risks (Meyer, 2019). Third, utilizing the universal CCF provides a complete overview of the organizations' cybersecurity landscape, thus, giving organizations the opportunity to effectively manage their cybersecurity policy (Dimov, 2017). The significance of this research study is critical as a result of Obama's warning that cybersecurity is a "human crisis" that affects both national and corporate security (Executive Order No. 13,636, 2013).

Barriers and Issues

This research study encountered several barriers. SME responses solely drove the data collection for this research study. According to Hasson and Keeney (2011), low participant rate of SMEs holds the potential of threatening the internal validity. Mullen (2003) asserted that pioneering researchers used very small number of panel SMEs. Therefore, this research study

employed a large number of SMEs to maintain the internal validity of the research. Another barrier related to the low response rate and high attrition rate. Walker and Selfe (1996) contended that 8% was an unacceptable response rate, while 100% was acceptable. However, they noted the rigor of a consensus requires that a “70% minimum response rate should be achieved” (p. 41). Moreover, the attrition rate is likely to pose an external threat if many SMEs dropout of the research (Mullen, 2003). To mitigate the attrition rate, Avella (2016) noted that the prospective SMEs be aware of the time commitment and their level of expectation during the recruitment process. Thus, during the recruitment process, the SMEs were notified of the time commitment and participation requirement during the research process.

Rowe et al. (1991) pointed out that the SMEs’ level of expertise and agreement significantly influenced the study's validity. Hogarth (1978) posited that a panel of SMEs with different expertise most likely created a validity problem if no attempt was made to determine their specific area of expertise. Rowe et al. (1991) further noted that a possible barrier happened when SMEs changed their agreement to conform to the group instead of changing their opinion, thus threatening the internal validity. A final barrier was locating and identifying the SMEs for the research. Therefore, to overcome these barriers, we utilized the CAE Forum to provide a talk about the study and solicit SMEs from the CAE community, as well as the cybersecurity industry.

Limitations and Delimitations

Limitations

The SMEs’ level of commitment to the research was a potential limitation. The SMEs were likely to drop out of the research because of passage of time. Therefore, all efforts was made to

mitigate the limitation. The likelihood of low SMEs participation was a limitation to research. Thus, the recommendation from the literature review was to notify the SMEs of the time requirement and their participation to mitigate this limitation. Another potential limitation was SMEs located in one specific location. To mitigate this limitation, the SMEs were pooled from academic institutions, as well as public and private sectors from different geographical locations.

Delimitations

One of the main delimitations of this research was the commitment required from the SMEs necessary for data collection. The research relied upon SMEs' feedback from the survey. SMEs worked with a large dataset requiring extended time to complete the rounds. The SMEs were informed about the extended time taken to complete the survey and their commitment to the process was necessary.

Definition of Terms

The following represent definitions and terms referenced throughout the research.

Ability – “is competence to perform an observable behavior or a behavior that results in an observable product” (NICE, 2017, p. 6).

Business Email Compromise – “is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments” (ICE, 2018, p. 25).

Competency – “the capability of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position” (NICE, 2017, p. 10).

Cybersecurity – “computing-based discipline involving technology, people, information and processes to enable assured operations in the context of adversaries” (JTFCE, 2017, p. 16).

Data Breach – “when sensitive, protected or confidential data belonging to a well-known or established organization is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so” (ICE, 2018, p. 15).

Explicit Knowledge – “refers to knowledge that is transmittable in formal, systematic language” (Nonaka, 1994, p. 16).

Knowledge – “Knowledge is defined as a justified belief that increases an entity’s capacity for effective action” (Alavi & Leidner, 2001, p.109).

Organizational Users – are any employees who utilize computers in their day-to-day jobs (Yang et al., 2015).

Reliability – “occurs when a test measures the same thing more than once and results in the same outcomes” (Salkind, 2018, p. 88).

Skill – “a combination of ability, knowledge, and experience that enables a person to do something well” (Boyatzis & Kolb, 1991, p. 280).

Social Engineering – “the different ways that cybercriminals or malicious groups exploit weaknesses in organizations, systems, networks, and personal information used to enable a later cyberattack” (JTFCE, 2017, p. 53)

Subject Matter Experts – “individual . . . at the top of their field of technical knowledge, interested in a wide range of knowledge not only in their own field but everything around it” (Skinner et al., 2015, p. 33).

Tacit Knowledge – “has a personality quality, which makes it hard to formalize and communicate” (Nonaka, 1994, p. 16).

Task – “is a specific defined piece of work that, combined with other identified tasks, composes the work in a specific specialty area or work role” (NICE, 2017, p. 6).

Vulnerability – “a potential weakness in an asset or its defensive control system(s)” (Whitman & Mattord, 2018, p. 14).

Summary

This research addressed the cybersecurity threats to organizational information security and financial losses caused by organizational users' limited cybersecurity competency. To mitigate the cybersecurity threats levied against organizations, this research aimed to design, develop, and empirically test a universal Cybersecurity Competency Framework (CCF). This universal CCF included a list of demonstrated cybersecurity knowledge, skills, and organizational users' tasks. The main research goal led to five specific goals derived to address the main research question. A total of 42 cybersecurity experts comprised the SMEs who participated in the research study to validate the contents of the universal CCF. This research study was conducted in three phases for data collection. The first phase of the mixed-method approach validated the KSTs for the universal CCF. The literature review contains further details on the KSTs. The second phase of the started with the SMEs' validated the KSTs. The SMEs identified the KST's weights and the threshold level. Phase 3 concluded with the SMEs aggregation of the KST weights into the universal CCF index.

The relevance and significance of this research contributed to the cybersecurity body of knowledge. Specifically, creating the universal CCF helped categorize organizational users' cybersecurity competency and organizational cybersecurity structures (Jajodia et al., 2017). The universal CCF is of significance because organizations are able to identify cybersecurity

competency gaps in their organizational users (Cunningham et al., 2007). Given this relevance and significance, organizations have the opportunity to effectively oversee and govern their cybersecurity policy (Dimov, 2017).

Chapter 2

Review of the Literature

Introduction

In this chapter, a review of the literature was provided to gain an astuteness of the literature about cybersecurity workforce, cybersecurity knowledge, skills, abilities, tasks, and competency. The systematic research for quality peer-review literature established the theoretical foundation, corroborated the research problem's presence, and justified new contribution to the body of knowledge (Levy & Ellis, 2006). The concept-centered approach for examining IS literature utilized a multi-disciplinary strategy that joined knowledge from medical, transportation, aviation, and power plant resources to ensure the knowledge was explicit, comprehensive, as well as reproducible (Fink, 2020; Levy & Ellis, 2006).

Cybersecurity Workforce

Cyber-attacks continue to increase in complexity; while government, industry, and international organizations face a perpetual challenge in recruiting cybersecurity professionals to protect their data assets, creating a global challenge for a cybersecurity workforce (Brilingaite et al., 2020; Burley & Lewis, 2019; Catota et al., 2019; Clark et al., 2018; Crumpler & Lewis, 2019). Several countries have created cybersecurity workforce or structured guidelines to provide training development, capacity building strategies, and education-specific studies (Catota et al., 2019). The European Network and Information Security Agency (ENISA) developed an information security guideline for Member States and European Institutions with conventional approaches and procedures in relation to cybersecurity (Brilingaite et al., 2020). According to Catota et al. (2019), the United Kingdom developed a cyber policy to protect their

cyberspace and incorporated cybersecurity at all levels of education, noting that cybersecurity training and development from an early age is a proponent to mitigate cybersecurity vulnerabilities.

Obama created the National Initiative for Cybersecurity Education (NICE, 2010) to consistently improve programs for cybersecurity awareness. The inconsistency and definition of NICE (2010) evolved into NCWF (Paulsen et al., 2012). Choudhury (2007), Hoffman et al. (2012), and Parsons (2010) postulated that building a holistic cybersecurity workforce is essential. Obama underscored the urgent need for a national cybersecurity workforce and called for several government agencies, various academic institutions, industry, non-government organizations, and international organizations to be involved in building a cybersecurity workforce structure (Paulsen et al., 2012). Even though NCWF (Paulsen et al., 2012) is still relevant, continued measures through Executive Order No. 13,800, (2017) is necessary to strengthening the cybersecurity of federal networks and critical infrastructure. The Executive Order also emphasized that cybersecurity workforce is vital to the American economy given that the workforce depends on the government to keep information assets safe.

Newhouse et al. (2017) spearheaded the development of the cybersecurity workforce and declared that a reference structure outlining the multi-disciplinary nature was necessary. They further noted that the cybersecurity workforce's core function incorporates knowledge sharing at its highest level. Also, the level of knowledge and skills required to fulfill cybersecurity tasks strengthen the organizations' cybersecurity posture. Newhouse et al. (2017) outlined three building blocks useful for organizations to develop a proficient cybersecurity workforce or to make an addition to an existing cybersecurity workforce. Lexicon is considered the first building

block, as it utilized a universal language clarifying communication between an organization and organizational users. The criticality analysis is the second building block, identifying the KSTs essential to the effective operation of the workforce. While these building blocks are salient to the success of an organization's cybersecurity workforce, the study of these functions is outside the scope of this research. The third building block, the competency analysis, is relevant to this research because it informs organizations of the expectancy level for positions. Additionally, the competency analysis allows organizations to fine-tune relevant cybersecurity tasks to meet KSTs for the work roles that make up the job positions.

Newhouse et al. (2017) outlined three criteria for conducting the cybersecurity competency analysis within organizations. For the first criterion, organizations performed stock-taking of their current cybersecurity workforce. The stock-taking was necessary to determine the number of vacant positions, identify the organizational users' skills and tasks performed, as well as determine the size of the workforce. To establish the second criterion, organizations developed an understanding of the cybersecurity workload and organizational users' cybersecurity competency. For the final criterion, organizations addressed the gaps in the cybersecurity workforce to customize positions according to cybersecurity skills.

Bastian et al. (2020) utilized competency analysis to investigate the workforce planning problem within the human resource department that oversees the United States (U.S.) Army Cyber Branch. This branch protects the Department of Defense networks and systems from cyber-attacks. To accomplish the first criterion of competency analysis, they examined the U.S. Army Cyber area of expert career fields, utilizing a mixture of personnel accessions, branch transfers, and promotions to determine the number of newly hired cyber-officers, branch

transfers, and cyber-officers that got promoted each year. The workforce planning problem was a combination of organizational need for staffing and personnel promotion guidelines. These workforce problems were further complicated by stochastic retention rates for every year a cyber-officer worked and promotion level for each year over a 30-year timeframe. Utilizing a scenario-based approach and a robust optimization representation, Bastian et al. (2020) validated a workforce planning model allowing cyber-officers to be promoted to vacant positions based on their competency, and the model is generalizable to other military specialists.

Borba et al. (2019) noted that several studies (Franzese et al., 2006; Garcia et al., 2012) had been conducted on the operation and maintenance workforce planning of electrical power systems, but limited studies focused on the competency of organizational users to form multitasking teams. Additionally, Borba et al. (2019) sided with Wan et al. (2011) in noting that the refinement of tasks for workforce planning took into consideration organizational users' competency to meet the future requirements of the tasks. Borba et al. (2019) utilized a mathematical computation to identify the organizational users' competency to aid with the multitasking of organizational users. Similar to Borba et al. (2019), this research utilized a mathematical computation to distribute 100 percentage of points to identify the organizational users' competency.

Assante and Tobey (2020) acknowledged that there is a shortage of novice, intermediate, advanced, and expert organizational users in the workforce. These organizational users are urgently needed to safeguard government, private, and public sector assets from cyber-attacks. Assante and Tobey (2020) suggested a cybersecurity workforce developed to identify organizational users' competency because advanced cybersecurity threats are not easily

identified. They agreed with Momin and Mishra (2015) that the KSTs needed for cybersecurity threat can be identified through Human Resources (HR) strategic workforce planning. Momin and Mishra (2015) as well as Philip and Lindley (2006), employed predictive analysis, quantitative analysis, and organizational users' performance to assist HR in identifying the organizational users' competency. Philip and Lindley (2006) noted that utilizing HR data can identify gaps in workforce planning development. Assante and Tobey (2020) developed a cybersecurity workforce model utilizing HR data to identify organizational users' knowledge and skills based on the tasks for organizational users to become experts in cybersecurity. As airline pilots are trained with different types of simulators, organizational users should utilize cybersecurity training simulators to identify different types of cybersecurity threats (Assante & Tobey, 2020).

Milloux and Grimalia (2018) recognized the urgency for a cybersecurity resiliency workforce and outlined workforce responsibilities based on job descriptions and KSTs. The work roles were identified according to the competency of novice, journeyman, and expert, setting the stage for scalability. According to Milloux and Grimalia (2018), the work roles were dependent upon experience and specific job descriptions to demonstrate how organizational users would communicate and interact with other personnel and security stakeholders. Further, Milloux and Grimalia (2018) stated that organizational users acquired KSTs in three cyber domains with 10 years' experience to be considered an expert, and organizational users search for advanced cybersecurity positions to further their careers. Even though Milloux and Grimalia (2018) provided the outline for the workforce model, they stopped short of specifying a workforce plan. However, this research provided the essential guidelines for implementing a workforce plan.

Furthermore, organizations would have difficulty determining organizational users' competency as outlined in Milloux and Grimalia (2018). This research instead utilized the instructions of Momin and Mishra (2015) on workforce planning and the types of assessment to determine organizational users' competency.

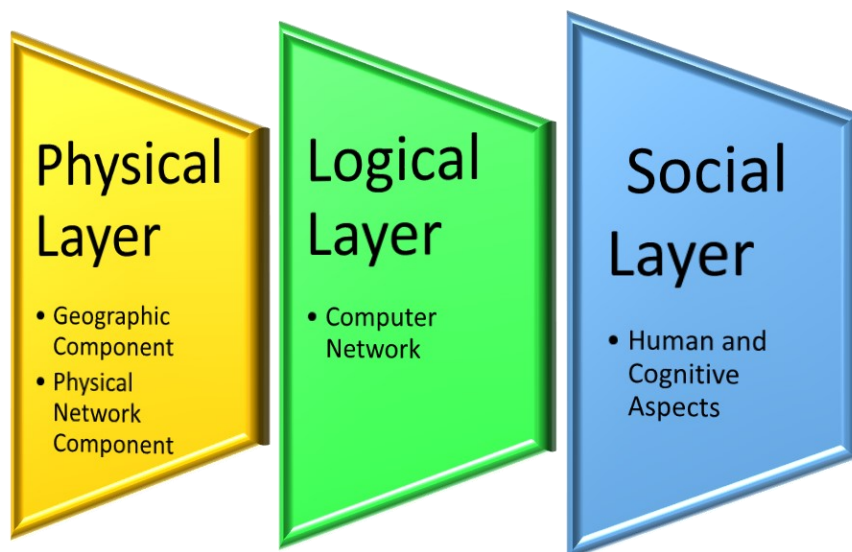
Burley and Lewis (2019) acknowledged that the cybersecurity workforce shortage is a global problem affecting companies and predicted a shortage of approximately 1.8 million organizational users by the year 2020. Burley and Lewis (2019) pointed out that Boeing Company, the world leader in aerospace, suffered from a paucity in its cybersecurity workforce. Instead of assessing the competency of organizational users' KSTs to identify talents from within Boeing, they recruited college graduates. Moreover, the college graduates' knowledge and skills were not in accordance with the tasks required for the work roles. However, Burley and Lewis (2019) noted that Boeing's willingness to hire college graduates strengthened their cybersecurity workforce pipeline. This action allowed the company to utilize HR strategic workforce planning to identify organizational users' competency and to place them in positions suitable for cybersecurity work. Burley and Lewis (2019) developed Wirojanagud et al. (2007)'s study recognizing organizational users' differences in terms of KSTs, bridging the gap between HR and organizational users' agility to strengthen the cybersecurity workforce at Boeing. The case study from Burley and Lewis (2019) guided this research about utilizing an HR strategic plan for developing a cybersecurity workforce. Dawson and Thomson (2018) pointed out the usefulness of the cybersecurity workforce that supports the exponential growth of online devices, organizational users' vulnerabilities, and the complexity of cyber infrastructure. Dawson and Thomson (2018) noted that the cybersecurity workforce was originally designed to support the

U.S. government's hiring requirements and was the only comprehensive roster of work roles in the cyber community.

Ani et al. (2018) as well as Dawson and Thomson (2018) contended that the composition of the cyber domain system has three layers: physical, logical, and social. Newhouse et al. (2017) built the cybersecurity workforce using these three layers. Training and Doctrine Command (TRADOC, 2010) provided definitions for the three layers of the cyber domain system. The physical layer contains the hardware and infrastructure, laying the foundation for the Internet and the geographical location of the hardware. The second layer contains the logical devices that are connected to the computer network. The logical devices connected to the network are computers and cellphones, among various network devices. The social layer involves the human and cognitive factors interacting within the network. Figure 1 contains the Cyber Domain System.

Figure 1

Cyber Domain System



Dawson and Thomson (2018) noted that the seven work-role categories are aligned with the physical and logical layers of the cyber domain, and very little focus has been on the social/human layer. A plethora of research has noted that human factors comprise the social layer and are the leading cause of cybersecurity vulnerabilities (Ani et al., 2018; Carlton & Levy, 2015). Yet the social layer is widely ignored within the context of cybersecurity workforce development (Brilingaite et al., 2020; Wei et al., 2020). Garvin et al. (2013) posited that cybersecurity resilience was contingent upon mitigating human errors. Therefore, cybersecurity professionals considered the social layer and not focus only on the technical and logical layers when mitigating cyber-attacks. Moreover, Ani et al. (2018) utilized a scenario-based situation to underscore the importance of the social layer in the cybersecurity workforce, stating that organizational users' limited KSTs causes them to undervalue the technical and logical layers.

Even though Ani et al. (2018) as well as Dawson and Thomson (2018) noted the social layer is critical to mitigate cybersecurity vulnerabilities, Crumpler and Lewis (2019) argued that cybersecurity workforce programs such as compliance audits and policy planning under the social layer have very little impact on organizations' cybersecurity posture. Crumpler and Lewis (2019) maintained that tasks including penetration testing, secure system design, and tool development within the technical layer constitute the greatest cybersecurity need to mitigate cyber-attacks and the best methodology to strengthen the organization's cybersecurity posture.

Crumpler and Lewis (2019), Hoffman et al. (2012), as well as Urias et al. (2017) noted the urgency to build the cybersecurity workforce. Mailloux and Grimaila (2018) mentioned the world is dependent upon the technical layer, and the cybersecurity workforce adapt to the

increasing demand. A summary of the prior research regarding the cybersecurity workforce is listed in Table 1.

Table 1

Summary of Cybersecurity Workforce Literature

Study	Description of the Problem and Theory	Methodology	Sample	Instrument	Main Findings or Contributions
Ani et al., 2018	Limited involvement of professionals to mitigate the larger cybersecurity problem	Test-scenario via survey	37 professionals	Human factor security evaluation	The technical layer of the cybersecurity workforce was essential, but the social and human aspects were equally important
	Shortage of cybersecurity professionals in the cybersecurity workforce	Concept paper	United States cybersecurity workforce	None	The workforce was required to understand the weaknesses and threats in cybersecurity
Bastian et al., 2020	Cyber workforce planning problem in the United States Army	Empirical study via survey	Three alternative approaches	Stochastic parametric distribution	Recognized issues with personnel policies and recommended changes
Brilingaite et al., 2020	A shortage of skilled cybersecurity professionals in the workforce	Case study	77 participants	Cybersecurity defense exercise	Developed a framework to assist in cybersecurity competency during hybrid cybersecurity defense exercise

Study	Description of the Problem and Theory	Methodology	Sample	Instrument	Main Findings or Contributions
Burley & Lewis, 2019	Global cybersecurity workforce shortage and limited robust cybersecurity programs to meet the industry demands	Case study	One company	Cybersecurity workforce training and development guidelines	Developed cybersecurity programs and offered flexible guidance on a holistic view of the cybersecurity field
Catota et al., 2019	Limited research identifying the factors that influence a cybersecurity workforce and education	Empirical study via interviews	13 universities and polytechnic schools	Cybersecurity development	A lower confidence level in the institutions to provide adequate cybersecurity education
Choudhury, 2005	The absence of a formalized workforce planning in local government	Empirical study via survey	10 counties	Workforce planning	Workforce planning was not a new concept but a strategic human resources management component
Crumpler & Lewis, 2019	Insufficient training and development preparing students for cybersecurity workforce	Conceptual paper	None	Cybersecurity skills shortage	A focus must be on cybersecurity technical areas to address the cybersecurity workforce shortage
Parsons, 2010	Failure in cybersecurity workforce planning	Literature review and synthesis	None	Workforce planning	Developed a reliable cybersecurity workforce
Urias et al., 2017	Limited standardized theory or methodology offered for cybersecurity training	Live virtual constructive-based training scenario	Three training zones	Cybersecurity training environment	Developed a virtual constructive environment for cybersecurity training exercises

Cybersecurity Knowledge

Definition of Knowledge

Several researchers noted that the definition of knowledge has been a long-standing issue (Alavi & Leidner, 2001; Davenport & Prusak, 1998; Nonaka, 1994). Nonaka (1994), who commented that the search for the definition of knowledge is never-ending, the definition is unclear, and adopted the definition of knowledge from the Greek philosopher Plato as a “justified true belief” (p. 15). Additionally, Shulman (1987) provided a simple definition that knowledge is what is known. Nonaka (1994) further pointed out that even though the definition of knowledge is unknown, minimal emphasis has been placed on how knowledge is created, how the knowledge created can be processed and managed. He noted that knowledge creation can be drawn from tacit and explicit knowledge. Nonaka (1991) described tacit knowledge as an individual quality that is difficult to formalize and communicate. An example of tacit knowledge is the informal technical skill of kneading dough. Likewise, Nonaka (1991) defined explicit knowledge as transmittable into methodical language and something that can be taught. An example of explicit knowledge is a handbook of types of security vulnerabilities compiled with information gathered from organizational users (Krogh et al., 1997).

Nonaka (1991) pointed out that four basic combinations of knowledge creation existed between tacit and explicit knowledge: socialization, combination, externalization, and internalization. *Socialization* is the interchange from tacit knowledge to tacit knowledge. An example of socialization is the process of sharing tacit knowledge from an expert organizational user to a novice organizational user through observation, such as a novice organizational user observing an expert cybersecurity professional identifying a phishing email (Nonaka, 1991;

1994). *Combination* is the interchange from explicit knowledge to explicit knowledge. An example of combination is organizational users collecting cybersecurity source codes of varying types of vulnerabilities at granular levels and collating them into a cybersecurity vulnerability handbook that can be utilized by cybersecurity experts (Akram & Ping, 2020). *Externalization* is the interchange from tacit knowledge to explicit knowledge (Nonaka, 1991; 1994). An example of externalization is when an organizational user is able to develop a vulnerability benchmark based on their own tacit knowledge developed over the years of working with different types of vulnerabilities (Akram & Ping, 2020). *Internalization* is the interchange from explicit knowledge to tacit knowledge where new information is shared throughout the organization (Nonaka, 1991; 1994). An example of internalization is when organizational users utilize the vulnerability benchmark handbook to improve their own tacit knowledge, finding novel ways to identify cybersecurity vulnerabilities (Akram & Ping, 2020). Figure 2 illustrates the nodes of creating knowledge.

Figure 2

Knowledge Creation Nodes

		Tacit knowledge	To	Explicit knowledge
From	Tacit knowledge	Socialization		Externalization
	Explicit knowledge	Internalization		Combination

Bassellier et al. (2001) contended that explicit and tacit knowledge are required for organizational users to express knowledge in Information Technology (IT). Markus (2001) stated that only explicit knowledge was the domain of IT. For the purpose of building a cybersecurity framework, both explicit knowledge and tacit knowledge are salient for this research. Table 2 lists the summary research defining knowledge.

Table 2

Summary of Knowledge Defined Literature

Study	Description of the Problem and Theory	Methodology	Sample	Instrument	Main Findings or Contribution
Akram & Ping, 2020	The rate of cybercrimes increased exponentially day by day	Case study	One company	Vulnerability source code	Proposed a vulnerability benchmark at different levels of granularities
Bassellier et al., 2001	Limited competence with IT line managers	Literature review and synthesis via interviews	Two sets of literature articles	Explicit and implicit knowledge	Developed a theoretical model linking IT competence and business technology leadership
Krough et al., 1997	The misconceptions of knowledge activism	Case study	One company	Knowledge activist	Provided the guidelines for knowledge activism
Nonaka, 1994	A shift in how organizations create and process knowledge	Conceptual paper	Four concepts of explicit and tacit knowledge	Organizational knowledge creation	Provided an examination of knowledge creation

Cybersecurity Knowledge Units

Even though it has been duly researched that organizational users are the weakest link when protecting organizational assets, the essential question is: What cybersecurity knowledge units should organizational users know to be competent in cybersecurity when protecting organizational assets? Bassellier et al. (2001) asserted that explicit cybersecurity knowledge enables organizational users to communicate effectively with cybersecurity professionals. Some studies have provided cybersecurity knowledge units that organizational users possessed when optimizing cybersecurity within the organization (Burley & Lewis, 2019; Mailloux & Grimaila, 2018).

Newhouse et al. (2017) categorized cybersecurity knowledge units into seven categories that organizational users employed to enhance cybersecurity knowledge at its highest level. The Securely Provision (SP) role revolves around a traditional IT field consisting of software developers, computer programmers, and network architects. The Operate and Maintain (OM) role provides support to system administrators. The Oversee and Govern (OV) role revolves around managerial roles, cyber law, and policy development. The Protect and Defend (PR) role identifies, analyzes, and mitigates threats to cyber analysts and network defenders. The Analyze (AN), Collect and Operate (CO), and Investigate (IN) roles revolve around the broad field of digital forensics and tend to be government or law enforcement positions.

Dawson and Thomson (2018) explained that within the SP category organizational users possessed the knowledge to envision, design, and develop secure IT systems for aspects of network development. The knowledge required to design and develop secure IT systems has experienced challenges to provide secure information systems because of the rapidly-developing

changes in the IT industry (Hsu & Sabherwal, 2012). Abualoush et al. (2017) investigated the relationship among Knowledge Management (KM), IS, and Employees' Empowerment (EE) on Employees' Performance (EP). Their findings indicated that KM and IS are positively and significantly associated with EE. The results from Abualoush et al. (2017) agreed with prior research (Khodabakhshi et al., 2013; Somayyeh & Morteza, 2015) that organizational users were empowered knowing their performance improved knowledge creation and honed skills that were significantly associated in securing networks that mitigated cyber-attacks. Therefore, this research study included the areas of KM and IS into the CCF necessary to secure networks that mitigate cyber-attacks.

In another study, Cavusoglu et al. (2015) employed only senior IT professionals with knowledge of information security to determine why information security systems in organizations continued to be a problem even with significant investments in technical and KM resources. According to Nonaka (1991) as well as Arling and Chun (2011) when creating knowledge to solve information security problems, the knowledge to resolve or mitigate the problem required organizational users from all levels of the organizations and the four nodes of knowledge creation. Cavusoglu et al. (2015) acknowledged that including organizational users from all levels of the organizations could have better served their data collection. They noted that a single organizational user would not be knowledgeable enough about every aspect of security issue in the organization. Therefore, this research study employed all organizational users' cybersecurity knowledge to build a universal cybersecurity workforce.

The knowledge required for organizational users in OM category of NCWF (NICE, 2017) enabled them to support, administer, and maintain IT systems, ensuring its security,

performance, efficiency, and effectiveness (Dawson & Thomson, 2018). Zhang et al. (2018) designed and developed a probabilistic optimization model that can be employed in a decision support system to configure security solutions for an information systems infrastructure. Zhang et al. (2018) noted that the model can be employed by organizations to manage the information systems infrastructure that supports their security controls. Moreover, Horsman et al. (2014) presented a knowledge-creation approach to support, administer, and maintain IT systems. Their approach employed the triage concept used in medicine when prioritizing injured patients. In a similar context, the incident response can allow users to categorize cyber incidents, allowing organizations to prioritize cyber incidents based on severity. Horsman et al. (2014) demonstrated the use of their model with a probability model similar to Zhang et al. (2018). The advantage of a probabilistic models was the likelihood of focusing on cyber incidents that could possibly cause disruption to organizations. Therefore, this research study included KSTs as part of a probabilistic approach to mitigate cyber incidents.

Organizational users possessed the knowledge of leadership, as well as management, to oversee and govern cybersecurity work in organizations (Newhouse et al., 2017). Several studies acknowledged that the study of leadership dates back more than 100 years, with varying definitions and styles of leadership (Amagoh, 2009; McCleskey, 2014; Popper & Lipshitz, 1993; Seele & Eberl, 2020). Popper and Lipshitz (1993) noted that the essence of leadership is the act of motivating people in a non-coercive manner. Furthermore, Popper and Lipshitz (1993) noted that an effective cybersecurity leader can match different types of cybersecurity work with the most appropriate cybersecurity experts, while allowing those experts to lead cybersecurity projects. Nonaka et al. (2000) agreed with Popper and Lipshitz (1993) that different

cybersecurity leaders should assume leadership roles based on their cybersecurity KSTs, guaranteeing that the most appropriate person would be in any particular role. This research determined the competency required to oversee and govern cybersecurity work.

Cybersecurity leadership in organizations is essential and currently facing challenges because the Board of Directors responsible for hiring organizational users in leadership job positions for cybersecurity governance lagged concerning the breadth and depth of cybersecurity (Huang et al., 2016; Longo & Giaccone, 2017; Shaikh & O'Connor, 2020). Additionally, Auffret et al. (2017) pointed out that organizations are experiencing a shortage of cybersecurity professionals to govern cybersecurity operations efficiently and effectively because of limited cybersecurity knowledge. According to Aldawood and Skinner (2020), along with Hatfield (2018), the leading cause of cybersecurity threats in an organization was social engineering. Hatfield (2018) as well as Tetri and Vuorinen (2013) described social engineering as the penetration of information systems through the use of social methods. Aldawood and Skinner (2020) aimed to find other tools to mitigate social engineering apart from awareness programs by interviewing expert cybersecurity professionals. Aldawood and Skinner (2020) revealed that contextual social engineering awareness and cybersecurity organizational culture lead to a decrease in social engineering in organizations. This research followed Aldawood and Skinner (2020) approach to employ cybersecurity experts to oversee and govern cybersecurity operations.

Organizational users required knowledge for protection and detection from cyber-attacks to safeguard organizational infrastructures, such as the networks (Al-Matari et al., 2018), and physical systems, such as the power grid (Yagan et al., 2012). Knowledge of protection for the networks and power grid includes physical security. Whitman and Mattord (2018) defined

physical security as the “protection of physical items, objects, or areas from unauthorized access and misuse” (p. 20). Protection for physical security is paramount not only for the networks but also for the software, data, organizational users, and procedures (Whitman & Mattord, 2018). Physical security protection varied between organizations, as they have different operating structures. However, organizational users should have practical cybersecurity knowledge to report cybersecurity threats levied against their organization.

The network that supports cyber-physical energy systems, such as electrical power grids, needs to be protected from sophisticated cyber-attacks (Ji et al., 2016; Ten et al., 2010; Yagan et al., 2012). The algorithms that are required for cyber-physical energy network security are best understood by expert organizational users with advanced cybersecurity knowledge (Ten et al., 2010). Ji et al. (2016) noted that such organizational users were essential to comprehend the coupling of networks, thereby detecting the hacking of the electrical cyber-physical systems, such as the 2003 North American blackout and the 2003 Roman blackout. Moreover, Mylrea et al. (2017) warned that blackouts should not be the only concern for organizations, because hackers are likely to reduce the electrical bills of customers, creating financial and economic losses.

Organizational users not only possess the knowledge to protect physical items but also possess the knowledge to protect passwords and sensitive information (Abuadbba & Khalil, 2017; Liang et al., 2018). Password failure, such as utilizing the same password on multiple applications, is one main reason for the loss of data (Liang et al., 2018). The significance of password protection should be emphasized to organizational users (Dell’Amico et al., 2010; Liang et al., 2018). Diedrich and Guzman (2015) noted that organizational users complained that

there were too many passwords to retain; they also noted that organizational users had limited knowledge on the password lifespan. Diedrich and Guzman (2015) suggested that organizations implement a knowledge management system for organizational users to gain and share knowledge on relevant IT as well as cybersecurity topics, including password management. Liang et al. (2018) supported Diedrich and Guzman (2015) by implementing a user-controllable framework for mitigating the loss of sensitive data as a result of password failure. Similarly, Raponi and Di Pietro (2018) proposed the usage of a password protection policy. Raponi and Di Pietro (2020) replicated their prior study (Raponi & Di Pietro, 2018), noting that organizations that strengthened their password policies by implementing knowledge management showed improvement in protecting sensitive data, while other organizations still suffered from vulnerabilities.

Kriz (2011) emphasized that organizational users acquired knowledge to review and evaluate cyber-attacks, as well as developed a global framework to improve their cybersecurity infrastructure. James (2018) concurred with Kriz (2011) that organizations were reluctant to implement cybersecurity best practices by reforming their workforce structure to review and evaluate any types of cyber-attacks because of the negative publicity associated with reporting cyber-attacks. The restructuring (Borba et al., 2019) and implementation of cyber defense systems (Ben-Asher & Gonzalez, 2015) would allow for organizations to be more cyber resilient (Mailloux & Grimaila, 2018), increase organizational users' cybersecurity knowledge, and provide relevant best practices to structure, distribute, and align cybersecurity knowledge to respond effectively to cyber-attacks (James, 2018).

Neigel et al. (2020) advocated that cybersecurity knowledge should be focused on the human aspect, as it is questionable how many novice organizational users read and understand the cybersecurity guidelines or handbooks. However, David et al. (2020) stressed that emphasis should not only be on the human aspect of cybersecurity knowledge, but that organizations constantly upgrade hardware and software to outpace cyber-criminals. Similarly, Clark et al. (2018) called for organizations to focus on the technical aspect of organizational users' cybersecurity knowledge required when programming systems to mitigate cybersecurity attacks. The literature revealed a gap in the human and technical aspects of cybersecurity knowledge. This research employed SMEs to validate the cybersecurity knowledge required to mitigate cybersecurity attacks.

Ani et al. (2018) as well as Ben-Asher and Gonzalez (2015) noted that organizational users' cybersecurity knowledge on firewall and technology intrusion detection systems was essential to safeguard workstations from cyber-attacks. As an example, an organizational user with limited technical cybersecurity knowledge were not able to mitigate a cyber-attack, thereby yielding to a cyber-attacker. Organizational users' technical cybersecurity knowledge is important to guide the hardware and software related IT, as well as to protect cybersecurity infrastructure.

Clark et al. (2018) posited that knowledge creation among organizational users improves cybersecurity knowledge through teamwork because novice organizational users with limited cybersecurity knowledge were in a position to learn from other organizational users who were more advanced in cybersecurity knowledge. Wegner (1986) noted that one organizational user should not be responsible for the entire cybersecurity knowledge in organizations, because knowledge is created among organizational users in an effective manner based on their expertise

and role in the organizations. For example, organizational users with limited cybersecurity knowledge may report suspicious vulnerabilities to expert organizational users working in a cybersecurity department; the decision to procure new anti-virus systems for the organization is transferred to expert or advanced organizational users (Clark et al., 2018).

Organizational users possessed knowledge to analyze, review, evaluate, and respond to cybersecurity incidents (Gourisetti et al., 2017; Onwubiko & Ouazzane, 2020). Gourisetti et al. (2017) as well as Onwubiko and Ouazzane (2020) underscored the necessity for organizations to implement a response planning team, to communicate cybersecurity incidents to stakeholders, to perform an analysis of cybersecurity incidents, and to make improvements to the current cybersecurity infrastructure. Onwubiko and Ouazzane (2020) compared cybersecurity incident response teams to emergency responders. They stated that emergency services, firefighters, police officers, and hospitals are bound by prescribed rules, protocols, and procedures set forth in an emergency response manual that can be enacted in the case of an emergency. The personnel are knowledgeable about the emergency response manual and can respond to any urgent situation (Onwubiko & Ouazzane, 2020). In a similar context, the cybersecurity incident response team in organizations possessed cybersecurity knowledge, perform cybersecurity drills, and be prepared for any cybersecurity incidents like emergency responders. Onwubiko and Ouazzane (2020) confirmed that novice organizational users followed organizational cybersecurity incident response protocol if they are appropriately trained and reported cybersecurity incidents to expert organizational users on the cybersecurity incident response team.

Mailloux and Grimaila (2018) as well as Mylrea et al. (2017) underscored the growing need for organizational users to be knowledgeable about recovering from cyber-attacks, establishing maintenance strategies, and restoring the services or products that were affected due to cyber-attacks. Few research findings maintained that cybersecurity knowledge should focus on vulnerabilities of organizational users to mitigate cyber-attacks (Neigel et al., 2020; Parsons et al., 2014). While organizational users' cybersecurity skills are significant to mitigate cyber-attacks, a focus on cyber-physical systems is important. Furnell et al. (2006), Jones et al. (2018), as well as Herath and Roa (2009) confirmed that organizational users' cybersecurity knowledge should not be limited to non-technical vulnerabilities and also include training and development on technical vulnerabilities. Jones et al. (2018) recommended that cybersecurity knowledge include networks and programming if organizations are striving for a holistic cybersecurity workforce.

Organizational users also possessed knowledge of denial and deception techniques, a necessity for collecting and operation of cybersecurity information (Newhouse et al., 2017). Denial technique is the process of denying cyber-attackers access to organizational information assets, while deception is the process of creating misleading information through factual and fabricated information (Heckman et al., 2013). Cyber criminals are relying upon more sophisticated tools to disrupt services, and organizational users formulate different types of deception techniques to prevent cybersecurity threats from becoming cyber-incidents (De Faveri et al., 2018). However, Conti and Fanelli (2019) asserted that designing sophisticated tools prevented 80 out of 100 cyber-attacks, but the remaining 20 cyber-attacks were difficult challenges that required organizational users to study cyber criminals' activities and developed

the best continuous cyber defense mechanisms. Conti and Fanelli (2019) acknowledged that organizational users might not be able to disrupt every cybersecurity threat.

The knowledge to investigate cyber incidents or crimes related to IT, networks, and digital devices was a requirement for organizational users (Newhouse et al., 2017). Mavroeidis and Bromander (2017) contended that cybersecurity threat intelligence drove organizations to identify, gather, and analyze cybersecurity threats. Organizational users required knowledge pertaining to cybersecurity threat intelligence when sharing threat data and threat information (Mavroeidis & Bromander, 2017). Ben-Asher and Gonzalez (2015) developed an intrusion detection system to investigate whether or not organizational users' cybersecurity knowledge can identify malicious cybersecurity threats based on a sequence of network activities. Ben-Asher and Gonzalez (2015) confirmed that organizational users' cybersecurity knowledge positively associated with detecting malicious cybersecurity threats. Similar to Ben-Asher and Gonzalez (2015), this research validated the cybersecurity knowledge required for the competency necessary to detect cyber-attacks. A summary of prior research regarding cybersecurity knowledge units is listed in Table 3.

Table 3*Summary of Cybersecurity Knowledge Units Literature*

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Abualoush et al., 2017	Limited research on the interplay among knowledge management, information systems, and employee empowerment on their performance	Empirical study via survey	287 employees in the pharmaceutical industry	Efficiency and effectiveness on Information systems	Knowledge management and information systems significantly affect employee empowerment
Amagoh, 2009	A shortage of practical leadership limits organizations' ability to implement and maintain their organizational objectives	Literature review and synthesis	100 research articles	Leadership development	Leadership development should be incorporated into the culture of the organization to yield leaders who can implement and maintain their organizational objectives
Arling & Chun, 2014	Limited organizations comprehend how to maximize knowledge management to achieve their organizational goals	Empirical study via longitudinal case study	One company	Archived data and interviews	Developed a knowledge creation framework
Bastian et al., 2020	Cyber workforce planning problem in the United States Army	Empirical study via survey	Three alternative approaches	Stochastic parametric distribution	Recognized issues with personnel policies and recommended changes

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Ben-Asher & Gonzalez, 2015	The cognitive process required for adequate network protection was limited	Empirical study via questionnaire	55 participants from the university	Competency with intrusion detection system	Competency played a role in detecting cyber-attacks
Borba et al., 2019	Limitation on optimization model for workforce planning in operation and maintenance companies	Literature review and synthesis	None	Workforce problem: Strategic, tactical, and operational planning	Most companies in operation and maintenance employed operational planning to resolve workforce problems
Cavusoglu et al., 2015	Lack of theoretical and empirical corroboration for the variations in the levels of information security control resources	Empirical study via survey	241 Managerial IT professionals from various organizations	Organizational information security control resources	Organizational internal policies and pressures were significant in the variations of information security control resources
David et al., 2020	Even though organizations invest in hardware and software for cybersecurity defense, the involvement of individual specialty knowledge is under studied	Empirical study via survey	262 participants of an information-sharing center	Theoretical framework and hypotheses	Resourcefulness, usefulness, and reciprocated beliefs were significantly related to knowledge absorption, while rewards were negatively associated with knowledge absorption
Hatfield, 2018	The interrelatedness of social engineering in politics and cybersecurity obscure organizational users' ability to determine and reject social engineering	Empirical study via survey	134 scholarly articles	Social engineering and its relationship with epistemic asymmetry, technocratic dominance, and teleological replacement	Revealed a theoretical assortment of contemporary annotations about cybersecurity

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
	attacks in cyberspace				
Onwubiko & Ouazzane, 2020	Lack of a standardized playbook or operating procedures for cybersecurity incident management	Explanatory and experimental research	15 years of combined experience for cybersecurity professionals	Cybersecurity incidents	Provided a holistic cybersecurity incident response framework
Parsons et al., 2014	Limited validated instruments to measure the employees' computer behavior when protecting organizational information systems	Explanatory research	500 employees	Knowledge, attitude, and behavior used to measure human aspects of information security	A significant difference in employees' behavior toward knowledge of policy, procedure, and attitude
Yagan et al., 2012	The interconnectedness of smart systems is complex, and studies of cascading failures are yet to be understood	Analytical and experimental research	Two interacting networks	Cyber-physical system	Developed a robust network that can withstand cascading failure, while easily understood by network management
Zhang et al., 2018	Limited optimization model that holds the potential to strengthen a decision support system for modeling security solutions for organizational information system.	Empirical research via survey	Two models	Decision support system	Proposed a model for security solutions for a pragmatic IT system using breach probability estimates

Cybersecurity Skills

Skills Defined

Boyatzis and Kolb (1991) as well as Levy (2005) defined skill as an amalgamation of organizational users' knowledge, ability, and experience to perform something well. Gaining a skill, is not an overnight step but is rather a developmental and experiential process over longer time (Bleed, 2008). Moreover, Bleed (2008) pointed out that skill should be acquired, and the acquisition of skill is rooted in cognitive knowledge where organizational users asked questions such as "what," "how," and "why" (p. 157). Similarly, Gravill et al. (2006) noted that the acquisition of skills is a learning process occurring in three incremental stages: declarative ("know-what"), procedural ("know-how"), and strategic ("know-why"; p. 380). Declarative is the primary stage where organizational users begin to formulate the foundation for their cybersecurity skill building. For example, in the declarative process, organizational users begin to ask what a phishing email is and gather as much information as necessary to build their skill. Organizational users are given facts, brochures, or graphs on phishing emails, which are translated into explicit knowledge (MacLean & Cahillane, 2015). The second stage of acquiring skill is procedural, where information is structured and organized, or a refinement of declarative knowledge (Gravill et al., 2006; MacLean & Cahillane, 2015). Organizational users begin to apply the knowledge gained from reading about phishing emails to identify such emails. For example, organizational users asked how they can utilize the information on brochures to identify phishing emails. MacLean and Cahillane (2015) noted that when organizational users were influenced by procedural knowledge, it was the formulation of a skill-based behavior. The autonomous stage is the third stage of skill acquisition (Cornford & Athanasou, 2006; MacLean

& Cahillane, 2015). During this stage, the skill is executed automatically without monitoring, assistance from brochures, or relying upon sequential steps (Cornford & Athanasou, 2006). From this point on, the organizational users possessed the skills needed to identify phishing emails without referencing any materials. According to MacLean and Cahillane (2015), the repeated action in the autonomous stage is similar to driving a car or flying an airplane where the skill does not require any reference material. In Figure 3, Gravill et al. (2006) noted the three stages of acquiring skills.

Figure 3

The Stages of Skill Acquisition

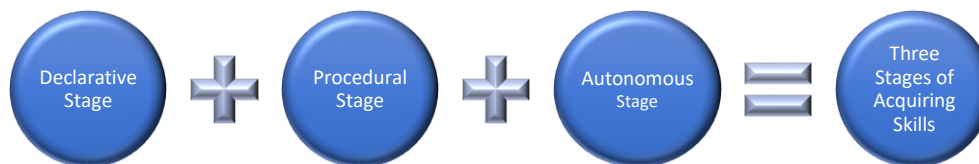


Table 4 lists the summary research defining skills.

Table 4

Summary of Skills Definition Literature

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Boyatzis & Kolb, 1991	Limited research involving individuals referencing learning style instruments	Empirical study	205 MBA students	Self-assessment on learning skills profile	Developed and validated a self-assessment instrument that individuals can use to evaluate

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
					their skill profiles
Cornford & Athanasou, 1995	Scant research on skill acquisition and the development of expertise	Literature review and synthesis	None	Skill acquisition	Provided an outline of skill-acquisition through learning
Gravill et al., 2006	Self-assessment challenges or organizational users	Empirical study via survey	67 participants from four large organizations	Self-managed learning	The findings indicated that organizational users had trouble self-assessing their declarative and procedural knowledge
Levy, 2005	Even though online learning in higher education created success for universities, a focus on online MBA programs' advantages afforded to students raised questions	Empirical study via longitudinal study	One online MBA program One on-campus MBA program	Learning skills profile	Both online and on-campus MBA programs significantly influenced skills
MacLean & Cahillane, 2015	Few institutions maintained updated e-learning policies and guidelines	Case study	One PC-based tool	Skill acquisition	Improvement in KSTs, modifications to policies would be beneficial to institutions

Organizational Users' Cybersecurity Skills

Carlton and Levy (2017) defined cybersecurity skills as the skills organizational users needed to prevent damage to IT when using the Internet. Furthermore, Carlton and Levy (2017) pointed out that organizational users' limited and dated cybersecurity skills as well as noted the essential

skills for scenario-based applications critical for addressing cybersecurity threats. Even though organizational users possessed these essential skills (Carlton & Levy, 2017) to prevent damage to organizational infrastructure, the development of the cybersecurity workforce had limited concentrated effort defining the skills required for a competency analysis (Newhouse et al., 2017). The skills required for the cybersecurity workforce competency analysis were correlated with tasks, and the organizational users without the skills were not able to complete the tasks (Newhouse et al., 2017).

The primary goal of every organization is to secure their information assets from unauthorized users (Al-Safwani et al., 2018). To secure organizational information assets, organizational users possessed skills to securely build IT systems to prevent unauthorized access from cyber criminals (Newhouse et al., 2017). The skills that were required to secure IT systems and networks include risk management. Organizational users serving as senior executives should be skillful in identifying the necessary protections, such as security control assessment, and applying information security privacy principles to organizational requirements (Newhouse et al., 2017). Al-Safwani et al. (2018) outlined some security controls, such as firewalls, email gateways, routers, and anti-virus servers, in which organizational users' skills were needed to utilize these security controls to prevent vulnerabilities. Paananen et al. (2020) pointed out that organizational users serving in information security management be skillful in developing information security privacy principles necessary for confidentiality, integrity, and maintenance of organizational business goals. Previously, Baskerville and Siponen (2002) noted that skills in writing information security policies were essential because the function would assist organizational users in decision-making about how they protect organizational informational

assets. Nyanchama (2005) posited that building the IT systems was essential, but most importantly, the systems must be effectively and efficiently managed. Haquaf and Koyuncu (2018) aimed to find the skills required for information security management. Haquaf and Koyuncu (2018) acknowledged that managing information security was dependent upon professional experts to attain needed security governance. They determined that significant skills were required for IT security management for varying frameworks and market demands. They concluded that organizational users must be able to design and develop IT security systems, implement security policies, and coordinate information security governance to provide the required security for corporate objectives. Similar to Haquaf and Koyuncu (2018), this research study determined the cybersecurity skills were needed for a cybersecurity competency framework.

According to Newhouse et al. (2017), skills in database management were necessary to provide support, maintenance, performance, and security of IT systems. Gorlatykh and Zapechikov (2018) pointed out that organizational users have skills in storage space allocation, restoration, deleting files when designing databases, and writing queries for conducting security searches to protect confidential data. Likewise, skills were required for writing algorithms to detect cyber-attacks, especially in cyber-physical systems that were prone to such attacks (Ten et al., 2010).

Similar to database management, knowledge management was also important for operating and maintaining IT systems (Newhouse et al., 2017). Skills in conducting information searches (Spink & Sollenberger, 2004), knowledge mapping (Humayun et al., 2020), and knowledge management technologies (Alstete & Meyer, 2019; Mehra et al., 2014) were essential because

cybersecurity threats and vulnerabilities be thoroughly researched for building organizational users' cybersecurity skills. Spink and Sollenberger (2004) conducted a study on mediated information search using organizational users to retrieve data on complex systems to resolve information problems. Their findings indicated that organizational users be skillful in multitasking; developing search terms, queries, and strategies; and using knowledge management technologies to optimize organizational users' skills. These skills were necessary when researching cybersecurity threats levied against organizations (Spink & Sollenberger, 2004).

To provide support and maintenance to an organization's IT system, organizational users possessed skills in technical support established by organizational processes and network services, develop and maintain systems specific to the organization's requirements, and conduct testing operations for systems security (Newhouse et al., 2017). Ben-Asher and Gonzalez (2015), as well as Sharma et al. (2019), noted that some of the most important responsibilities of organizational users were the protection of network resources and skill installing different hardware and software, such as firewalls and intrusion detection systems. Moreover, Sharma et al. (2019) revealed that network intrusion detection systems were constantly under attack because cyber-attackers were skillfully learning the algorithms to organization networks, and organizational users' cybersecurity skills should be constantly upgraded or improved upon to protect those networks.

To oversee and govern IT systems, organizational users required leadership and management who possess strong communication skills. Newhouse et al. (2017) posited that all levels of management within organizations possessed communication skills to effectively conduct cybersecurity work. Coffelt et al. (2019) contented that communication skills were some of the

most necessary skills for job requirements and stated that the definition of communication skills varies among organizations. Coffelt et al. (2019) noted that organizations requiring written communication skills were expecting organizational users to write effectively as a mode of communication. They described oral communication skills as effectiveness in speaking with other individuals and when conducting meetings. Further, they described visual communication skills as effectiveness in composing graphs, flow charts, or other types of data visualizations (Coffelt et al., 2019). Furthermore, soft and hard skills are requirements for IT leaders to effectively conduct cybersecurity work. Charoensap-Kelly et al. (2016) defined a soft skill as a type of skill that has little or no involvement with computers to complete the job. Soft skills are also known as interpersonal or people skills. Technical or hard skills require knowledge and the utilization of computers to complete the job. Wilkerson (2020) acknowledged the skills gap in organizational users and noted that institutions preparing students for the job market teach communication skills as one of the requirements for cybersecurity education. Additionally, Wilkerson (2020) revealed that IS organizational users believed that soft skills were more essential than technical or hard skills. However, Downey et al. (2008) revealed that both hard and soft skills were important for completing a job. Levy (2005) compared the management skills for online and on-campus Master of Business Administration (MBA) programs, noting that MBA programs were providing enhancements of managerial skills. Furthermore, Levy (2005) noted that skills included “a component of practical wisdom” (p. 2). These skills were comprised of analytical (technical), problem-solving (technical), and communications skills (soft and hard). Based on the literature review, the conclusion can be made that gaps exist within the literature as to which type of communication skills were most important to cybersecurity work.

Organizational users in leadership positions are required to possess skills in developing and overseeing organizational Information Security Policy (ISP). Whitman and Mattord (2018) defined ISP as written instructions by organizations informing organizational users about protecting information and organizational assets. They further noted that confidentiality is provided to protect the content of the information from unauthorized access. Haqaf and Koyuncu (2018) posited that information security management was essential for every organization that values their information assets. They also noted that developing and managing information security was a position reserved for expert organizational users to maintain continued security governance. Additionally, their findings indicated that developing and implementing IT security policies ranked among the highest skills required for information security management. Diesch et al. (2020) agreed with Haqaf and Koyuncu (2018) that skills in IT security policies were essential. They further indicated that the content of ISP be written with clarity and consider the interconnectedness of relevant information. Diesch et al. (2020) developed an expansive model of relevant success factors for organizational information security in which 19 industry experts validated their information security model. These success factors were identical with those of NIST (2018).

Security Education, Training, and Awareness (SETA) are some of the practical pursuits that would possibly ensure that organizational users obtain the cybersecurity skills necessary to prevent cyber-attacks. Diesch et al. (2020) acknowledged that training and development programs, as well as curricula and extensions of information security management, were previously skills reserved for technical expert organizational users. Further, they noted these responsibilities shifted from technical expert organizational users to management executives

(Diesch et al., 2020). However, both technical and management skills were required for a well-rounded approach to training and development. Ransbotham and Mitra (2009) postulated that a comprehensive and holistic training and development program required organizational users with technical skills and a business-focused perspective to protect information assets. Beuran et al. (2018) and Brillingaite et al. (2020) recognized the gaps in manual training programs in organizations due to a focus solely on technical skills. Utilizing the skills from technical and managerial executives, Beuran et al. (2018) designed and developed an automated cybersecurity training and development framework for organizational users to hone their technical as well as non-technical cybersecurity skills, while practicing with real-life cyber incidents. To evaluate the framework in terms of the functionality, they employed all the security testing and assessment techniques outlined in NIST (2017) guidelines.

A cybersecurity skills shortage was another problem acknowledged by several researchers (Brillingaite et al., 2020; Dodel & Mesch, 2019; Smith, 2018; Wilkerson, 2020). Brillingaite et al. (2020) recognized the increasing number of sophisticated cybersecurity threats and the shortage of skilled cybersecurity organizational users. They responded to the urgent demand for skilled organizational users by providing a training platform to emulate a real-life situation. Brillingaite et al. (2020) used cyber-defense exercises to mitigate cyber-attacks and provided training to organizational users. They designed these exercises for a group of organizational users with similar skills to practice, train, test, and verify their professional skills for cybersecurity preparedness. The cyber-defense exercises encouraged technical and non-technical organizational users to work together against cybersecurity threats.

Organizational users responsible for overseeing the training of personnel in the cyber domain were required to possess skills in IT network vulnerability. Whitman and Mattord (2018) defined vulnerability as a possible weakness in an organization system or in its defensive control systems. Organizational users should learn to identify the weaknesses in their network. Holm (2012) noted that to manually track, identify, and remediate network vulnerabilities in a sophisticated IT environment was a challenge for organizational users. Further, Holm (2012) posited that organizations were employing network vulnerability scanners to facilitate vulnerabilities. Holm (2012) also pointed out that network vulnerability scanners are software that organizations utilize to scan the architecture of a network, report any detected vulnerabilities, and recommend remediation. He further pointed out that organizational users be skillful when interpreting remediation guidelines provided from the vulnerability scanner (Holm 2012). The remediation guidelines were necessary to improve organizational network infrastructure and prevent future cyber-attacks (Holm, 2012). Moreover, Holm (2012) pointed out that some network scanners were not likely to detect vulnerabilities but were likely to provide remediation guidelines. Similarly, some network scanners were likely to detect network vulnerabilities, yet failed to provide remediation guidelines (Holm, 2012). Therefore, organizational users' skills were important to identify which scenario was better for the organization.

Bechtsoudis and Sklavos (2012) contended that organizational users not only possess skills in vulnerability detection, but also possess skills in penetration testing, which went beyond vulnerability detection. Whitman and Mattord (2018) agreed that penetration testing was a level of mastery beyond vulnerability testing and described penetration testing as a simulated attack by

a hacker. Whitman and Mattord (2018) further noted that penetration testing was categorized as either black box or white box. Within black box testing, organizational users have no prior knowledge of the organization's network infrastructure. Within white box testing, organizational users target a specific segment of the network infrastructure for specific vulnerabilities. Bechtsoudis and Sklavos (2012) confirmed that an organization's users be well-skilled in network infrastructure because specific tools used for different types of penetration testing were required to investigate network infrastructure flaws. Furthermore, Bechtsoudis and Sklavos (2012) pointed out that organizations with misconfigured network infrastructure or networks with design flaws might not reap the benefits from penetration testing. They posited that the tools used for penetration testing were not compatible with misconfigured network infrastructures. As a result, these organizations were not likely to conduct penetration testing due to misconfigured, dated network infrastructure and insufficient organizational users' skills in penetration testing (Bechtsoudis & Sklavos, 2012).

Organizational users required skills in social engineering to prevent unauthorized users gaining access to authentic information. Hatfield (2018) as well as Tetri and Vuorinen (2013) noted that organizational users possessed skills in impersonation given that hackers were utilizing advanced tools to trick organizational users in divulging organizational information to gain network access. Likewise, organizational users possessed skills in reverse social engineering to prevent the distribution of emails that contain malicious information. Hatfield (2018) stated reverse social engineering occurred when organizational users were tricked into initiating contact with other organizational users. Hatfield (2018) noted that organizational users possessed skills in identifying phishing emails because hackers were crafting emails that looked

identical to legitimate organizational emails. He further noted that these phishing emails were meticulously designed so that expert organizational users would experience challenges determining the authenticity (Hatfield 2018). Therefore, organizational users continuously hone their skills to identify any scenario of phishing.

To protect and defend organizational information assets, organizational users must possess skills in identifying, analyzing, and mitigating cybersecurity threats levied against organizational internal IT systems and networks (Newhouse et al., 2017). According to Menges and Pernul (2018), cyber-attacks on organizational networks were increasing, defense mechanisms were likely to fail, and the need to protect information assets was significant. They pointed out that protecting and defending these assets required organizational users' skills of information sharing in incident reporting. Incident reporting describes steps taken to report security threats or suspicious activities (Menges & Pernul, 2018). Organizational users must be able to identify and report phishing emails as well as any variations of suspicious activities (Alhogail, 2020; Menges & Pernul, 2018). Alhogail (2020) agreed that organizational users' skills in information security were necessary for mitigating risks and expenses. Also, Alhogail (2020) revealed that when organizational users shared information, they were improving the organization's information security incident response best practices, protecting the organization from malicious activities. Additionally, organizational users responsible for incident management must possess skills in utilizing organizational users' feedback to improve processes, products, and services as they relate to incident reporting (Newhouse et al., 2017). When organizational users report any indications of a threat, these reports must be documented to learn what happened and determine actions that can be taken to prevent cyber incidents. Using this feedback, organizations can

install automated email notification informing organizational users when an email is outside of the organization. Menges and Pernul (2018) noted that these incident reporting mechanisms might not close the gaps for cyber incidents but could minimize organizational users' reliance on intuition and assist them in honing their skills in recognizing phishing emails.

Organizational users must possess skills in analyzing and evaluating incoming cybersecurity information to determine the usefulness for intelligence (Newhouse et al., 2017). Further, Newhouse et al. (2017) pointed out that skills in threat analysis were essential to analyze cybersecurity information. When analyzing cybersecurity information, organizational users relied upon cybersecurity indicators to identify possible cybersecurity threats of one or more occurrences. Menges and Pernul (2018) defined a cybersecurity indicator as a signal that there are possible occurrences of an incident. Upon identifying these possible occurrences of cybersecurity threats, organizational users conduct deep web analysis to track Uniform Resource Locator (URL) addresses and determine the origin of the cybersecurity threats. Skills were also necessary to trace email addresses, mail servers, and mimicked email addresses. As an example, Hatfield (2018) noted that skilled organizational users utilized cyber indicators, deep web research, and email tracing to identify the cyber criminals and their country of origin responsible for the cyber-attack on the National Democratic Party during the 2016 presidential election. Skills in threat analysis were important when analyzing cybersecurity information; therefore, skills in threat analysis are included in this research.

Organizational users must also be skillful in the exploration of malicious network activities to ensure unauthorized cyber criminals do not have access to the organization's sensitive information, such as usernames, passwords, or credit card information (Newhouse et al., 2017).

Xiong et al. (2017) recognized that heavy network traffic rates in organizations lead to heavy processing and organizations tend to partition the traffic into multiple processors. Organizational users must be skillful in recognizing which network processors were subjected to malicious behaviors, while isolating and preserving the affected network packets for further analysis. Xiong et al. (2017) recognized the need for a robust network traffic partitioning scheme to defend against malicious cyber-attacks. They introduced a framework for easier recognition of malicious behaviors, isolating them for further analysis. Their findings revealed that the proposed scheme was more efficient than organizational conventional packet distribution performance when isolating malicious behaviors. Therefore, skills in analyzing cybersecurity information are included in this research.

Organizational users must possess skills in collecting cybersecurity information that was likely used for the development of intelligence (Newhouse et al., 2017). These skills were also necessary for specialized denial and deception operations for intelligence development (Newhouse et al., 2017). Sarker et al. (2020) affirmed that organizational users' skills in machine learning algorithms can be utilized to collect insightful cybersecurity incident examples from training data for organizational detection and prevention, rather than collecting data manually from network packets. An example of utilizing organizational users' skills in machine learning algorithms was when they formulate the mathematical computation associated with each cyber-threat and cyber incident to reveal hidden patterns in malicious activities.

Cyber events or crimes in organizations must be thoroughly investigated by organizational users. Organizational users must possess skills to investigate cyber events or crimes related to IT systems, networks, and digital evidence (Newhouse et al., 2017). Furthermore, Newhouse et al.

(2017) noted that cyber investigation was necessary for identifying, collecting, examining, and preserving the evidence from the cybersecurity threats or cyber incidents. Organizational users must be able to identify all relevant information that amounted to a cyber-threat or incident. Skilled organizational users were required to manually comb through weeks or months of evidence, normally unstructured data, to identify the attackers (Karafili et al., 2020). Karafili et al. (2020) recommended an augmentation-based reasoner that assisted organizational users during the investigative proceedings to analyze the evidence and to easily identify the cyber-attackers. The augmentation reasoner not only assisted in identifying the cyber-attackers, but also assisted in collecting new evidence, examining the evidence, and providing new investigative pathways for organizational users to follow. Karafili et al. (2020) also noted that once a cyber-attack happens, the process of attribution takes place, where the action of the cyber-attack gets assigned to a specific group of attackers. Digital forensics assist organizational users to investigate these cyber-attacks, but incomplete or conflicting data create a challenge. As an example, after a cyber-attack on the Democratic Party during the 2016 Presidential election, the evidence was available for organizational users to investigate. The massive number of emails and network packets was too much manual work even with digital forensics. An automatic reasoning base assisted the organization to identify, collect, examine, and preserve the evidence for further governmental investigation. This research employed SMEs to validate the cybersecurity skill needed for a cybersecurity competency framework necessary to investigate cyber-attacks. Table 5 describes the summary of prior research on cybersecurity skills.

Table 5*Summary of Cybersecurity Skills Literature*

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Alstete & Meyer, 2019	Organizational memory loss continued to be a problem for organizations when passing on knowledge from one generation to the next	Conceptual paper	A seven-layer framework	Knowledge layer	Intelligent agents significantly affected the retrieval, analysis, and knowledge management preservation
Carlton et al., 2019	Non-IT professionals' limited cybersecurity skills increase cybersecurity threats in organizations	Empirical study	173 non-IT professionals	Skills assessment	Skill-based assessment application significantly assisted non-IT professionals to mitigating cyber-attacks
Diesch et al., 2020	A scant research on the management success factors, their interplay, and the impact on organizations' information security	Empirical study via survey	136 articles	Management success factors	Provided a holistic model of the management success factors that were positively related to information security
Dodel & Mesch, 2019	Individual Internet users' inadequate computer safety compromises cybersecurity infrastructure	Empirical study via survey	1850 Israeli Internet users	Cyber-safety behavior	A structural and computer disparities directly as well as indirectly affect an individual's interest

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Haqaf & Koyuncu, 2018	A research gap exists in professional training programs required for honing skills needed for information security management	Literature review via survey	100 items	Information security skills	A comprehensive list of skills was required for information security management, training programs, and certifications
Holm, 2012	Manually tracking network vulnerability continued to be a problem for the compounded IT environment	Experimental study	Seven automated network vulnerability scanners	Assessment scanner	Provided mediation guidelines to secure organizations' networks
Karafili et al., 2020	The process of collecting information after cyber-attack was human-based	Literature review and synthesis	None	Cyber-attack	Developed a proof-reader to assist in the cyber-attack investigation, thus eliminating human intervention
Menges & Pernul, 2018	The design format suitable for specific cases of incidents reporting remains unclear	Literature review and synthesis	None	Evaluation criteria	Developed a comprehensive model for incident reporting to better assist in information sharing
Paananen et al., 2020	The purpose, definition, and development of Information Security Policy continued to an issue	Literature review using guidelines from Levy & Ellis, 2006	87 ISP articles	ISP development	ISP had different definitions based on the organization. Fragments of the definition led to ambiguity in the research field and results

Cybersecurity Abilities

Abilities Defined

Psychologists and their antecessors have struggled for over 100 years to uncover the nature of human cognitive abilities, questioning associative factors, such as if there is an abundance of distinct abilities that may be utilized individually or in association (Carroll, 1993). Carroll (1993) also questioned if general intelligence facilitated human cognitive abilities. Sternberg and Kaufman (1998) noted that experts at a 1921 symposium on intelligence and measurements defined intelligence as involving the importance of the ability to learn and adapt to varying conditions. Over six decades later, Sternberg and Detterman (1986) directed a similar symposium questioning experts on intelligence; again, adaptive abilities maintained their prominence. Thus, according to multiple researchers (Carroll, 1993; Sternberg & Detterman, 1986; Sternberg & Kaufman, 1998), the conclusion can be made that intelligence facilitates human cognitive abilities.

Human cognitive abilities can be described in multiple ways. Sternberg and Kaufman (1998) posited that three broad areas comprised human cognitive abilities: analytical, creative, and practical. They noted that analytical abilities were required to solve problems that existed in an individual's life. The concept of analytical abilities involved recognizing the presence of a problem, defining the nature of the problem, developing a solution for the problem, and monitoring the solution process. Creative abilities, according to Beaty et al. (2018), were required to solve open-ended problems. They also posited that creative organizational users had the capacity to conceive novel ideas to solve problems, such as designing and developing IT products to mitigate cyber-attacks. Practical abilities, according to Sternberg and Kaufman

(1998), were required to solve real-world problems. Alijughaiman and Ayoub (2012) provided clarification of practical abilities as a combination of organizational users' analytical and creative abilities applied to real-world open-ended problems. They also noted that organizational users with practical abilities were capable to work in an organization, successfully perform their new job role, and implement the required skills to complete the job. Expert organizational users with practical abilities are capable of realizing their true potential and accomplishing their goals.

Table 6 lists the summary research defining abilities.

Table 6

Summary of Abilities Defined Literature

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Alijughaiman & Ayoub, 2012	Identified gaps in NIST framework	Conceptual paper	Four frameworks	Cybersecurity framework	Proposed an additional compliance assessment process
Beaty et al., 2018	A clarification on the neurocognitive attributes that distinguish the highly creative brain is necessary	Empirical study via predictive modeling	163 participants	Divergent thinking	A significant relationship exists between creative thinking ability and self-reported creative behavior
Beaty et al., 2018	A clarification on the neurocognitive attributes that distinguish the highly creative brain is necessary	Empirical study via predictive modeling	163 participants	Divergent thinking	A significant relationship exists between creative thinking ability and self-reported creative behavior

Organizational Users' Cybersecurity Abilities

Organizational users working with IT must have analytical, creative, and practical abilities for job competency. Havelka and Merhout (2009) pointed out that no consensus exists regarding the KSTs for IT professionals. Their findings revealed that abilities were a fundamental competency for IT organizational users to realize their potential. Newhouse et al. (2017) underscored that abilities were required to securely provision IT systems and network development. Levy (2005) posited that organizational users' abilities were associated to their job performance, which was relevant for employment. Newhouse et al. (2017) acknowledged that the abilities organizational users must possess for risk management were the interpretation and application of laws, regulations, policies, and guidance relevant to organizational objectives. The practical ability required for risk management is the application of explicit and tacit knowledge combined with skills to write clear and concise information security policies free from ambiguities and misinterpretations. Buthelezi et al. (2016) noted that some of the problems with information security policies were the results of ambiguity in the language and a focus should be on increasing the clarity. A specific example of abilities when writing information security policies occurred when the user recognizes the language written for the password requirement was vague, even though the organizational objectives had specific password requirements. Buthelezi et al. (2016) further noted that organizational users' interpretations of password requirements caused non-compliance because of the ambiguities in the information security policy. While Newhouse (2017) acknowledged that abilities were necessary for cybersecurity mitigation, Buthelezi et al. (2016) noted that cybersecurity should serve as a competent task completion. Based on the literature, the definition of abilities is mixed with competency in

completing a task. Petersen et al. (2020) noted that abilities were necessary but not considered as building block for NICE Framework. Also, a focus must be on cybersecurity knowledge and skills, thus, sidelined abilities. Therefore, abilities are outside the scope of the research.

To operate and maintain IT systems and networks, organizational users must have the necessary abilities to provide support and maintenance, while ensuring performance, effectiveness, and efficiency (Newhouse et al., 2017). Further, Newhouse et al. (2017) noted that abilities in database management were important to operate and maintain organizations' systems. The specific abilities for data management include backup, restore, delete, and transaction log files. File system backup is necessary, as organizational users must be able to identify file sizes for consistency when preserving the data. Deka and Barua (2014) postulated that organizational users must also be able to analyze and evaluate the file system to determine the appropriate system downtime to conduct backup of organizational data. A large file system with petabytes of data took longer for file backup and was not ideal during an organization's normal working hours. Therefore, organizational users must possess the ability of effective time management. Time management was important not only for file backup, but also for file restoration and deletion. Zhang et al. (2018) emphasized that file restoration and deletion were important to database systems' operation and maintenance, but the execution time can affect organizational operation. They suggested that organizational users must be creative when restoring and deleting files.

Organizational users must have the ability to identify the knowledge management technology tools appropriate for their applications (Newhouse et al, 2017). Organizations processing petabytes of information required organizational users to have the ability to evaluate the

technological tools available to handle the volume of data. Additionally, they must also have the ability to find solutions for less common problems and the technological tools to solve more complex organizational problems.

To oversee and govern IT systems, organizational users must have abilities in cyber law to provide legal advice and advocate for organizations. Newhouse et al. (2017) posited that organizational users serving in the capacity to provide legal advice must be able to oversee and evaluate the potential impact of emerging technologies on laws, regulations, and policies as it relates to cybersecurity. Abilities were also necessary when developing, updating, and maintaining standard operating procedures (Newhouse et al., 2017). A specific example of abilities to oversee and govern occurs when an organizational user violated security policies; the legal advisor for the organization must evaluate the violation and determine the necessary legal action.

Newhouse et al. (2017) also stated that organizational users coordinating cybersecurity training and development programs in organizations must have the ability to develop training programs in a virtual environment. Furthermore, abilities are required to develop clear directions and instructional materials. Organizational users coordinating cybersecurity training programs must be able to utilize critical thinking abilities to develop tools that can enhance organizational users' cybersecurity abilities. Beuran et al. (2018) recognized the need for cybersecurity training and development programs in organizations and developed an automated content generation program for cybersecurity training to improve accuracy. Beuran et al. (2018) noted the effectiveness of cybersecurity training and provided manageable descriptions with fewer complexities. Similar to Beuran et al. (2018), this research organizations would be able to

determine organizational users' cybersecurity abilities, thereby aligning training and development programs according to those abilities.

Ben-Asher and Gonzalez (2015) acknowledged that human cognitive and analytical abilities were required for the successful detection of cyber-attacks. Moreover, they stated that organizational users must identify the most appropriate intrusion detection technologies for recognizing host- and network-based intrusions. Their findings indicated that organizational users must learn to summarize and examine feedback to improve their ability when detecting novel cyber-attacks.

According to Newhouse et al. (2017), organizational users must have the abilities to protect and defend internal IT systems and networks. Further, Newhouse et al. (2017) noted that organizational users must be able to analyze malware. D'Elia et al. (2020) recognized organizational users' struggle to analyze malware, while noting the same struggle occurred with automated systems. To address the analysis gap, they proposed a system for transparency with manipulation capabilities, a requirement when dissecting malware. With the introduction of this customized tool, organizational users can spend less time analyzing malware. Additionally, organizational users responsible for protecting and defending the internal IT systems and networks must have abilities in cloud computing. NIST (2011) described cloud computing as a "model for facilitating on-demand network access to a shared pool of configurable computing resources that requires minimal management effort or service provider interaction" (p. 2). Ab Rahman and Choo (2014) recognized a knowledge and ability gap when reporting incidents in cloud computing due to shared networks. To narrow the ability gap, they proposed a model combining cloud incident handling with digital forensics principles to better enhance

organizational users' capabilities when reporting cloud computing incidents. Ab Rahman and Choo (2014) indicated that, of the 139 articles reviewed, only a small number of studies underscored the potential of combining incident handling and digital forensics because of the high cost and the varied abilities of organizational users. Therefore, this research did combine incident handling and digital forensics, thus allowing organizations the opportunity to prepare for each task separately.

Organizational users must have analytical, creative, and practical abilities when analyzing cybersecurity information for intelligence purposes (Pettersen et al., 2019). Organizational users require analytical abilities to decipher complex cybersecurity information threats (Newhouse et al., 2017). Their creative abilities should encompass production of written cybersecurity materials and visual aids to depict complex information or ideas (Newhouse et al., 2017). Organizational users must have the practical abilities to communicate effectively with others when discussing cybersecurity information (Newhouse et al., 2017). Organizational users having the analytical, creative, and practical abilities were required to make recommendations necessary for problem-solving and situations where cybersecurity threat information was incomplete or inconsistent when analyzing cybersecurity threats.

Organizational users' shared abilities are required when collecting cybersecurity information. More specifically, Newhouse et al. (2017) postulated that the application of shared skills and strategies was essential for collection management and development of concepts to meet organizations' objectives. Archer and Cameron (2009) recognized the gap in collaborative skills among expert organizational users' capabilities. They interviewed 100 expert organizational users, which revealed that shared skills were essential when forming new alliances, a necessity

for collecting information. Furthermore, the ability to maintain relationships and resolve conflicts with stakeholders was crucial when developing cybersecurity intelligence.

Organizational users must have the ability to investigate cyber-attacks or incidents concerning IT systems and networks (Newhouse et al., 2017). Further, they must have the ability to identify and maneuver the dark web using specific networks to find the markets and forums of cyber-attacks (Newhouse et al., 2017). Saleh et al. (2018) described the Internet as the gateway for conducting business and providing services to public and private sectors globally. They further noted that the Internet created a lack of privacy, and several networks, such as TOR, provided an anonymous communication network to protect organizational users' identities. Likewise, organizational users must use the TOR network to investigate unscrupulous users attempting to gain access to the organization's network. Saleh et al. (2018) revealed that the TOR network was the design of a data breaching strategy, and organizational users must have the ability to track these data breaches.

Several researchers noted that organizational users must have the ability to competently complete a cybersecurity task (Buthelezi et al., 2016; Newhouse et al., 2017; Saleh et al., 2018). Whereas Archer and Cameron (2009) recognized organizational users' cybersecurity skills gap was attributable to abilities. A majority of the literature classified cybersecurity abilities as either skills or knowledge. Petersen et al. (2020) recognized that cybersecurity abilities were necessary for cybersecurity mitigation but not a cybersecurity competency. Table 7 describes the summary of prior research on organizational users' cybersecurity abilities.

Table 7*Summary of Organizational Users' Cybersecurity Abilities Literature*

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Archer & Cameron, 2009	Currently, there is an ability gap in collaborative leadership in the public and private sectors	Literature review via interviews	100 public and private sector directors	Leadership	The results identified the abilities required for collaborative leadership
Ben-Asher & Gonzalez, 2015	The cognitive process required for adequate network protection was limited	Empirical study via questionnaire	55 participants from the university	Organizational users' competency with intrusion detection system	Competency played a role in detecting cyber-attacks
Beuran et al., 2018	Even though countries were providing cybersecurity training and development programs for individuals, the background tools were not beneficial to the public	Empirical study	Three countries	Cybersecurity training activity	Implemented a cybersecurity training framework aimed to improve participants' cybersecurity skills and abilities
Buthelezi et al., 2016	Information security policies were prone to ambiguities	Case study	Ten information-security-related policies	Ambiguity themes	Policy writers must possess the ability to write clear and concise information security policies
D'Elia et al. 2020	Automatic characterization of malware process continued to struggle with manual intervention	Case study	One system	Malware dissection	Designed an automatic-manual transition system for dissection malware

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Havelka & Merhout, 2008	Scant research to find a consensus on the required KSTs for IT professional jobs	Empirical study via survey	Nine participants	Theory of IT professional competency	Abilities and skills were fundamental to IT professional jobs
Levy, 2005	Even though online learning in higher education created success for universities, a focus on online MBA programs' advantages to students raised questions	Empirical study via longitudinal study	One online MBA program One on-campus MBA program	Learning skills profile	Both online and on-campus MBA programs significantly influenced skills
Pettersen et al., 2019	Universities continued to struggle with training and development that influenced creative thinking	Empirical study via longitudinal study	99 undergraduate students	Practiced-based creativity tool	Education strengthened the development of creative ability more than the willingness to be creative
Razali & Trevelyan, 2012	limited information is available on the practical ability of students in a laboratory class	Empirical study via survey	139 students	Practical intelligence	Students were motivated to gain the practical abilities necessary to become practicing engineers
Saleh et al. 2018	Limited privacy when using Internet protocol led to the use of anonymous communication networks	Empirical study via survey	120 articles	TOR network	No consistent standards used for the TOR network in performance analysis, mainly through latency analysis

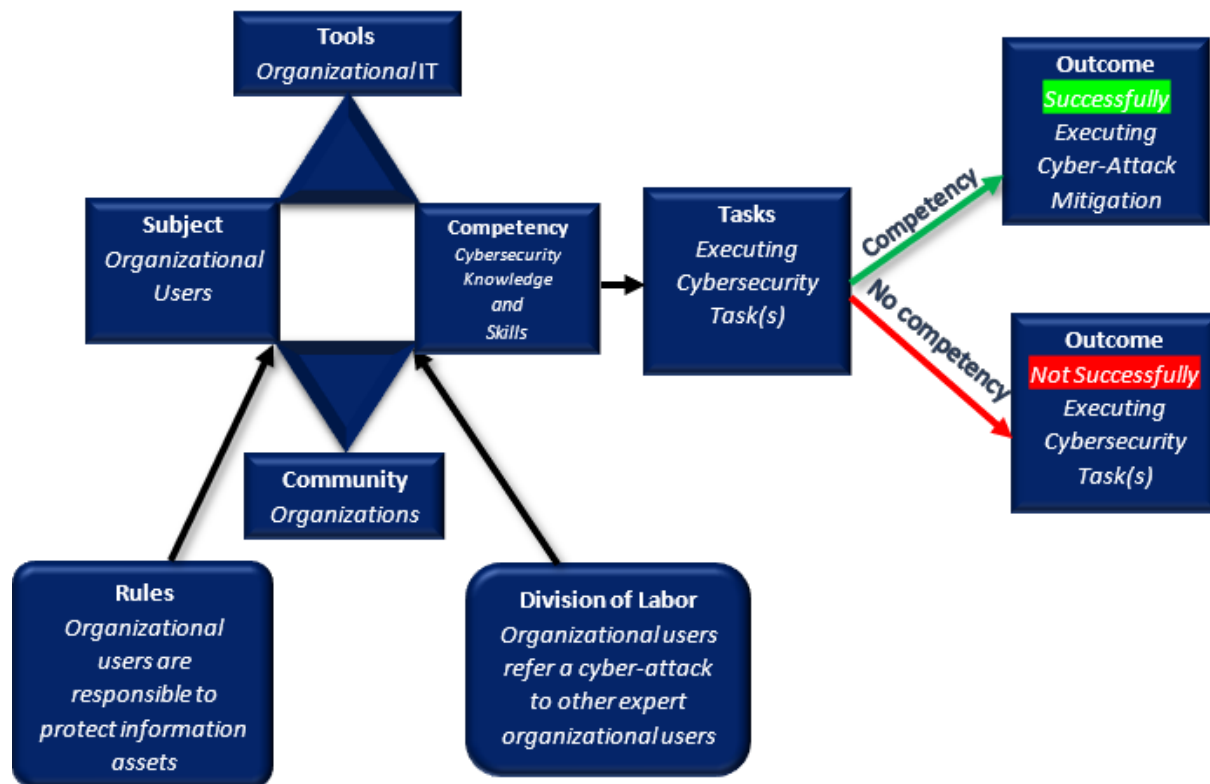
Cybersecurity Tasks

Activity Theory

A group of Russian psychologists in the 1920s developed the activity theory that is currently explored across multiple academic disciplines. Based on the concept of activity theory and other research, Bracewell and Witte (2003) formulated the definition of tasks “as the set of goals and actions that implement these goals, which are developed to achieve a solution to a complex problem within a specific work context” (p. 18). The application of activity theory in the context of cybersecurity mitigation focused on organizational users is shown in Figure 4.

Figure 4

Cybersecurity Mitigation Activity



One aspect of cybersecurity is to protect organizational information assets (Al-Safwani et al., 2018). The cybersecurity mitigation activity depicts the collective nature of work activities, similar to the medical profession's multi-professional teams (Engeström, 1999). The cybersecurity mitigation activity demonstrates the most significant features as the Tools (organizational IT, i.e., networks) and the Action (cybersecurity tasks) based on the organizational objectives. According to Engeström (1999), aside from the tools and activities, the most significant constructs were the mediating factors, rules, and division of labor. The subject (organizational users) influences division of labor, where organizational users refer cyber-attacks to expert organizational users. Together, these organizational users are part of the community, given that they work within the organization. The rules are influenced by competencies (KSTs). Organizational users with limited cybersecurity competencies (KSTs) might not meet the organizational rules to protect information assets. Likewise, competent organizational users could meet the organizational rules, protect information assets, and execute cybersecurity tasks, thus mitigating cyber-attacks.

NCWF Tasks

Organizational users must be able to perform the tasks that provide solutions to cybersecurity problems in organizations. During the research to determine the tasks required for NCWF, Newhouse et al. (2017) underscored that organizational users must perform tasks in risk management by studying, designing, and developing secure IT systems, as well as in networks. Moreover, Al-Safwani et al. (2018) observed that eliminating risks was not possible. Instead, they recommended that organizational users must perform tasks in risk management by reviewing their risk management policies to confirm the acceptable level of risk for software, IT

systems, and networks, respectively. Likewise, Meyer et al. (2020) confirmed the necessity of organizational users performing several tasks utilizing fuzzy logics to develop modern energy grids to minimize security risk.

To operate and maintain IT systems and networks, organizational users' tasks were salient. Newhouse et al. (2017) posited that organizational users must perform the required tasks to aid, administer, maintain, and ensure IT systems and network performance effectiveness. Deka and Barua (2014) acknowledged that database management tasks were necessary to safeguard against data loss and corruption, as well as to retain old files for future reference. Even though Deka and Barua (2014) recognized that database backup tasks were necessary, organizational users often neglected to perform such tasks. Deka and Barua (2014) proposed a scheme for consistent backup of an active file system that supported online transactions, eliminating organizational users' neglectfulness. Based on Deka and Barua (2014) recommendations, this research included database management as an observable task within the workforce. Organizational users must perform knowledge management tasks to assist organizations in determining and documenting information content (Newhouse et al., 2017). Sarnikar and Deokar (2017) agreed with Newhouse et al. (2017) that organizational knowledge management was continuously evolving. Instead of a rigid information system, organizations must adopt knowledge-based systems that fully support technological changes for IT performance and security. Sarnikar and Deokar (2017) also noted that organizational users must be able to perform tasks in system analysis and design techniques to allow for easier adoption of the system. Based on Sarnikar and Deokar (2017) recommendations, this research included robust knowledge management systems within the workforce.

Tasks in leadership and managerial development were required when overseeing and governing cybersecurity work. Newhouse et al. (2017) declared that organizational users must offer legal advice and advocate for relevant topics on cyber law. Furthermore, Newhouse et al. (2017) pointed out that organizational users must also demonstrate the task of evaluating the effectiveness of the law, regulations, policies, and standard operating procedures. Organizational users must also perform tasks using risk assessment tools to assess the organization's cybersecurity risk levels and provide senior executives information about its security posture (Brunner et al., 2020). Similar to Brunner et al. (2020) research, this study included risk management assessment as part of the framework.

Organizational users demonstrate tasks in training and development on cybersecurity work. Newhouse et al. (2017) postulated that, when overseeing and governing, organizational users must demonstrate tasks in writing cybersecurity training manuals based on their physical environment and the organizational requirements, as well as conduct periodic evaluations of the cybersecurity training manuals to ensure they have been updated with the latest cybersecurity information. Karjalainen (2020) recognized the necessity of organizational information security policies while proposing that organizations tailor their training and development toward organizational users' information security behavior. Karjalainen (2020) revealed that organizational users' compliance with information security policies occurred gradually, leading to a routine over time. Therefore, organizational users responsible for information security policies wrote those policies according to the organizational users' information security behavior. This research included training and development as a required task for organizational users.

To protect and defend organizational internal IT systems, networks, organizational users demonstrated tasks in identifying, evaluating, as well as mitigating threats levied against organizations (Newhouse et al., 2017). Ben-Asher and Gonzalez (2015) pointed out that organizational users demonstrated tasks in developing cyber defense tools to mitigate cyber-attacks. As an example, hackers relied upon sniffers to gain access to organizational networks. Organizational users could utilize cyber defense tools to identify these sniffers trying to achieve unauthorized access to their networks and deny this access. Once hackers gain access to organizations' IT systems or networks, they could access confidential information (Ben-Asher & Gonzalez, 2015). Ben-Asher and Gonzalez (2015) indicated that expert organizational users were more capable of utilizing cyber defense tools than were less experienced organizational users. This research provided the tasks necessary to identify organizational users' capabilities and to delineate areas for improvement.

Cyber-attacks levied on organizations must be analyzed. Organizational users demonstrated the tasks of investigating, evaluating, and responding to cybersecurity threats resulting in cyber incidents in organizations' networks. Menges and Pernul (2018) pointed out that more technologically advanced tools utilized by hackers contributed to cyber incidents, and these incidents were reported. Moreover, Menges and Pernul (2018) pointed out a gap when organizational users report cybersecurity incidents. They noted that organizational users investigating cybersecurity incidents demonstrated tasks in information sharing with different stakeholders to avoid ambiguity problems and the gap in reporting cyber incidents. Similarly, organizational users demonstrated the task of evaluating network packets to identify the affected network(s) with minimal interruption to daily organizational activities (Menges & Pernul, 2018).

Organizational users demonstrated the tasks of seamlessly transferring affected networks to a secure network, while preserving the affected network for further investigation. Menges and Pernul (2018) further stated that when evaluating cyber incidents, organizational users demonstrated reading machine language tasks to definitively know the extent of the damage caused by the cyber-attack. Their findings revealed one form of the incident-reporting formats provided only limited task information about cyber-attacks. This research addressed such a limitation by providing a comprehensive list of tasks when reporting cyber-attacks as outline in the NCWF (NICE, 2017) specialty area for investigating cyber-attacks.

The collection and operation of cybersecurity information were necessary for denial and deception operations (Newhouse et al., 2017). Newhouse et al. (2017) posited that organizational users must collect and evaluate inbound cybersecurity information to establish any credence for intelligence purposes. They further pointed out that organizational users demonstrated the task of reviewing collected cybersecurity information for accuracy and pertinence. The review of cybersecurity information was necessary when determining the type of denial and the deceptive operations organizations conducted when testing their cybersecurity posture. Heckman et al. (2013) conducted a real-time cyber-operation experiment dividing organizational users into red and blue teams, then performing cyber-attacks against each team. Heckman et al. (2013) indicated that one team was not effective in denying adversary access to real-time information. Their limited competency was the result of not recognizing false information in real-time. This research prepared organizational users with the necessary knowledge and skills to competently complete the task of collecting information from the cyber-operation.

Cybersecurity events levied against organizations were investigated. Newhouse et al. (2017) posited that organizational users demonstrated tasks investigating cybercrimes focusing on collecting, processing, and analyzing cybersecurity forensics. Pătrascu and Patriciu (2013) defined cybersecurity forensics as “the application of computer analysis and investigation techniques to gather evidence suitable for presentation in a court of law” (p. 457). Newhouse et al. (2017) further noted that organizational users demonstrated tasks in communicating with other organizational users involved in cybersecurity incidents when investigating cybercrimes. Karie et al. (2019) agreed that communication between cybercrime investigators and other organizational users was necessary when gathering evidence to assist in litigation. They further pointed out that a significant amount of evidence collected from cybercrime scenes came in multiple sources and varying file formats. To mitigate the problem, they proposed a generic framework Deep Learning cognitive tool to process the large volume of data collected from cybercrime scenes. Their findings revealed that well-protected evidence assisted cybersecurity investigators and law enforcement when investigating cybercrimes. Similar to Karie et al. (2019), this research provided organizational users with the necessary knowledge and skills essential to complete the tasks to investigate cybercrimes. Table 8 describes the summary of prior research on cybersecurity tasks.

Table 8*Summary of Cybersecurity Tasks Literature*

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Al-Safwani et al., 2018	The lack of practical guidelines based on expert opinion is necessary	Empirical study	One model	Risk assessment	Developed a model with distinct guidelines for control analysis in a structured approach
Ben-Asher & Gonzalez, 2015	The cognitive process required for adequate network protection was limited	Empirical study via questionnaire	55 participants from the university	Organizational users' competency with intrusion detection system	Competency played a role in detecting cyber-attacks
Deka & Barua, 2014	Limited research has been conducted for an online backup file system	Experimental study	Two file systems	File system	Implemented a scheme for consistent online backup
Heckman et al., 2013	Although organizations continued to perform denial and deception operations, vulnerabilities remained a problem for organizations	Experimental via scenario	Two teams Red/blue	Cyber-wargame	A continuous need to experiment with cyber-wargames to enhance the defense of cybersecurity information
Karie et al., 2019	A lack of computing techniques for organizational users created a struggle to sift through a large volume of digital forensics data	Literature review	None	Deep learning	Developed a framework for deep learning techniques to assist in digital forensics

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Karjalainen et al., 2020	Human errors continued to be a challenge for organizations	Empirical study via interview	77 face-to-face interviews	Information security policy	Failure to comply with information security compliance occurred in stages from initial beliefs and later developed into routine practice
Menges & Pernul, 2018	The design format suitable for specific cases of incident reporting remained unclear	Literature review and synthesis	None	Evaluation criteria	Developed a comprehensive model for incident reporting to better assist in information sharing
Meyer et al., 2020	Organizational users continued to face challenges to securely protect energy grid power systems	Case study	One optimization algorithm	System protection security assessment	The protection of the power system was more effective due to the optimization algorithm
Pătrascu & Patriciu, 2013	Limited information on the usage of cloud computing and digital forensics	Literature review	None	Cloud forensics	Proposed a unique way to oversee cloud environment over numerous datacenters

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) Literature

Cybersecurity is an emergent body of work that translates into professional development (Shoemaker, 2015). Shoemaker (2015) also noted that the cybersecurity was too involved to be isolated as electronics. Francis and Ginsberg (2016) as well as Shoemaker (2015) pointed out

that NIST (2011) and the Department of Homeland Security (DHS) developed the NICE framework outlining the complete range of KSTs required for the cybersecurity workforce. The framework included a consistent lexicon that classified and categorized cybersecurity work, as well as provided the first complete definition of cybersecurity. They further noted that NIST and NICE were responsible for defining and creating the standards that govern cybersecurity in the professional world as well as in educational training and development. Shoemaker (2015) acknowledged the NCWF brought stability to the cybersecurity domain, and also argued cybersecurity was portrayed less authoritatively before the framework. He further pointed out that the preparation and culmination of NCWF, a meticulous process, took three years. Francis and Ginsberg (2016) as well as Shoemaker (2015) noted that because of the preparation, the NCWF, now broadly considered to be authoritative, incorporated all cybersecurity domain professions and mastered the body of knowledge, thus, creating a unified structure referenced globally.

Newhouse et al. (2017) posited that the NCWF categorized cybersecurity work under specialty areas, which are grouped into seven categories. Newhouse et al. (2017) further pointed out that the framework listed the job descriptions under each specialty area, along with the required KSTs for the organizational users. The detail-oriented framework furnished organizations and educational institutions with concrete and official descriptions of the cybersecurity knowledge and skills required to perform cybersecurity tasks (Shoemaker, 2015). Even though the framework contained the cybersecurity KSTs, the competency to determine the threshold for the KSTs was necessary. This research determined the competency for KSTs, a necessity for cybersecurity mitigation.

Competency

Competency Defined

Competency has been studied in various domains, such as the public sector (Horton, 2000), healthcare (Englander et al., 2013), human resource development (Le Deist & Winterton, 2005), cybersecurity (Fonseca & Ng-Picoto, 2020; Tobey et al., 2018), and the IT sector (Bassellier et al., 2016). Yet, the definition varied throughout those studies. Boyatzis (1982) noted that competency consisted of multiple components that differentiated successful and less successful organizational users. He stated that the components were personal characteristics, experience, motives, habits, and attributes. Boyatzis (1982) defined competency as fundamental qualities of an individual that are closely connected to effective or superior work performance. Woodruffe (1991) explained competency as an area of a job in which an organizational user could perform well. Johnson et al. (2008) noted the distinction between competency and core competency. He indicated that competency was the coupling of “skills and abilities by which resources are deployed through an organization’s activities and processes” (p. 96). However, core competency differed in that it is used to achieve a competitive advantage in a manner other organization cannot replicate or obtain (Johnson et al., 2008). An example of competency was an organizational user having the skills and abilities to process identity theft claims occurred in the company but lack the core competency to block the theft from occurring. Whereas an example of core competency was that one specific company in the retail industry no longer encounters identity theft, while other retail industry companies suffer from identity theft. The company executives later found out that a group of organizational users designed and developed an intrusion detection device to recognize and block identity theft. Other companies could not

eliminate identity theft because of the unique set of knowledge, skills, and abilities only reside with those employees at that specific retail company. Similar to Boyatzis (1982), Le Deist and Winterton (2005) noted that competency was a fuzzy logic that was closely defined as a characteristic that propelled superior job performance that included KSTs, traits, and habits. Le Deist and Winterton (2005) also noted the definition of competency used in three continents varied because of the inconsistent usage of the word competency. Boak (1991) contended that competency was the preferred terminology in North America, whereas, in Europe and Australia, the preferred terminology was competence. Englander et al. (2005) noted that scholars during the 1990s referred to competency as a behavioral approach, a tradition in the United States.

Tobey et al. (2018) underscored the complexity of competency while presenting arguments to emphasize that a deconstruction of the concept was necessary to better understand it and to provide a glossary. They pointed out that most scholars equated competency as KSTs and the performance of job tasks. They emphasized that organizations placed a threshold on competency to measure the KSTs, which were components of competency. Tobey et al. (2018) defined a threshold as a “transition point or liminal space that determines the level of competency” (p. 25). They defined competency as a “comprehensive and accurate understanding of the absence of ignorance, misunderstanding, and misconception” (Tobey et al., 2018, p. 36). According to Tobey et al. (2018) these definitions were necessary to better understand competency.

Cognitive intelligence was the preferred methodology when testing organizational users' competency but was later described as an ineffective methodology. Thus, competency replaced cognitive intelligence (Englander et al., 2005). Englander et al. (2005) further pointed out that organizations measured competency by observing organizational users' identifiable performance

differences. Subsequently, skills and cognitive abilities were identified as components of competency. In an earlier study, Jeris and Johnson (2004) pointed out that through accreditation agencies, curricula, and qualifying examinations, organizations worldwide accepted KSTs as competency components. Evers et al. (1998) acknowledged that the most holistic competency framework included knowledge, skills, abilities, and job tasks. Moreover, Lucia and Lepsinger (1999) confirmed that organizations typically utilized a competency framework to connect the Human Resource Department with organizational strategies. Lucia and Lepsinger (1999) described the competency framework as an analytical tool to determine the KSTs needed to perform job roles in organizations effectively and assist in accomplishing their strategic management. Table 9 lists the summary research defining competency.

Table 9

Summary of Competency Defined Literature

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Bassellier et al., 2001	Limited competence with IT line managers	Literature review and synthesis via interviews	Two sets of literature articles	Explicit and implicit knowledge	Developed a theoretical model linking IT competence and business technology leadership
Englander et al., 2013	A limited taxonomy for competency domains and specific competencies were unavailable	Empirical study	48 competencies and eight domains	Competency	Developed a taxonomy of health professional competencies

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Fonseca & Picoto, 2020	The challenges of digital information forced companies to re-evaluate their strategic development of competencies	Exploratory study	16 professionals	Digital transformation	The results revealed the digital competencies necessary for organizational re-evaluation
Horton, 2000	The origin of competency management in two countries continued to be of concern, while the need for effective and efficient public sector managers was increasing	Literature review	Five articles	Competency movement	The need for competency-based management was significant, but no agreement existed on the specific set of competencies required for managers in the public sector
Le Deist & Winterton, 2005	The definition and usage of competency have been inconsistent across three continents	Literature review	Five countries	Comprehensive model of competency	Developed a framework identifying the combination of competencies for specific occupations and upward mobility
Tobey et al., 2018	Although competency had been used as a multidimensional construct, the definition of competence remained complex	Literature review	None	Competency assessment	Developed a glossary of terminologies bringing clarity to competency-based assessment for cybersecurity reference

NIH Competency Framework

The competency framework allows organizational users to know the competency level that supports their career goals and assists organizations in making strategic decisions to address

competency gaps. The competency also underscored the areas in which organizational users were most proficient and areas where training and development were needed to promote their professional development (NIH, 2020). Boyer et al. (2020) confirmed that competency determines the tasks for each job role. Boyer et al. (2020) also acknowledged that organizations benefitted from utilizing a competency measure because it helped clarify the training and development necessary to promote career growth. Gander (2006) maintained that a well-constructed competency framework with components of competency outlining job roles was insufficient without an assessment of competency to determine the job roles across the organization.

Cybersecurity Competency

Organizations continued to assess their organizational users' competency by relying upon a vetted competency measurement or creating their scalability standards. Gander (2006) stated that a taxonomy of competency was required to assess organizational users' cybersecurity performance. Moreover, several researchers acknowledged that competency was built in stages and developed over time (Ayres et al., 2012; Carpenter, 2017; Cornford & Athanasou, 1995; Gander, 2006; Schrimmer et al., 2019; Soundaram & Pon-Reka, 2008).

Gander (2006) recommended that the competency should start at the lowest level. Carpenter (2017) as well as Soundaram and Pon-Reka (2008) referenced the NIH competency framework starting at the lowest level and progressing to the highest level. *No competency*, organizational users does not have the cybersecurity knowledge and skills to competently complete cybersecurity tasks. *Fundamental awareness* is the cybersecurity knowledge required for organizational users when understanding cybersecurity information. Ben-Asher and Gonzalez

(2015) recognized that *novice* organizational users had limited experience when detecting malicious cyber-attacks, and knowledge must be developed at an *intermediate* level to make a detection decision accurately. Carpenter (2017) referenced the NIH competency framework as a Likert-scale to identify the KSTs for organizational users' job positions. Their findings revealed that a significant number of the 500 respondents ranked themselves at the *advanced* level because, at that level, an organizational user would have mastered cybersecurity complexity. Carpenter (2017) also revealed that fewer organizational users were interested in training and development at the *expert* level because of the mastery required for cybersecurity work.

Soundaram and Pon-Reka (2008) utilized the NIH competency framework in a study to determine the IT employees' competency in small, medium, and large organizations. They further noted that organizations regularly assessed IT employees' competency to prepare for their training and development programs. To determine the employees' competency, they utilized the NIH competency framework. Their findings revealed that the IT employees in medium-size organizations had a slightly higher competency than IT employees in small and large organizations, especially results driven by competency. Although their research focused on the organizational size, the NIH competency framework is applicable to any organization. This research utilized the NIH competency framework in the context of cybersecurity to determine organizational users' cybersecurity competency not only for cybersecurity professionals, but for non-professional across the organizations.

A summary of research regarding the NIH competency framework and its application follows in Table 10.

Table 10*Summary of NIH Competency Framework Literature*

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Ayres et al., 2012	One particular healthcare sector failed to address the need for information competencies	Empirical study via longitudinal study	30 participants	Competency	A significant number of the participants were assigned to the intermediate level, fewer assigned to the advanced level
Ben-Asher & Gonzalez, 2015	The cognitive process required for adequate network protection was limited	Empirical study via questionnaire	55 participants from the university	Organizational users' competency with intrusion detection system	Competency played a role in detecting cyber-attacks
Boyer et al., 2020	A limited continuing development nurse competency framework was available	Empirical via survey	42 nurses	Competency development	Developed a nursing competency framework for nurses
Carpenter, 2017	A difference in competency with two set of employees	Empirical study via survey	376 employees	Competency scale	The competency scale revealed the level of dispersion among the employees
Cornford & Athanasou, 1995	Limited research in Australia on skills acquisition for the development of an individual from beginner into an expert	Conceptual paper	None	Developing experts using the competency framework	Competency was incremental, acquiring skills and knowledge with a purposive goal and desire to be an expert

Study	Description of the Problem Theory	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Gander, 2006	Limited information for organizations to develop and measure competencies	Conceptual paper	None	Learning to develop a competency indicator scale	Provided instructions for developing competency
Schrimmer et al., 2019	Little uniformity is available in the definition of competencies and an essential requirement for healthcare quality	Literature review and synthesis, comparative analysis via group interviews	Six work groups	Competency	Developed a quality competency framework using a three-tiered competency to identify observable behaviors
Soundaram & Pon-Reka, 2008	Addressing the competency gaps in the organization	Empirical study via questionnaire	250 employees in IT industry	Competency and nonparametric testing	The competency differed according to size of the company

Summary of What is Known and Unknown

A review of various aspects of cybersecurity literature was conducted to provide the groundwork for this research. The literature review provided a portrayal of what is known and unknown about the cybersecurity competency framework (Dawson & Thomson, 2018; Newhouse et al., 2017). To effectively manage cybersecurity, various countries created guidelines or frameworks for training and development. Throughout the literature review, cybersecurity KSTs were required to complete job tasks. According to Nonaka (1991), knowledge creation was fundamental in understanding cybersecurity mitigation. Over time, organizational users' cybersecurity knowledge matured, thus, improving their skills and abilities

to mitigate cyber-attacks (Toth & Klein, 2014). Even though organizational users' matured knowledge improved their skillsets, globally, organizational users' cybersecurity skills were in short supply, yet essential for mitigating cyber-attacks (Crumpler & Lewis, 2019). Tobey et al. (2018) noted that skills must be measured, as they are a component of competency.

The NIH competency framework has been used in the fields of medicine, aviation, social justice, and human resources. In the medical profession, a Clinical Research Coordinator and Registered Nurse competencies were different because of the KSTs required for the job task (Rojewski et al., 2019). The measurement for organizational users' cybersecurity competency appeared to be absent from the literature. Thus, this research designed, developed, and validated the universal CCF to determine organizational users' KSTs referencing the NCWF.

Chapter 3

Methodology

Overview of Research Design

This research study was classified as developmental and conducted in three phases to design, develop, and validate a universal CCF using the NCWF KSTs. Ellis and Levy (2009) described developmental research in the context of researchers building a “thing” to answer a problem (p. 1). Klein (2013) agreed that developmental research utilizes a study to design and develop an entire process, or it utilizes parts of the components of a process to answer research questions. To answer the research questions, an explanatory sequential mixed method approach was performed.

The goal of this chapter is to explain the research method and the research design process employed in this research study. The chapter also explains the survey instrument development, the instrumentation and its appropriateness, study population, and the sample size. Finally, this chapter explains the procedures and techniques of the data collection and the reasons behind utilizing such techniques. Thereafter, discussions are provided on the instrument reliability and validity, the approach adopted to ensure the reliability and validity of the gathered data, and the statistical analysis methods used.

Research Method

Tashakkori and Creswell (2007) broadly defined mixed methods research as the collection and analysis of quantitative as well as qualitative data. Creswell (2014) pointed out that multiple forms of mixed methods designs exist. However, the commonly used mixed methods are

convergent parallel, explanatory sequential, and exploratory sequential. In the explanatory sequential (quantitative-qualitative) mixed methods, the study collects the quantitative data, analyzes the results, and builds on the results to formulate the qualitative research. This research study employed the explanatory sequential mixed method approach to answer the research questions.

Creswell et al. (2003) pointed out that explanatory sequential design has two distinct phases: quantitative and qualitative. In the quantitative phase, the research study utilizes a survey instrument to collect and analyze numeric data. The result from the quantitative phase builds the data collection instrument for the qualitative phase. The qualitative phase collects the data through an interview or questionnaire to explain the results from the quantitative phase. At this stage, Fetters et al. (2013) conceptualized that the quantitative and the qualitative data integration occurred at the methods level through linking both databases in several ways: connecting, building, merging, and embedding. Fetters et al. (2013) pointed out that the integration at the methods level *connects* the quantitative and qualitative data through sampling. The *building* occurs when one data collection procedure informs the other data collection procedure. The *merging* takes place by bringing together both the quantitative and qualitative databases for further analysis and comparison. The *embedding* involves linking the data collection and analysis at several points.

Fetters et al. (2013) also noted that in the explanatory sequential mixed method approach, the integration of the quantitative and qualitative data occurs at the interpretation and reporting level using the narrative approach. The integration at the interpretation and reporting level occurs when the quantitative and qualitative data are amalgamated to show that they were more

informative than a single result (Creswell, 2015; Fetters et al., 2013). McCrudden and McTigue (2019) noted that integration of the reports includes converting one data type into another by applying a code to qualitative data, then converting coded qualitative data into quantitative data. Creswell (2014) explained that the integration of coded qualitative data into quantitative data produces a joint display. The joint display is a visual tool used to represent quantitative and qualitative data analysis or report presentation in a single report. This research utilized Fetters et al.'s (2013) framework by using a two-phase explanatory sequential mixed method and triangulating into a third phase with an expert panel of cybersecurity and IT SMEs to validate quantitative and qualitative data for the universal CCF.

Research Design

The research design is a blueprint that structured the study from the initial stage until the end. Creswell (2014) referred to research design as a proposal to conduct the research, which involves the intersection of the research philosophy, the research strategies, and the specific methods. The philosophical aspect of this research design examined pragmatism by using a quantitative approach to answer the research question but incorporating the qualitative approach to examine the “what” and “how” of the quantitative data. The research strategy employed the explanatory sequential approach, given that this approach is the most appropriate for when the quantitative data collection occurs first. The specific methods are outlined in the research design.

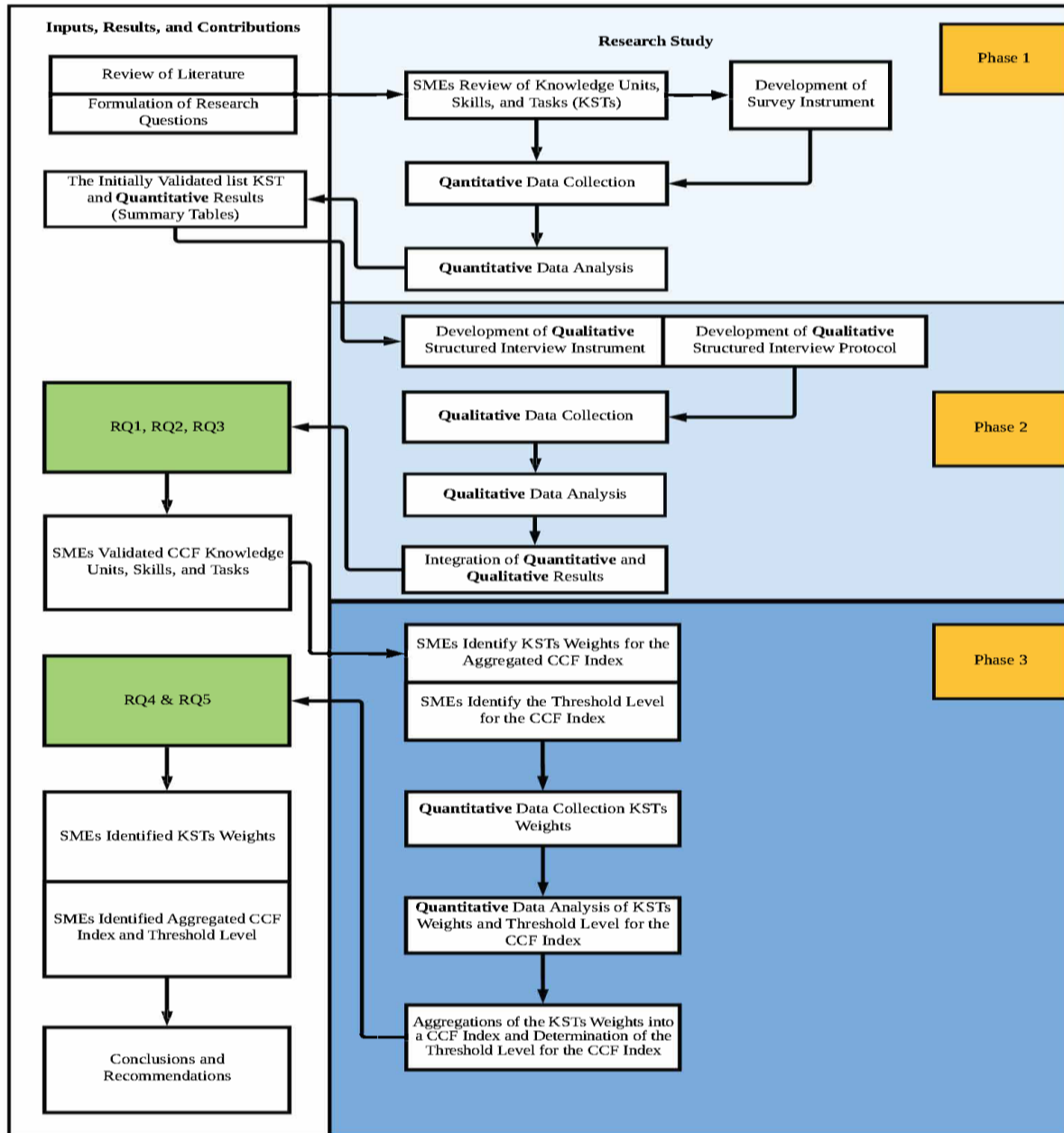
Ivankova et al. (2006) stated that a multistage mixed method research design is difficult to understand without a graphical model. Ivankova et al. (2006) suggested that when quantitative and qualitative data are used in explanatory sequential mixed methods research, the research design should include the use of capitalized and lowercase letters or some other designation to

distinguish the priority of the data. In this research design, the designation for **Quantitative** and **Qualitative** are in bold case. The research design assists the reader to conceptualize the sequence of the data: the connection, the building, the merging, and the embedding (McCrudden & McTigue, 2019). Therefore, the research design for this study provided a series of detailed steps in three phases that must be followed.

The main research question that this research study addressed was: What are the organizational user's KSTs needed for the validated universal CCF? Figure 5 illustrates the research design that this study utilized to address the main research question.

Figure 5

Research Design Process for Development of a Universal CCF



Phase 1 – Survey Instrument and Measures

Survey Instrument Development

Fox et al. (2003) noted that web-based survey instruments were inexpensive when collecting a large amount of data in a short time frame. The survey items for this research study were adapted from the NCWF (NICE, 2017). The NCWF (NICE, 2017) framework contained a large number of KSTs. The instrument development for Phase 1 Survey commenced with the KSTs. A summary with the total NCWF (NICE, 2017) KSTs is listed in Table 11.

Table 11

Summary of the NCWF (NICE, 2017) Spreadsheet with KSTs

NCWF KSTs	Total
Knowledge	594
Skills	368
Tasks	930

Fox et al. (2003) pointed out that a number of practical issues need consideration before the construction of the survey instrument. Included for consideration in this research study prior to the construction of the survey instrument were the selection of the SMEs and the reduction of the KSTs to satisfy the scope of the study.

Selection of the SMEs

Before the main study, SMEs were recruited for a focus group on the survey instrument development. The purpose of the focus group was to evaluate the NCWF (NICE, 2017) KSTs to ascertain the items for the survey instruments. Hasson and Keeney (2011) pointed out that the aggregation of SMEs' opinions was widely used and necessary for research and instrument development. The SMEs were professionals in cybersecurity, information security, and knowledge management. The selected SMEs secured the content validity of the survey items.

Hong et al. (2019) agreed that in a mixed-method study, the purpose of selecting the participants was essential in the content validity.

Reduction of the KSTs

Kost and Correa da Rosa (2018) pointed out the impact of a lengthy survey instrument is likely to compromise the reliability. The SMEs from the focus group examined the list of KSTs to shorten the survey instrument and secure the reliability. Appendix A contains the Proposed Checklist of KSTs. According to Kost and Correa da Rosa (2018), a shorter survey instrument also holds the potential to improve the response rate. Therefore, the shortened survey instrument in this research study likely increased the response rate.

Instrument to Validate KST

Instrument development for the Phase 1 quantitative data survey continued with the accepted KSTs. Based on the SMEs' accepted KSTs, the assessment of the survey instrument utilized a seven-point Likert scale. Joshi et al. (2015) asserted that the Likert scale is widely used in the social science and medical fields for data collection. Additionally, when considering the reliability of the responses, the seven-point Likert scale achieved better than the five-point Likert scale. The seven-point Likert scale reveals more about the descriptions of the design, thus, appeals to the intellect of the SMEs. The seven-point Likert scale ranged as follows: (7) "Extremely important," (6) "Very important," (5) "Moderately important," (4) "Neutral," (3) "Slightly important," (2) "Low importance," and (1) "Not at all important." The competency survey instrument for the KSTs is shown in Appendix B.

Main Data Collection

Quantitative Data

Phase 1 of the research design continued with the quantitative data collection. The collection of knowledge or collective discussion began with the initial quantitative survey to measure the cybersecurity KSTs. Before the issuance of the survey instrument, several revisions and amendments were conducted based on the recommendations from the focus group. In the explanatory sequential mixed method approach, Fetters et al. (2013) emphasized that quantitative data collection occurs before qualitative data collection, thus becoming the main data collection. The survey instrument for the main data collection was designed using the Google Forms® platform. The survey measured the SMEs' responses about the content validity of the cybersecurity NCWF (NICE, 2017) KSTs that formulated the organizational users' universal CCF.

Main Data Analysis

Quantitative Data Analysis

The quantitative data analysis began with the data collected from the survey. Based on the literature and the definition of the explanatory sequential mixed method, the quantitative data occurs first, thus the quantitative data analysis is the core of the research study. The purpose of this analysis is to identify the importance of the KSTs for organizational users given access to the organizational network.

Based on the data collected, a report on the sample size was conducted to determine the number of SMEs participated in the research study (Creswell, 2014). A weekly check on the survey responses eliminated the potential for any response bias. Additionally, early in the data collection process, the SMEs received an email reminding them about the survey response.

Creswell (2014) noted that a nonresponse or a response in the final week of the survey is a potential response bias. To determine the level of importance, the descriptive statistics guided the outcome of the quantitative data. The level of dispersion included the standard deviation and the mean. The findings from the descriptive statistics provided the foundation for the qualitative data. The procedure to analyze quantitative data consisted of SPSS software and Microsoft® Excel. The SMEs' responses stored in Google® Forms were exported into Microsoft® Excel. In Microsoft® Excel, the SMEs' responses to each of the KSTs were coded according to the actual number on the Likert scale. The demographics were coded with "1" for male and "2" for female. Upon completion of the coding, Microsoft® Excel calculated the mean for the KSTs. The acceptance rate for the mean score was 70%. Creswell (2014) noted that a general practice is to retain the factors for at least 70% of the total variability. Okoli and Pawlowski (2004), as well as Walker and Selfe (1996), noted that a 70% acceptance rate was suitable for the points allocation. Upon completion of the collection and analysis of the quantitative data, the results generated the initial validated list of KSTs summarized in tables 16, 17, and 18 in Chapter 4.

Phase 2 – Qualitative Data

Phase 2 of the research design started with the initial validated list of KSTs. The development of the qualitative structured interview instrument began with the summary tables from Phase 1. Ivankova et al. (2006) noted that in the explanatory sequential mixed method, the qualitative data collection and analysis start after the quantitative data analysis. According to Castro et al. (2010), the strength of the qualitative data determines the richness of the descriptive account. In this research study, the SMEs' lived experience with cybersecurity and information security accounted for the richness of the qualitative data.

The development of the qualitative structured survey instrument used the descriptive statistics from the KSTs to formulate the qualitative questions. When formulating the qualitative questions, Castro et al. (2010) posited that obtaining rich qualitative responses requires narrowly framing the questions in the form of a sentence completion. An example of sentence completion is: “Your impression of the KU ranking is ...” In this research study, to obtain the rich qualitative responses necessary for coding, the focus questions were framed as sentence completion items about the quantitative rankings. Appendix C contains the qualitative interview questions. Castro et al. (2010) pointed out that the content analysis of a structured interview is to identify the participants’ knowledge. Castro et al. (2010) also noted that a concentration on the thematic coding of a structured interview secured the content analysis. In this research study, the SMEs' qualitative responses and the thematic coding secured the content analysis. In addition, the survey instrument contained demographic data.

Affixed to the qualitative survey instrument was the qualitative structured interview protocol. Creswell (2014) noted that a qualitative interview could be lengthy, necessitating a structured interview process to effectively capture all the data points. In this research study, the purpose of the structured interview protocol was to provide a logical model for the audio-recorded interview to guide the interviewer and ensure all the participants were asked the same questions. Appendix D contains the structured interview protocol.

Qualitative Data Collection

The structured interview protocol provided the blueprint for the collection of the qualitative data. A recorded 40-minute Zoom meeting and a questionnaire served as the method for the qualitative data collection. Creswell (2014) pointed out that multiple sources of qualitative data collection are necessary to build a coherent justification for the themes. The SMEs received an email invitation to confirm they had completed the quantitative data collection. Appendix E contains the email invitation confirmation. Upon confirmation, they were given an invitation to participate in the qualitative data collection.

Qualitative Data Analysis

According to Chenail (2012), one of the hurdles to overcome in qualitative data analysis is finding the unit of analysis. Sekaran and Bougie (2016) concurred with Chenail (2012), noting that qualitative data analysis is not easy because of the volume of data collected through interviews, open-ended questions, and video recordings. Sekaran and Bougie (2016) also noted that identifying the unit of analysis was essential in the data reduction. When analyzing the qualitative data, three primary steps were significant: data reduction, data display, and drawing and verifying the conclusion (Sekaran & Bougie, 2016).

The qualitative data analysis began with the data reduction through coding and categorizing each question for the KSTs. The interviews were conducted through Zoom utilizing the live transcript feature to store the data. The transcripts of each interview were downloaded in a Microsoft Word document. Chenail (2012), as well as Creswell and Poth (2018), noted the necessity for using digital files to organize and manage the data. Chenail (2012) recommended the Microsoft Word Insert Comment reviewing option as a simple method for an audit trail to create codes for analytical purposes. Sandelowski (2000) noted that a focus must be placed on

summarizing qualitative verbal data to generate the codes, unlike quantitative data with pre-existing codes. Chenail (2012) concurred with Sandelowski (2000) in recommending the technique of highlighting the transcript, whether one word or an entire document, to create codes unit-by-unit, with the codes appearing in the left column. This research study utilized Chenail's (2012) recommendation for generating the codes. The analysis continued with meticulously reading the transcript line-by-line. The generation of the codes occurred by highlighting sections of the transcript and adding the tagged code on the left column. Also, the responses to binary questions were tabulated accordingly. Afterward, all the codes were categorized. The data reduction continued with identifying the units of analysis derived from the categorized codes. Chenail (2012) described a unit of analysis as one undivided entity upon which to focus the qualitative analysis. The unit of analysis for this research study is the SME.

Creswell (2014) noted the significance of displaying the qualitative data after the reduction. Creswell and Poth (2018), as well as Sekaran and Bougie (2016), agreed that displaying the qualitative data in an organized format after the data reduction was necessary. Creswell (2014) noted that a narrative display was ideal to showcase the organized qualitative data. The narrative is vivid with the SMEs' direct responses. Additionally, the narrative was the most appropriate display to assist in formulating the conclusions.

Sekaran and Bougie (2016) postulated that drawing the conclusion was the final process of the qualitative data analysis. Creswell and Poth (2018) concurred with Sekaran and Bougie (2016) that accounting for the findings was essential when displaying and reporting the qualitative data. The conclusion of this qualitative data analysis reported the themes and explanations derived from the SMEs' responses about their impression of the KST rankings,

their agreement or disagreement with the quantitative results, and their reasons for agreeing or disagreeing with the results. Also, the conclusion provided the thematic explanation of the SMEs' overall comments on the KSTs. The qualitative data analysis results are provided in chapter four.

Reliability and Validity of the Qualitative Data Analysis

Creswell and Poth (2018), as well as Sekaran and Bougie (2016), pointed out the importance of verifying the reliability and validity of the qualitative analysis. Sekaran and Bougie (2016) emphasized that triangulation is a technique associated with reliability and validity of qualitative research. Bazeley (2002) asserted that triangulation uses different methods to achieve the same results, with a view of providing corroborating evidence for the conclusions drawn. In this research study, the qualitative data were collected using semi-structured interviews and questionnaires. The data collection through the questionnaire was necessary, given that SMEs were located across different geographical areas and time zones. Additionally, the use of the questionnaire allowed one SME to participate in Phase 1 data collection though he was on active military duty. The questionnaire was administered to the SMEs as they had completed the Phase 1 survey, and their responses were essential for the reliability and validity of the conclusion. Sekaran and Bougie (2016) pointed out that validity in qualitative research has a different meaning than validity in quantitative research. The validity in qualitative research measures accuracy of the results represented in the data collected. In this research study, data from the semi-structured interviews and the questionnaires were assessed for validity. Additionally, the external validity of the qualitative data in a research study is the transferability of the context to another study. Sekaran and Bougie (2016) pointed out that external validity involves the

transferability of the data to future studies. This research study was found to have external validity because the results could be applicable to other studies.

Integration of Quantitative and Qualitative

Creswell et al. (2003) and Ivankova et al. (2006) referred to integration as the level or levels in the research process where the mixing of the quantitative and qualitative methods occur. In this research study, the quantitative and qualitative data were integrated in Phase 2. The statistical results from the KSTs led to formulation of the questions for the structured interview. The findings from the interviews and questionnaires explained the results from the survey data collected in Phase 1. The interpretation of the rankings addressed research goals one to three and RQ1 to RQ3.

Phase 3 – Identification of KST Weights and Threshold Level

KST Weights

Phase 3 of the research design began with the SMEs' validated KSTs to identify the weights for the aggregated universal CCF index. The Google Forms survey contained all the validated KSTs and requiring responses from 20 SMEs, as shown in Appendix F contains the weights and threshold level survey instrument. An email containing the link to the survey was sent to the SMEs. The level of importance (weight) of each competency component was not the same. The SMEs' validated KSTs were used to calculate the weight computation. To determine the weight, each SME was asked to divide 100 points among the KUs, Skills, and Tasks. To compute the weight for the KUs, the total number of SMEs' points was added and then divided by the number of SMEs' responses. To compute the weight for the Skills, the total number of SMEs' points was added and then divided by the number of SMEs' responses. To compute the weight for the

Tasks, the total number of SMEs' points was added and then divided by the number of SMEs' responses. The SMEs' validated weight determined the order of importance for the KSTs. The SMEs' validated weight was utilized as a measure of central tendency to include the mean, and the levels of dispersion included the standard deviation (Hasson & Keeney, 2011; Salkind, 2018).

Threshold Level

The data analysis continued with the SMEs' collected weights to identify the threshold level for the universal CCF. To determine the threshold levels, the SMEs were asked to identify the percentage of points from the maximum composite score that defined the universal CCF competency level. Each SME submitted a percentage of points that they determined was the universal CCF competency threshold. The percentage of points submissions were averaged to identify the threshold level for the universal CCF. Phase 3 data were analyzed using Microsoft Excel.

The aggregation of the KST weights into the CCF index and the determination of the threshold level for the CCF index began with the equation to compute the overall CCF index using the previously determined weights from the SMEs based on their ranking of the Ks, Ss, and Ts:

$$CCF = (K) * \left[W_{KUs} * \left(\sum (KU_x) \right) + W_{Skills} * \left(\sum (SKL_y) \right) + W_{Tasks} * \left(\sum (TSK_i) \right) \right]$$

The variable K was a normalizing coefficient to make the total a minimum of 0 and maximum of 100. The variable W_{KUs} represents SMEs' mean for knowledge units. The variable KU_x , x represents the maximum number of knowledge units in NIST (2017). The variable W_{Skills}

represents SMEs' mean for skills. The variable SKL_y , y represents the maximum number of skills in NIST (2017). The variable W_Tasks represents SMEs' mean for tasks. The variable TSK_i , i represents the maximum number of tasks in NIST (2017).

Upon completion of the aggregation of the KSTs' weights into the CCF index and the determination of the threshold level for the CCF index, the results had addressed research goals four to five and RQ4 to RQ5.

Validity and Reliability

Validity

Sekaran and Bougie (2016) pointed out that the development of the survey instrument must adequately measure the intended concept for validity. The SMEs validated the KSTs during Phase 1 of the research study. Sekaran and Bougie (2016) simplified content validity as a panel of judges attesting that the survey instrument includes sufficient scale items to measure the concept. In this research study, the panel of experts from the cybersecurity and IT professions validated the contents of the KSTs used for the survey instrument in Phase 1. Sekaran and Bougie (2016) noted the achievement of construct validity occurred when the results from the survey instrument fit the intended theories. According to Sekaran and Bougie (2016), one method of assessing construct validity is through convergent validity. The employment of the mixed-method approach accounted for the construct validity. Sekaran and Bougie (2016) explained that criterion-related validity is established by testing the power of the measure to differentiate the individuals who are outliers. The achievement of the criterion validity occurred when the SMEs' acceptance rate for the KSTs was at 70% or greater. Terrell (2015) pointed out the use of the concurrent strategies in the quantitative-qualitative mixed method was acceptable

for attaining concurrent validity. Concurrent validity was accomplished by employing the same SMEs for all phases of the research study.

According to Salkind (2018), as well as Sekaran and Bougie (2016), internal validity is an observable effect caused by a subsequent change in the theorized variable and not by variables unrelated to the research context. Most importantly, Guzys et al. (2015) noted that content analysis assured the internal validity when analyzing the data. Additionally, Guzys et al. (2015) argued that the concept of using a panel of experts is heuristic in nature, which utilizes their opinions, experience, intuition, and tacit knowledge. Tacit knowledge is difficult to codify, which poses a threat to internal validity, given that some essential knowledge might be excluded. To mitigate the potential threat of tacit knowledge, the SMEs were not allowed to modify the KSTs adapted from the NCWF (NICE, 2017).

Sekaran and Bougie (2016) maintained that external validity is the generalization of the results from the initial sample to another sample. A potential threat to the external validity of this research study would have been the absence of generalization across SMEs. To ensure the generalization of the results, the SMEs were solicited from several backgrounds, including IT and cybersecurity, as well as various geographic locations.

Reliability

Salkind (2018) contended that reliability occurred when a test measures the same thing more than once and the results remain consistent. Sekaran and Bougie (2016) maintained that reliability is an indication of stability; the test measurement is bias-free and ensures consistency across the different items in the instrument. The SMEs operated virtually and individually, eliminating any group collaboration and geographical bias. A quality control check on the survey

instrument is necessary to increase the reliability. Salkind (2018) recommended eliminating unclear items because they hold the potential to be unreliable. Hasson et al. (2000) suggested a small panel of five to seven participants to validate an instrument for quality control. In the initial stage, a focus group of five SMEs performed a quality control check on the survey instrument to determine if any of the KSTs were outside the scope of the research study. Hasson and Keeney (2011), as well as Salkind (2018), stated that once the survey instrument has been validated and is ready for the general population, the number of participants should be increased to enhance the reliability, since a larger panel more accurately mirrors the perspective of the population. This research study sought 50 SMEs for Phase 1 to maximize the reliability.

Sample Size

Sampling is a statistical method that is essential when conducting a research study. According to Sekaran and Bougie (2016), sampling involves selecting a group of individuals within a study's population to answer the research questions. The population is the entire group of individuals with knowledge and interest in the research. The selection of the SMEs was essential for reliable results. The SMEs from the targeted population for this research study possessed expert knowledge and skills in cybersecurity and IT. Specifically, they had a lived working experience in the public and private sector, as well as in academia. These cybersecurity and information security experts were the unit of analysis (individuals). The SMEs were recruited from LinkedIn and the Center of Academic Excellence (CAE). Email served as the mode for communicating with the targeted population.

The SMEs for the Phase 1 quantitative survey were randomly sampled from the cybersecurity and IT communities. According to Sekaran and Bougie (2016), random sampling

is the preferred method for quantitative research, as it gives participants an equal opportunity to participate in a research study. Additionally, the results from random sampling allow the study to be more generalizable.

The literature indicated that the sample size for quantitative data collection depends on the research problem. Skulmoski et al. (2007) noted that the sample size for quantitative data ranges from one and beyond, since the research problem varies. Sekaran and Bougie (2016) pointed out the impractical nature of collecting data with a very large sample size. Okoli and Pawlowski (2004) noted that selecting the number of participants for the sample size depends on the group dynamics to attain the threshold level rather than the power of the statistics, and previous studies recommended a panel of 10 to 18 participants. Skulmoski et al. (2007) concurred with this range for the sample size. However, Meadows et al. (2004) suggested 28 participants is more appropriate for a competency-based study. Similarly, Collins et al. (2019) utilized a study population of 28 to develop and validate a competency framework. Therefore, this research solicited a significant number of SMEs from the cybersecurity community and information systems community to establish a population between 28 and 50 SMEs to participate in the research study. The link to the survey instrument was posted in several cybersecurity newsletters and emailed to cybersecurity professionals. The quantitative data were gathered in one shot for three months, thus constituting a cross-sectional study.

The sampling for Phase 2 of this research study commenced with selecting the SMEs for the semi-structured interview. Creswell and Poth (2018), as well as Sekaran and Bougie (2016), noted that in qualitative research, the sampling begins with the identification of the target population. For this research study, the target population was the pool of SMEs who participated

in the Phase 1 quantitative survey. The SMEs who participated in the Phase 1 survey were familiar with the research and experts in cybersecurity. Therefore, purposive sampling was the preferred sampling technique employed for the qualitative data collection. Sandelowski (1995) commented that there were no computations or power analyses to determine the sample size for qualitative research. Sandelowski (1995) continued that the minimum sample size should be enough to manage the research and the maximum sample size should be enough to provide new and richly textured understanding of the research. Furthermore, Fugard and Potts (2015) discussed using the population of interest as a construct to determine whatever sampling approach the research undertakes. Meanwhile, Fusch and Ness (2015) stated that a large or small sample size is not a guarantee for data saturation. For the scope of this research study, there were no selected minimum or maximum sample sizes for Phase 2. The research study reached the sample size when there were no more new data, new themes, and new codes. The population of interest was the SMEs from Phase 1, who received emails to participate in the semi-structured interview. Fugard and Potts (2015), as well as Fusch and Ness (2015), pointed out that when no new or rich themes were found, data saturation started to unfold. In one study, Fugard and Potts (2015) pointed out that data saturation occurred after six interviews. In another study, Francis et al. (2010) pointed out after ten interviews additional interviews developed into new themes. For this research study, data saturation occurred after 12 interviews.

The sampling for Phase 3 of this research study commenced with selecting the SMEs to identify the weights for the CCF index. Similar to Phase 2, the targeted population was SMEs from Phase 1. The sample size for Phase 3 consisted of twenty SMEs. The link to the survey

instrument was emailed to cybersecurity professionals who participated in Phase 1 data collection.

Pre-Analysis Data Screening

Several researchers contended that preemptive measures of data collection were necessary to avoid data collection errors (Burlig, 2018; Coffman & Niederle, 2015; Levy, 2006). Furthermore, Schneider and Deenan (2004) advised that when collecting data, researchers should be well trained in data collection and accuracy, noting that even the best-trained researchers are likely to commit human errors. To avoid any data collection errors, the design of the instrument took into consideration the format and effective use of space. Schneider and Deenan (2004) maintained that if data gathering is from an existing source, the data should be documented in the same order as the sources because shifting data items is likely to cause data collection errors. The data collection for the universal CCF was the data items from the NCWF (NICE, 2017). The KSTs were structured logically, clearly, and concisely using the same identification numbers and descriptions as the NCWF (NICE, 2017). Additionally, Levy (2006) cautioned that validity issues are likely to occur due to missing data. Therefore, to avoid any validity issues, a pre-analysis data screening was conducted to ensure data collection accuracy. The survey instruments were designed so that each data item had a corresponding response as a method of completing the entire survey. If any SME intentionally or unintentionally failed to provide a response, the unanswered data item were highlighted for easy identification. The SMEs had the opportunity to review and provide a response to all missing data items.

The pre-screening for Phase 2 data collection examined the textual responses from the questionnaire. The SMEs who opted to complete the questionnaire were informed to fully

complete the questions and responses of Not Applicable (N/A), No Comments, and blank were not acceptable. SMEs who submitted a questionnaire with a response of Not Applicable (N/A), No Comments, and blank were notified through email to provide an acceptable response. A focus group tested the questionnaire, structured interview protocol, and participant invitation letter to identify any errors.

The pre-screening continued with Phase 3, allocating weights for the CCF index to ensure any data processing errors would not occur. The focus group tested the link to ensure the survey was accessible and the points allocated totaled 100. The SMEs were informed that the total allocation of points must equal 100. Any response with zero points for the total allocation was not considered for the study.

Resources

This research study involved human subjects; thus, Nova Southeastern University (NSU) Internal Review Board (IRB) was contacted before any part of the research study began. Appendix G contains the approval letter. The solicitation of SMEs to participate in the research study was conducted through email invitation. Additionally, Google Forms were employed for Phase 1 and Phase 3 survey instruments; Phase 2 solicitation was via email. The results from the Phase 1 survey instrument were exported into Microsoft® Excel, which was used to analyze the statistical data. The transcripts of the interviews and questionnaire responses from Phase 2 were exported into Microsoft® Word for analysis, coding, categorization, and display of the results. The results from the Phase 3 survey instrument were exported into Microsoft® Excel, which was used to analyze the statistical data.

Summary

This chapter provided an overview of the research methodology. The research study utilized an explanatory sequential mixed-method approach to validate the universal CCF. This research study answered the following research questions:

The main Research Question (RQ) this research study addressed was: What are the organizational user's competency and KSTs needed for the validated universal CCF? Further research questions this research study addressed were as follows:

RQ1: What are the specific NCWF *KUs* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ2: What are the specific NCWF *skills* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ3: What are the specific NCWF *tasks* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ4: What are the SMEs' identified NCWF KSTs weights for the development of an aggregated score for the proposed universal CCF?

RQ5: What are the SMEs identified threshold levels for the aggregated score of the proposed universal CCF?

The RQs were addressed over three phases using a developmental design that included quantitative and qualitative data to construct, as well as validate, the universal CCF. In Phase 1, the research study validated the survey instrument, collected the quantitative data, and analyzed the data. The survey instrument served as the main data collection for the research study. Phase 2 consisted of the qualitative data collection and analysis, as well as integration of the quantitative

and qualitative data. Chapter 3 concluded with a description of Phase 3 data collection and analysis for the KSTs weights and aggregation of the universal threshold score.

Chapter 4

Results

Overview

This chapter contains the results of the data collection and the data analysis performed for this research study. The main goal of this research study was to design, develop, and validate a universal CCF that included a measure to determine the demonstrated cybersecurity knowledge, skills, and tasks of organizational users to identify their competency. Each of the three phases of this research study provided results as follows: In Phase 1, the SMEs identified the KSTs necessary for the survey instrument development. Additionally, Phase 1 detailed the quantitative data collection for the mixed-method approach. In Phase 2, the results from the Phase 1 quantitative survey formulated the semi-structured interview and the questionnaire needed for the qualitative data collection. Phase 2 ended with the integration of the quantitative and qualitative data. Phase 3 began with calculating the weights needed for the aggregated CCF index. Phase 3 continued with the detailed quantitative data collection and analysis of the KST weights assigned by each SME. The analysis identified the threshold level for the universal CCF index. Phase 3 ended with aggregating the KST weights and determining the threshold level for the universal CCF index.

Phase 1 – Instrument Development Findings

In 40-minute Zoom interviews, each member of a focus group of SMEs reviewed the spreadsheet to ascertain the KSTs were within the scope of the research study. Secondly, they categorized the KSTs into technical and non-technical. Culot et al. (2019) referred to technical cybersecurity as a specialized technical field that requires advanced and expert knowledge and

skills. Non-technical KSTs require no specialized advanced or expert knowledge and skills. Sussman (2018) pointed out that in 1968, the U.S. Army utilized non-technical methods in activities such as problem-solving, communications, and collaborations. Meanwhile, Sussman (2018) also considered non-technical KSTs as inter-disciplinary. In subsequent 40-minute Zoom interviews, based on the definition of technical and non-technical, two of the SMEs reviewed and separated the NCWF (NICE, 2017) KSTs into technical and non-technical categories. In separate Zoom interviews, the focus group of five SMEs reviewed this technical and non-technical list to ensure conformity to the definitions. The KSTs that were considered technical were outside the scope of the study and removed. A summary with the total technical NCWF (NICE, 2017) KSTs is listed in Table 12

Table 12

Summary of the Total Technical KSTs

Technical KSTs	Total
Knowledge Units	467
Skills	270
Tasks	761

The SMEs were tasked to review and accept the non-technical KSTs that organizations could utilize when granting end-users network access. A summary with the total non-technical NCWF KSTs is listed in Table 13

Table 13

Summary of the Total Non-Technical Approved KSTs from the SMEs

Non-Technical KSTs	Total
Knowledge Units	127
Skills	98
Tasks	169

The SMEs reduced the number of non-technical KSTs to utilize only those most applicable to the research study. Table 14 contains the final list of KSTs for the Phase 1 data collection.

Table 14

Summary of the Accepted Non-Technical KSTs Adapted from the NCWF (NICE, 2017) for the Survey Instrument

KSTs	Total
Knowledge Units	68
Skills	48
Tasks	33

In Phase 1, the quantitative data collection anticipated 50 SMEs to participate in the research study. Invitations to participate in the data collection were sent via email to 98 SMEs and posted in several cybersecurity newsletters. The Google link to the survey instrument was active for three months. The results from the survey instrument showed 42 SMEs completed the survey. The SMEs were cybersecurity practitioners, including administrative/executives, academics/professors/faculty members, cybersecurity/IT staffers, engineers, managers, professional staffers, and other SMEs. Moreover, the SMEs had experience ranging for one year to over 20 years. Additionally, 45% of the SMEs had between one and four cybersecurity certifications. A summary of the SMEs' demographics is listed in Table 15.

Table 15

Quantitative Demographics of SMEs (N=42)

Survey Question	Frequency	Percentage
Job Function:		
Administrative/executive	4	9.5%
Academics/professor/faculty member	19	45.2%
Cybersecurity/IT staff	10	23.8%

Survey Question	Frequency	Percentage
Engineer	1	2.4%
Manager	6	14.3%
Professional staff	1	2.4%
Other	1	2.4%
<i>Experience in IT/Cybersecurity:</i>		
Under 1 year	0	0%
1 - 5	10	23.8%
6 - 10	10	23.8%
11 - 15	10	23.8%
16 - 20	6	14.3%
Over 20	6	14.3%
<i>Number of cybersecurity certifications:</i>		
None	23	55%
One	12	29%
Two	1	2%
Three	3	7%
Four or more	3	7%

Quantitative Data Analysis

Knowledge Units

Appendix B contains the survey instrument for Phase 1 data collection. As shown in Appendix B, the SMEs were asked to indicate the level of importance for each of the Knowledge Units. The descriptive statistics, including the averages were computed for the KUs. The averages were calculated from the 42 SMEs' ratings of importance of the KUs. Averages above 70% were retained for the research study. The calculation of the averages continued with determining the average threshold of the KUs. The threshold was the average percentage of KUs rated with a score of five and above on the seven-point Likert scale. Table 16 provides the results for descriptive statistics for KUs.

Table 16*Results of the SMEs' Assessments of the Knowledge Units (N=42)*

ID	Description	Average Rating	% Rated ≥ 5
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	85%	71%
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	85%	76%
K0004	Knowledge of cybersecurity and privacy principles.	88%	93%
K0005	Knowledge of cyber threats and vulnerabilities.	85%	86%
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	88%	86%
K0007	Knowledge of authentication, authorization, and access control methods.	81%	83%
K0009	Knowledge of application vulnerabilities.	84%	81%
K0026	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	80%	74%
K0040	Knowledge of Information Technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	84%	74%
K0041	Knowledge of new and emerging Information Technology (IT) and cybersecurity technologies.	84%	71%
K0049	Knowledge of operating systems.	83%	74%
K0059	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, current version (ITIL)).	82%	74%
K0060	Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networking, content management systems, blogs).	84%	71%
K0101	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	85%	79%
K0104	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	84%	83%
K0106	Knowledge of adversarial tactics, techniques, and procedures.	81%	76%
K0107	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	86%	74%
K0110	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory	83%	83%

ID	Description	Average Rating	% Rated ≥ 5
	cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).		
K0113	Knowledge of hacking methodologies.	82%	74%
K0114	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	80%	79%
K0119	Knowledge of enterprise incident response program, roles, and responsibilities.	84%	74%
K0150	Knowledge of cyber defense and information security policies, procedures, and regulations.	82%	81%
K0151	Knowledge of organizational Information Technology (IT) user security policies (e.g., account creation, password rules, access control).	82%	88%
K0157	Knowledge of networking protocols.	84%	83%
K0158	Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	85%	90%
K0177	Knowledge of basic system, network, and OS hardening techniques.	83%	71%
K0205	Knowledge of data backup and restoration concepts.	79%	74%
K0210	Knowledge of organizational training policies.	84%	81%
K0212	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	84%	79%
K0215	Knowledge of applications that can log errors, exceptions, and application faults and logging.	80%	88%
K0229	Knowledge of network architecture concepts including topology, protocols, and components.	80%	76%
K0262	Knowledge of the basic operation of computers.	81%	74%
K0263	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	82%	88%
K0302	Knowledge of auditing and logging procedures (including server-based logging).	85%	90%
K0362	Knowledge of wireless application vulnerabilities.	86%	81%
K0375	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).	82%	83%
K0392	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	81%	88%
K0395	Knowledge of cyber operations terminology/lexicon.	85%	71%

ID	Description	Average Rating	% Rated ≥ 5
K0435	Knowledge of intrusion detection systems and signature development.	81%	79%
K0480	Knowledge of target communication tools and techniques.	83%	93%
K0548	Knowledge of white/black listing.	80%	79%

Skills

Appendix B contains the survey instrument for Phase 1 data collection. As shown in Appendix B, the SMEs were asked to indicate the level of importance for each of the Skills. The descriptive statistics, including the averages were computed for the Skills. The averages were calculated from the 42 SMEs' ratings of importance of the Skills. Averages above 70% were retained for the research study. The calculation of the averages continued with determining the average threshold of the Skills. The threshold was the average percentage of Skills rated with a score of five and above on the seven-point Likert scale. Table 17 provides the results for descriptive statistics for Skills.

Table 17

Results of the SMEs' Assessments of the Skills (N=42)

ID	Description	Average Rating	% Rated ≥ 5
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	81%	76%
S0003	Skill of identifying, capturing, containing, and reporting malware.	86%	86%
S0005	Skill in applying and incorporating information technologies into proposed solutions.	88%	79%
S0006	Skill in applying confidentiality, integrity, and availability principles.	85%	88%

ID	Description	Average Rating	% Rated ≥ 5
S0008	Skill in applying organization-specific systems analysis principles and techniques.	90%	81%
S0011	Skill in conducting information searches.	87%	90%
S0018	Skill in creating policies that reflect system security objectives.	84%	76%
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	88%	79%
S0036	Skill in evaluating the adequacy of security designs.	87%	74%
S0040	Skill in implementing, maintaining, and improving established network security practices.	88%	79%
S0042	Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).	87%	79%
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).	86%	81%
S0054	Skill in using incident handling methodologies.	90%	83%
S0056	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	88%	71%
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	85%	88%
S0063	Skill in collecting data from a variety of cyber defense resources.	86%	71%
S0066	Skill in identifying gaps in technical capabilities.	84%	79%
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	87%	76%
S0077	Skill in securing network communications.	87%	74%
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	86%	74%
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	88%	79%
S0097	Skill in applying security controls.	84%	81%
S0137	Skill in conducting application vulnerability assessments.	86%	71%
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	88%	71%
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	88%	81%
S0206	Skill in determining installed patches on various operating systems and identifying patch signatures.	84%	71%
S0208	Skill in determining the physical location of network devices.	88%	71%

ID	Description	Average Rating	% Rated ≥ 5
S0243	Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).	87%	74%
S0258	Skill in recognizing and interpreting malicious network activity in traffic.	84%	79%
S0259	Skill in recognizing denial and deception techniques of the target.	87%	76%
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	83%	90%
S0358	Skill to remain aware of evolving technical infrastructures.	90%	83%

Tasks

Appendix B contains the survey instrument for Phase 1 data collection. As shown in Appendix B, the SMEs were asked to indicate the level of importance for each of the Tasks. The descriptive statistics, including the averages were computed for the Tasks. The averages were calculated from the 42 SMEs' ratings of importance of the Tasks. Averages above 70% were retained for the research study. The calculation of the averages continued with determining the average threshold of the Tasks. The threshold was the average percentage of Tasks rated with a score of five and above on the seven-point Likert scale. Table 18 provides the results for descriptive statistics for Tasks.

Table 18

Results of the SMEs' Assessments of the Tasks (N=42)

ID	Description	Average Rating	% Rated ≥ 5
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	87%	86%

ID	Description	Average Rating	% Rated ≥ 5
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	90%	90%
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	89%	81%
T0016	Apply security policies to meet security objectives of the system.	89%	83%
T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).	91%	76%
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	90%	71%
T0024	Collect and maintain data needed to meet system cybersecurity reporting.	92%	76%
T0025	Communicate the value of Information Technology (IT) security throughout all levels of the organization stakeholders.	86%	88%
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	90%	79%
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	87%	76%
T0073	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	88%	83%
T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	86%	76%
T0092	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	86%	81%
T0133	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	89%	74%
T0142	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	88%	86%
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	88%	83%
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	87%	88%
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	88%	86%
T0203	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	87%	79%

ID	Description	Average Rating	% Rated ≥ 5
T0233	Track and document cyber defense incidents from initial detection through final resolution.	85%	79%
T0285	Perform virus scanning on digital media.	88%	95%
T0309	Assess the effectiveness of security controls.	90%	83%
T0381	Develop and facilitate data-gathering methods.	84%	74%
T0425	Analyze organizational cyber policy.	86%	81%
T0469	Analyze and report organizational security posture trends.	85%	79%
T0510	Coordinate incident response functions.	85%	79%
T0592	Provide input to the identification of cyber-related success criteria.	86%	83%
T0686	Identify threat vulnerabilities.	88%	90%
T0728	Provide input to or develop courses of action based on threat factors.	92%	83%
T0749	Monitor and report on validated threat activities.	86%	81%
T0845	Identify cyber threat tactics and methodologies.	89%	81%

Phase 2 – Qualitative Data Results

Unlike Phase 1 with an anticipated number of SMEs to participate in the data collection, in Phase 2, the qualitative data collection did not have a specific number of SMEs for the semi-structured interview. A total of 20 SMEs received an email invitation to participate in the semi-structured interview. Fusch and Ness (2015) noted that data saturation is indicative of the qualitative sample size. After 12 interviews, data saturation occurred because the research study did not identify any new themes. Therefore, the sample size was 12 SMEs. The results from the semi-structured interviews and questionnaires showed 12 SMEs participated in the qualitative data collection. The SMEs were cybersecurity practitioners, including administrative/executives, academics/professors/faculty members, cybersecurity/IT staffers, engineers, managers, professional staffers, and other SMEs. Moreover, the SMEs had experience ranging from one year to over 20 years. Additionally, 10 of the SMEs had Ph.D. in cybersecurity or closely related

field with the remaining two have Masters degrees. A summary of the SMEs' demographics is listed in Table 19.

Table 19

Qualitative Demographics of SMEs (N=12)

Survey Question	Frequency	Percentage
<i>Job Function:</i>		
Administrative/executive	1	11.1%
Academics/professor/faculty member	1	11.1%
Cybersecurity/IT staff	1	11.1%
Engineer	1	11.1%
Manager	2	22.2%
Professional staff	0	0%
Other	3	33.4%
<i>Experience in IT/Cybersecurity:</i>		
Under 1 year	0	0%
1 - 5	0	0%
6 - 10	3	33.4%
11 - 15	0	0%
16 - 20	2	22.2%
Over 20	4	44.4%
<i>Level of Education:</i>		
Undergraduate	0	0%
Masters in cybersecurity or relevant field	2	16.7%
Ph.D. in cybersecurity or relevant field	10	83.3%

In the explanatory mixed-method sequential research design, the collection, analysis, and reporting of the quantitative and qualitative data pursue different approaches. Creswell (2014) noted that in the mixed method research, neither the quantitative nor the qualitative findings alone are sufficient to answer the research questions. Traditionally, the quantitative findings are presented in tables, graphs, and figures that summarize the statistical findings. In this research study, the qualitative findings were summarized using succinct sentences that provided sufficient information to show a complete portrait of the quantitative findings. The qualitative statements

served to augment rather than duplicate the quantitative data provided in tables and graphs. Upon approval of the IRB request, the semi-structured interviews were conducted and recorded and the focus group recommendation to include a questionnaire was completed. The interviews and questionnaires provided the multiple sources for qualitative triangulation. The KSTs each had three open-ended questions to allow the SMEs to voice their impressions of the quantitative findings. During the interview, the responses from SMEs to the following questions were recorded: (1a) What is your impression of the KSTs rankings? Do you agree/disagree with the results? Why/why not? (1b) What additional comments do you have about the KSTs in the context of cybersecurity competencies of end-users that organizations grant network access? (1c) What additional overall comments would you like to share about the rankings for the KSTs as part of the cybersecurity competencies for end-users that organizations grant network access? The SMEs' responses were transcribed, categorized, and analyzed manually to identify the theme. Additionally, the SMEs' responses were triangulated with the semi-structured interviews and the questionnaires, thus adding to the validity of the research study.

The findings of the open-ended questions were reported using a narrative discussion. Creswell (2014) pointed out that the most popular approach to display the qualitative analysis is using the narrative discussion. He defined a narrative discussion as using a passage to communicate the findings from the qualitative data analysis. The narrative assists in building the discussion that uncovers the themes or categories developed from the data. When writing the report, Creswell (2014) recommended the following strategies:

1. The report includes narratives that provide support for the themes.
2. The report applies the participant's language to convey their lived experiences.

3. The report displays direct references from interview/questionnaire data.
4. The report identifies multiple perspectives from the participants.
5. The report uses descriptive detail.
6. The report specifies agreements or disagreements in the participants' lived experiences.

The following themes emerged from the SMEs' responses to the three interview questions and two probes:

Theme 1: Positive Impression of Rankings. (Interview question)

Theme 2: The Importance of KUs (Interview question)

Theme 3: SMEs lived experiences. (Interview question)

Knowledge Units

Theme 1: Positive Impression of Rankings. Theme 1 emerged based on the first interview question. The 11 SMEs were highly impressed with the *KU* rankings and used words such as positive, acceptable, and necessary to document their impressions. Given that the first question sets the tone for the interview, the positivity for the *KU* rankings revealed a high agreement, not skewed, and balanced among the SMEs. Further, the SMEs positively agreed that the *KUs* were important and contextually relevant for cybersecurity when granting organization users network access. Additionally, the SMEs stated that organizations should incorporate these *KUs* as part of their cybersecurity posture because they served as core concepts for cybersecurity mitigation. One SME noted that the averages were high and disagreed with the results. The SME's response held the potential to be an outlier.

Theme 2: The Importance of KUs. An important aspect of further understanding the KUs rankings was to solicit additional comments from the SMEs by asking the following interview question:

1b. "What additional comments do you have about the KUs in the context of cybersecurity competencies of end-users that organizations grant network access?" Of the 12 SMEs who provided comments, a majority noted the KUs as important, fundamental, essential, and core competencies in cybersecurity mitigation, holding the potential to reduce cost if effectively applied in organizations. In the context of cybersecurity security, the SMEs pointed out the importance of organizations including these KUs as part of their cybersecurity training and development. One SME noted the importance of the KUs by stating they "can show to the organizations the importance of knowledge in the context of cybersecurity competencies of end-users before they grant network access to those end-users and also to reinforce the cybersecurity education in the organizations."

Historically, organizations consider operational performance as lean and green by reducing production cost and improving quality. Given the cost associated with organizational users' cybersecurity errors, incorporating these KUs into organizations' cybersecurity development is critically important in reducing cost, as noted by several SMEs. Other SMEs suggested that organizations could group the KUs to facilitate their cybersecurity training and development. The grouping of the KUs could provide a more robust cybersecurity training and development that would better accommodate the organizational users.

Skills

Theme 1: Positive Impression Rankings. The qualitative data gathered assisted in understanding the “why” of the *Skills* rankings. The quantitative rankings showed a partial picture of the SMEs’ engagement. Moreover, without the SMEs’ impression of the rankings, the quantitative data held the potential to be superficial. The 11 SMEs were highly impressed with the *Skills* rankings and used words such as realistic, positive, acceptable, and above average to document their impressions. Further, a majority of the SMEs pointed out several of the skills with their high rankings and noted those skills were extremely important to adequately execute cybersecurity functions. The positive impression of the rankings continued with other SMEs acknowledging the Skills as the bedrock for cybersecurity mitigation, given that they are directly from NCWF (NICE, 2017). One SME commented that “skills in social engineering would be extremely helpful for most organizational users.” Organizational users’ limited skill in social engineering is costly for organizations. The FBI (2022) reported that in 2021 BEC was \$43 billion, a 65% increase from 2019 to 2021 (FBI’s Internet Crime Complaint Center (IC3), 2022). The SMEs commented that skills in social engineering would not eliminate BEC, but would be helpful in cybersecurity mitigation, thus reducing the cost associated with data breaches.

The SMEs were asked more probing questions to determine if they agreed/disagreed and why/why not with the Skills rankings. The 11 SMEs noted their high agreement with the rankings with comments such as the following: the skills are needed for risk mitigation, fundamental for organizations’ cybersecurity programs, and essential for well-balanced cybersecurity professionals. One SME disagreed with the averages because the organizational users would require formal training. The SME’s response held the potential to be an outlier

Theme 2: Applicable Skills. An important aspect of further understanding the ranking of the Skills was to solicit additional comments from the SMEs by asking the following interview question:

1b. "What additional comments do you have about the Skills in the context of cybersecurity competencies of end-users that organizations grant network access?" The 12 SMEs made comments such as the following: perfect, applicable, important, and accessible to organizational users in cybersecurity mitigation. The SMEs emphasized that the skills earned the higher values because skill is the application of knowledge, and a good amount of the skills are prevalent in the universal CCF. The comments continued with the SMEs recommending knowledge transfer to hone organizational users' cybersecurity skills for those skills with the lowest averages. One SME noted, "The skill with the lowest scores requires more technical skills, [but it] nonetheless can help with training."

Tasks

Theme 1: Positive Impression of Rankings. The qualitative data gathered assisted in analyzing the *Tasks* rankings. The quantitative rankings showed a partial picture of the SMEs' engagement. Meanwhile, the qualitative data are necessary to fully understand the SMEs' engagement of the Task rankings. To further clarify the Tasks rankings, 11 SMEs were highly impressed with the *Tasks* rankings and used words such as very pleased, acceptable, and necessary to document their impressions. A majority of the SMEs noted that the Tasks percentages scored higher than the KUs and Skills because organizational users need to perform these Tasks more frequently for cybersecurity mitigation. The SMEs continued to note that the Tasks "lined up" with industry standards and were "not surprised" about the higher averages.

The 11 SMEs mostly agreed with the Tasks rankings, mostly agreed the KUs and Skills worked together to assist the organizational users in completing the Tasks, and mostly agreed these Tasks provided organizations strong security strategy and response planning in cybersecurity mitigation. One SME disagreed with the rankings because they felt organizational users would need training to competently complete the Tasks.

Theme 2: Training and Development. An important aspect of further understanding the ranking of the Tasks was to solicit additional comments from the SMEs in the context of cybersecurity competencies of end-users to whom organizations grant net access. The comments centered around the Tasks are helpful for cybersecurity mitigation and training. Even though the Tasks had higher averages, seven of the 12 SMEs noted that organizations would need to provide training and development to organizational users for them to competently complete these cybersecurity Tasks. One SME commented, “Provide additional training on Tasks to be more appropriate for organizational users to improve cybersecurity in the organization.” A further comment pointed out the costs associated with cyber-attacks and noted one way of reducing those costs is to provide training and development to organizational users. “If the professional does not know how to do Tasks, they need to be made aware of the process at the very least to keep rounding out their overall skillset and keep the cost down.” In the context of cybersecurity, organizations must provide the cybersecurity training and development to organizational users to “round out their skillset.”

Theme 3: SMEs' Lived Experiences. An important aspect of gathering rich qualitative data on the KSTs rankings was to seek overall comments from the SMEs. The Lived Experiences of each SME provides an insight into their daily working life with cybersecurity coupled with

subjective and reflective comments open for interpretation. Overall, the SMEs noted that the KSTs were valuable contributions to an organization, complete and comprehensive, as well as valid and inclusive. One SME noted the “Principle of Least Privilege should be considered when granting organizational users network access.” The SME’s comment is subjective and open for interpretation, as five of the 12 SMEs pointed out that organizations should provide cybersecurity training to all organizational users for cybersecurity mitigation.

Integration of Quantitative and Qualitative Data Analysis

Fetters et al. (2013) noted that in mixed-method research the quantitative or the qualitative data cannot stand alone; integration is needed either at the research design level, the methods level, and the reporting level. Additionally, Creswell (2014) and Fetters et al. (2013) noted that integration at the reporting level should be done through a narrative approach by weaving the quantitative and qualitative data together. Creswell (2014) pointed out that the qualitative data should be used to support, expand, or contradict the quantitative findings. In this research study, a narrative approach for integration of the quantitative and qualitative data occurred at the reporting level. The qualitative data were used to support the quantitative findings.

Knowledge Unit

In the quantitative data analysis, the research study retained SMEs' scores averaging 70% and greater. Additionally, the research study retained the SMEs' score on the KUs rated 5 and greater on the Likert scale, which were averaged to determine the percentage rating. The quantitative results needed the qualitative data to support the averages. The 12 SMEs shared their impressions of the KU results; 11 SMEs agreed with the results and provided reasoned arguments to justify the KU percentages, while one SME (SME 9) disagreed with the

percentages and explained that some of the KUs were not known to end-users. SME 9 provided additional comments noting the uncertainty of all the KUs for the end-users. The other 11 SMEs provided additional comments in support of the KUs, noting the KUs are critically important in cybersecurity. Three email reminders were sent to one of the SME to provide additional comments on the KUs, but no response was received. Based on the qualitative data results, 11 SMEs validated the KUs needed for the universal CCF. Given the agreement of 92% of the SMEs on the KUs, research question one and research goal one were answered.

Skills

In the quantitative data analysis, the research study retained SMEs' scores averaging 70% and greater. Additionally, the research study retained the SMEs' score on the KUs rated 5 and greater on the Likert scale, which were averaged to determine the percentage rating. The quantitative results needed the qualitative data to support the averages. The 12 SMEs shared their impressions of the Skills results; 11 SMEs agreed with the results and provided reasoned arguments to justify the Skill percentages, while one SME disagreed with the percentages and explained "not all of the skills were not known to the end-users." One of the SME provided additional comments noting the uncertainty of all the Skills for the end-users. All SMEs provided additional comments in support of the Skills, noting the Skills are important. Based on the qualitative data results, 11 SMEs validated the Skills needed for the universal CCF. Given the SMEs' 92% agreement on the Skills, research question two and research goal two were answered.

Tasks

In the quantitative data analysis, the research study retained SMEs' scores averaging 70% and greater. Additionally, the research study retained the SMEs' score on the KUs rated 5 and greater on the Likert scale, which were averaged to determine the percentage rating. The quantitative results needed the qualitative data to support the averages. The 12 SMEs shared their impressions of the Tasks results; 11 SMEs agreed with the results and provided reasoned arguments to justify the Task percentages, while one of the SME disagreed with the percentages, explaining that "additional training [is] needed to competently complete these Tasks." Additionally, of the 11 SMEs who agreed with the results, six noted that additional training would be needed for organizational users to competently complete the Tasks. Based on the qualitative data results, 92% of the SMEs validated the Tasks for the universal CCF. Given the SMEs agreement on the Tasks, research question three and research goal three were answered.

Phase 3 – Identification of KST Weights and Threshold Level Analysis

In Phase 3, the quantitative data collection anticipated 20 SMEs to participate in the research study. Invitations to participate in the data collection were sent via email to 50 SMEs. The Google link to the survey instrument lasted for four weeks. Responses were received from 17 SMEs, which was 85% of the anticipated sample size.

Data Screening

The data screening did not identify any of the SME responses that needed to be removed. Furthermore, no response sets were identified, and the SMEs did not submit any malicious responses. When developing the survey instrument, all the items were set as "required," thus eliminating any incomplete responses.

KST Weights

The data analysis began with the SMEs' validated KSTs. The weights were not the same for the KUs, Skills, and Tasks. Therefore, the SMEs were asked to divide 100 points among the KUs, Skills, and Tasks, which were averaged and used as the weights to determine the order of importance. The KUs' average represented 37.65% with a standard deviation of 12.39 for the level of importance. The Skills' average represented 36.47% with a standard deviation of 10.42, and Tasks averaged 25.88% with a standard deviation of 8.70. Table 20 contains the summary of the SMEs' scores for the weighted average and the standard deviation.

Table 20

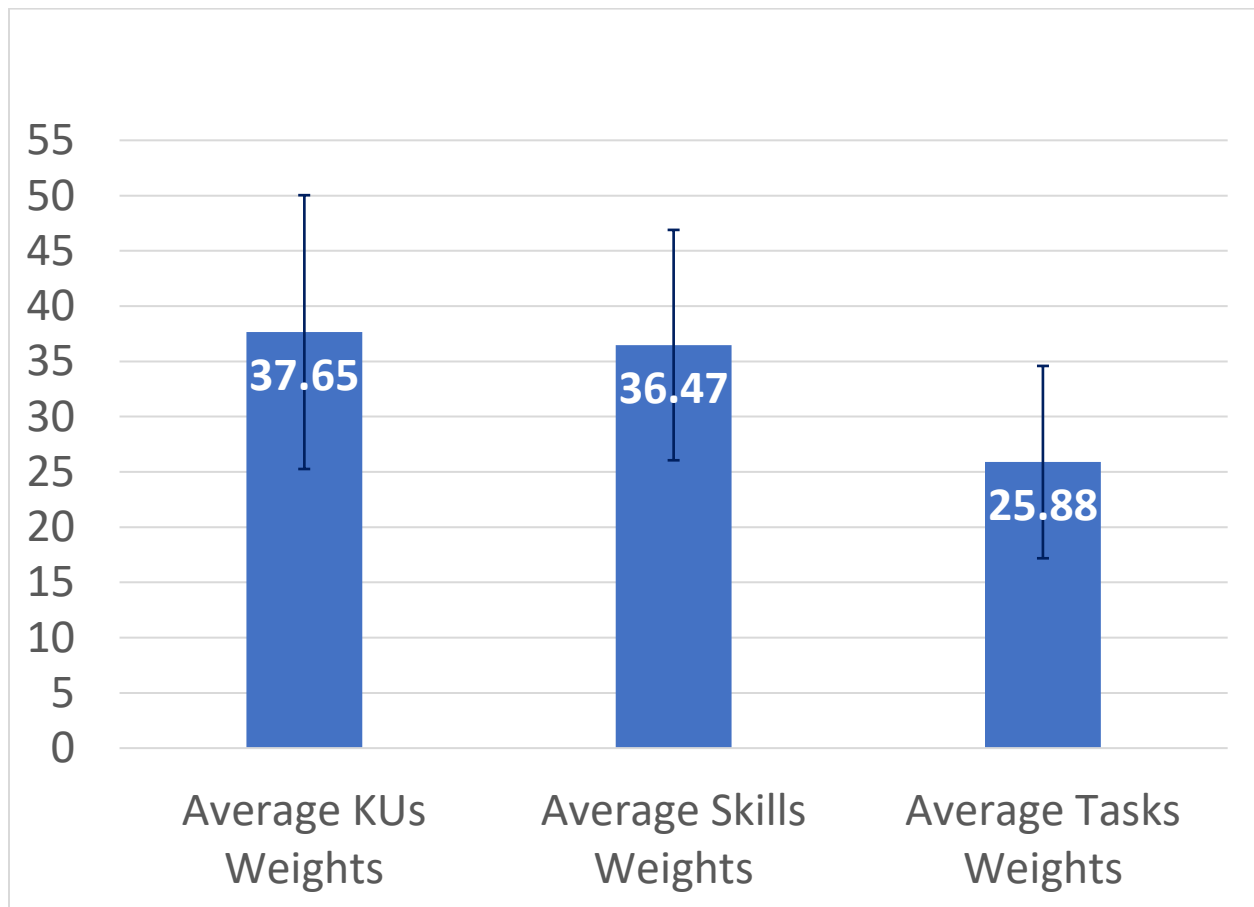
Summary Scores Weighted Average and Standard Deviation (N = 17)

SME	Average KUs Weights	Average Skills Weights	Average Tasks Weights	Total per SME
1	40	30	30	100
2	35	50	15	100
3	10	40	50	100
4	50	25	25	100
5	50	30	20	100
6	50	25	25	100
7	50	25	25	100
8	40	30	30	100
9	50	25	25	100
10	35	40	25	100
11	40	45	15	100
12	40	40	20	100
13	10	60	30	100
14	30	50	20	100
15	30	30	40	100
16	40	40	20	100
17	40	35	25	100
Average	37.65	36.47	25.88	100.00
St. Dev	12.39	10.42	8.70	

Based on the SMEs' scores, KUs had the highest importance, followed by Skills, then Tasks. The mean difference between KUs and Skills was 1.18%. Even though the mean difference was slightly over 1%, the Skills are important for cybersecurity mitigation. The mean difference between Skills and Tasks was 10.59%. Meanwhile, the mean difference between KUs and Tasks was 11.77%. Similarly, Skills were weighted 10.59% more than the Tasks. Figure 6 contains the graphical representation of the SMEs' scores for the weighted averages.

Figure 6

Summary Scores Weighted Average (N = 17)



To gain further information on the weights allocation, the SMEs were asked the following question: "What additional feedback do you have regarding the above weights?" The emerging theme was the value of knowledge.

Theme 1: The Value of Knowledge. To gain further information on the weights allocation, the SMEs were asked to provide additional feedback on this topic. Based on the SMEs' responses, the Value of Knowledge emerged as the theme. Seventeen SMEs responded to the survey and provided feedback, such as the following: knowledge is more important than skills, knowledge is needed to hone skills, and the value of knowledge is extremely important as a competitive advantage. Knowledge is considered valuable because cybersecurity mitigation rests on the organizational users' knowledge. Further, the SMEs commented that cybersecurity knowledge serves as a competitive advantage. Those organizations that invest in their organizational users' cybersecurity knowledge are protecting their business assets and gaining a competitive advantage over other organizations. One SME noted, "The value of knowledge is extremely important when protecting organizational assets."

Of the 17 SMEs, eight noted that knowledge should have the highest order of importance. Meanwhile, two SMEs noted Skills should have the highest order of importance, and two SMEs reported Tasks should have the highest order of importance. One SME noted that training is required for Tasks, and three SMEs did not provide any feedback. Of the 14 SMEs who provided feedback, a majority supported the KUs as the highest order and recommended training to competently complete cybersecurity tasks.

Threshold Level

The data analysis continued with the aggregation of the KST weights into the universal CCF index and the determination of the threshold level. The equation to compute the overall universal CCF index using the previously determined weights from the SMEs based on their ranking of the Ks, Ss, and Ts is as follows:

$$CCF = (K) * [W_{KUs} * (\sum (KU_x)) + W_{Skills} * (\sum (SKL_y)) + W_{Tasks} * (\sum (TSK_i))]$$

The calculation for the CCF = (37.65/100)*(1/(7*41))*Sum(KUs) + 36.47/100*(1/(7*32))*Sum(Ss) + (25.88/100)*(1/(7*31))*Sum(Ts).

The variable K is the normalizing coefficient. The W_{KUs} is the calculated mean (37.65%). The variable W_{KUs} represents the 41 KUs validated by the SMEs. For the sum (KU_x) , the organization will be able to measure each employee on their level of the KUs from 1 to 7 on each of the 41 KUs inputted in the index. The W_{Skills} is the calculated mean (36.47%). The variable W_{Skills} represents the 32 Skills validated by the SMEs. For the sum (SKL_y) , the organization will be able to measure each employee on their level of the Skills from 1 to 7 on each of the 32 Skills and inputted in the index. The W_{Tasks} is the calculated mean (25.88%). The variable W_{Tasks} represents the 31 Tasks validated by the SMEs. For the sum (TSK_i) , the organization will be able to measure each employee on their level of the Tasks from 1 to 7 on each of the 31 Tasks and inputted in the index. Given the index calculation, organizations will be able to determine their employees' competency scores.

Phase 3 data analysis continued with the SMEs' aggregated KSTs to determine the competency threshold level for the universal CCF. The SMEs provided their expert perspectives

on the percentage score necessary to achieved the universal CCF threshold level. The SMEs' percentage scores were averaged to determine the competency threshold level. Based on the computed average, the overall minimum index score for an organizational user to be competent was 72%, with a standard deviation of 12.25. Table 21 contains the summary of the SMEs' scores for the average threshold level.

Table 21

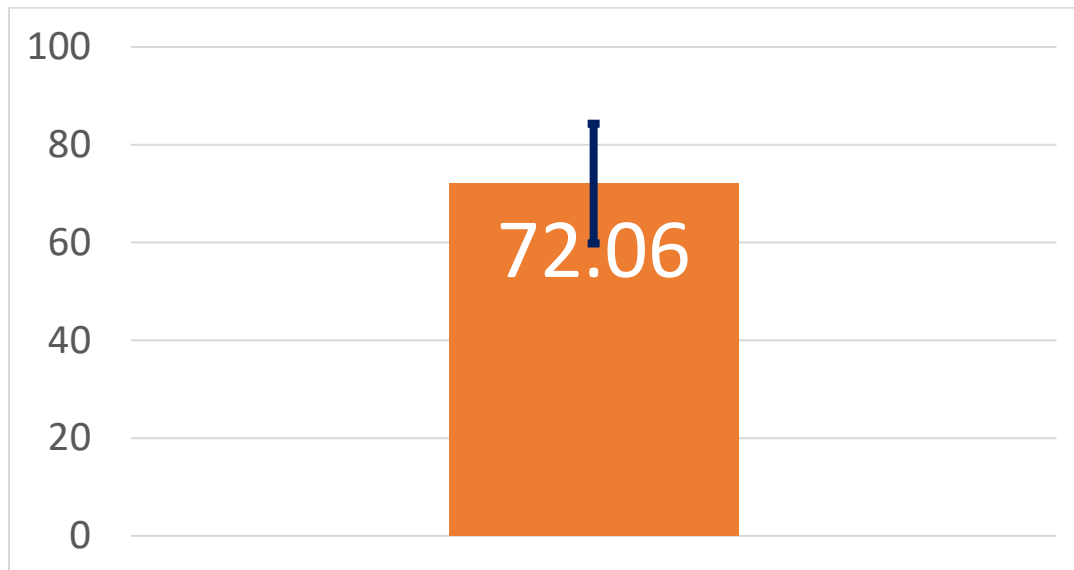
Summary Average Threshold Level

SME	Threshold Level
1	75
2	70
3	70
4	70
5	80
6	70
7	70
8	80
9	85
10	80
11	85
12	80
13	30
14	70
15	70
16	70
17	70
Average	72.06
STDEV	12.25

Figure 7 is a graphical representation illustrating the universal CCF threshold level.

Figure 7

Summary of the Competency Threshold Level (N = 17)



The SMEs' feedback was essential in determining the universal competency threshold level.

Therefore, the SMEs were asked the following question: "What additional feedback do you have regarding the above threshold level?" The emerging theme was competency threshold. Based on the theme, the SMEs' feedback on the competency threshold was as follows:

Theme 1: Acquiring Competency. The SMEs' feedback was essential in determining the universal competency threshold level. Therefore, the SMEs were asked to provide additional feedback regarding the competency threshold level. Based on the SMEs' feedback, Acquiring Competency emerged as the theme. Seventeen SMEs responded to the survey and provided feedback such as the following: acquiring competency is evolving, competency is essential for certification, and awareness and training are instrumental for improvement. Based on the SMEs'

feedback, a competency threshold requires cybersecurity competency-based training depending on established goals of the training, updated cybersecurity documentation, and a review of the organizational users' progress. The SMEs established 70 to 75% as ideal for a competency threshold.

Of the 17 SMEs, seven noted that competency threshold level should be 70%. Meanwhile, six noted that competency is evolving, open for interpretation, resides in knowledge, and requires continued training. Four SMEs did not provide any feedback. Given the SMEs' feedback that certification should be between 70% to 75%, research on four industry entry level cybersecurity certification programs showed the competency threshold level resided between 70% and 83.33%. Table 22 contains a summary of the entry level cybersecurity certification programs and their competency threshold level.

Table 22

Summary of Entry Level Cybersecurity Certification Programs

Entry Level Cybersecurity Certification Programs	Competency Threshold Level Percent
CompTIA Security +	83.33%
Certified Ethical Hacker	70%
CompTIA Cybersecurity Analysis	83.33%
GIAC Security Essentials (GSEC)	73%

Summary

Chapter 4 contains the data analysis and results for this research study. This research study employed a three-phased mixed-method approach, with data collection and analysis in each phase. Each phase of the research study addressed a research question. In Phase 1, quantitative

data results were used to build the survey instrument for Phase 2 qualitative data collection.

Upon completion of Phase 2 data analysis, the research study integrated the Phase 1 and Phase 2 results. The integration of Phase 1 and Phase 2 validated the KSTs needed for the universal CCF and addressed RQ1 to RQ3, as well as research goals one to three.

The weights assigned by the SMEs in Phase 3 showed that they considered knowledge as the most important competency, followed by Skills, then Tasks. The qualitative results revealed that training is needed for cybersecurity tasks. Phase 3 data collection and analysis continued with the aggregation of the validated weights into a single universal CCF index score. The SMEs determined that 72% was the threshold level. For example, SME 1 stated, "Generally, the cutoff for certification is 70 to 75 percent." A review of the industry entry level cybersecurity certification programs revealed the threshold scores were between 70% and 83.33%. The completion of Phase 3 addressed RQ4 and RQ5, as well as research goals four and five.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Cybersecurity has been a major concern for organizations, academic institutions, and public and private sectors. Cyber-attacks have increased exponentially since COVID-19 because of increased reliance on the internet, causing significant financial losses to organizations. These financial losses included hidden costs, such as negative publicity, with the potential to jeopardize an organization's competitive advantage. As a result, organizations can no longer ignore cybersecurity competency.

The main goal of this research study was to design, develop, and validate a universal CCF. This framework included a measure that determined the demonstrated cybersecurity KSTs adapted from the NCWF (NICE, 2017) and identified the cybersecurity competency of organizational users. An expert panel of cybersecurity professionals known as SMEs validated the cybersecurity KSTs necessary for the universal CCF. This research study achieved the main goal as well as five specific related goals with a three-phased research design. The first related goal of this research study identified the *Knowledge Units* (KUs) for the cybersecurity competency of the organizational users. The second related goal identified the *Skills* for the cybersecurity competency of the organizational users. The third related goal identified the *Tasks* applicable to the cybersecurity competency of the organizational users. The fourth related goal identified the weights for the development of an aggregated score for the universal CCF. The final related goal identified the threshold level for the universal CCF.

Discussion

The purpose of this research study was to utilize a unique way to address the exploitation of organizational information security owing to limited cybersecurity competency from organizational users. This research study developed a universal CCF to address the limited cybersecurity competency from organizational users. The results showed the SMEs validated 41 KUs, 32 Skills, and 31 Tasks needed for the universal CCF. The SMEs weighted the order of the competency components as: KUs, Skills, and Tasks. The qualitative results showed that training is needed for Tasks. The mean difference between the KUs and Tasks was 11.77%. Given that knowledge is fundamental in competently completing a task, to improve on knowledge transfer, organizations could employ the four ways of building organizational users' knowledge as proposed by Nonaka (1991) to assist in training. Nonaka (1991) pointed out four basic combinations of knowledge creation existed between tacit and explicit knowledge: socialization, combination, externalization, and internalization.

The mean difference between Skills and Tasks was 10.59%. Newhouse et al. (2017) noted that honed skills are essential in competently completing cybersecurity tasks. Carlton and Levy (2017) developed a scenario-based iPad application to measure non-technical users' cybersecurity skills. Organizations could utilize this iPad application to assist in honing organizational users' cybersecurity skills as part of their training to improve cybersecurity tasks. Cybersecurity is the core of organizational infrastructure that academic institutions, organizations, and public and private sectors can no longer ignore (Solms & Solms, 2018). Cybersecurity incidents to organizations and institutions resulting from data breach involve more than stolen data, financial damage, and regulatory fines (James, 2018). According to James

(2018), the hidden cost, such as negative publicity and loss of intellectual property, creates a competitive disadvantage to the organizations.

Implications for Practice

While most organizations have semi-annual or yearly training for employees to become proficient in their cybersecurity policy, no known organizations assess non-technical organizational users' cybersecurity competency using the NCWF (NICE, 2017). Organizations could implement the use of the universal CCF to assess their employees' cybersecurity competency by determining if they reach the threshold score of 72%. The universal CCF could enhance their existing cybersecurity policy to provide more mitigation against cyber-attacks on their employees. Knowledge and skills are essential components in cybersecurity competency. Furthermore, the results showed that organizations need to provide additional training to add to employees' existing knowledge and honed skills regarding cybersecurity tasks. Organizations could utilize the validated KSTs to be part of their cybersecurity management courses and offer internal training for cybersecurity certification.

Implications for Research

An implication for research signifies that non-technical organizational users require more cybersecurity training to competently complete cybersecurity tasks, thus mitigating cyber-attacks. A threshold level score referencing the NCWF (NICE, 2017) to assess non-technical organizational users had not been researched previously, and the results revealed that training in cybersecurity tasks is worthy of further research. The results also showed a slight difference between KUs and Skills, as well as a significant difference between Skills and Tasks. Similarly, the results indicated a greater difference between KUs and Tasks. A focus on the difference in

cybersecurity knowledge and cybersecurity tasks, as well as the difference between cybersecurity skills and cybersecurity tasks, is worthy of future research.

Limitations

This research study identified several limitations. The number of SMEs willing to participate in the data collection was limited. During Phase 1, the data collection was conducted during the COVID-19 pandemic. It is possible that the pandemic affected the SMEs' participation in the quantitative data collection. The SMEs were not readily accessible, and several reminder emails were sent to them. Another limitation was some of the NCWF (NICE, 2017) KST descriptions were a combination of more than one KU, Skill, and Task.

Recommendations and Future Research

This research study utilized the explanatory sequential mixed-method approach to construct a universal CCF for measuring cybersecurity competency of organizational users. The research study provides opportunities for future research. First, the KSTs derived from the NCWF (NICE, 2017) consisted of 1000 *KUs*, 650 *Skills*, and 270 *Tasks*. A future study would be necessary to identify specific KSTs for a desired job role. Second, a smaller pool of KSTs and a more robust survey instrument could be utilized for the data collection, reducing the data collection time and making participation more attractive to the SMEs. Third, from the results, several KSTs were deleted because they did not meet the minimum threshold. A future study would be helpful to assess those KSTs and identify a framework that would be applicable to certain job roles. Finally, a future study is necessary to revise the descriptions of the KUs, Skills, and Tasks that included two or more items joined by the word "and." For example, K0106 stated: Knowledge of what constitutes a network attack *and* a network attack's relationship to both threats *and*

vulnerabilities. As noted by one SME, an organizational user might be competent in one component of the description but incompetent in other components of the description. a revision of the KSTs in NCWF (NICE, 2017) to reclassify the descriptions into single components is necessary.

Summary

In summary, the universal CCF can assist an organization in measuring their employees' cybersecurity competency. The main research question that this study addressed was: What are the organizational user's competency and KSTs needed for the validated universal CCF? The research questions that this study addressed were as follows:

RQ1: What are the specific NCWF *KUs* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ2: What are the specific NCWF *skills* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ3: What are the specific NCWF *tasks* for the cybersecurity competency of the organizational users that are validated by SMEs?

RQ4: What are the SMEs' identified NCWF KSTs weights for the development of an aggregated score for the proposed universal CCF?

RQ5: What are the SMEs identified threshold levels for the aggregated score of the proposed universal CCF?

In the explanatory sequential mixed-method approach, quantitative or qualitative data results are not independent. Phase 1 provided the quantitative results needed to construct the qualitative semi-structured interview questions for Phase 2. In Phase 2, the qualitative data were gathered

and integrated, answering RQ1, RQ2, and RQ3. The results validated the KUs, Skills, and Tasks needed for the universal CCF.

Phase 3 answered RQ4 and RQ5. For RQ4, the results identified the weights of the KSTs needed for the universal CCF. The KUs were most important, followed by Skills, then Tasks. The aggregation of the universal CCF percentage score will enable organizations to identify the competency of their organizational users before granting network access. For RQ5, the results identified the threshold level for the universal CCF, which was 72%. The universal CCF threshold level reflects those used in industry entry level cybersecurity certification programs, which is between 70% and 83.33%.

Appendix A

Phase 1 Proposed Checklist of KSTs for the CCF

Knowledge Units:

ID	Knowledge Description
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0004	Knowledge of cybersecurity and privacy principles.
K0005	Knowledge of cyber threats and vulnerabilities.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.
K0007	Knowledge of authentication, authorization, and access control methods.
K0009	Knowledge of application vulnerabilities.
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0019	Knowledge of cryptography and cryptographic key management concepts
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.
K0029	Knowledge of organization's Local and Wide Area Network connections.
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
K0041	Knowledge of incident categories, incident responses, and timelines for responses.
K0049	Knowledge of Information Technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0059	Knowledge of new and emerging Information Technology (IT) and cybersecurity technologies.
K0060	Knowledge of operating systems.
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, current version (ITIL)).
K0094	Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networking, content management systems, blogs).
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.

ID	Knowledge Description
K0101	Knowledge of the organization's enterprise Information Technology (IT) goals and objectives.
K0104	Knowledge of Virtual Private Network (VPN) security.
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
K0110	Knowledge of adversarial tactics, techniques, and procedures.
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).
K0119	Knowledge of hacking methodologies.
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.
K0151	Knowledge of current and emerging threats/threat vectors.
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.
K0158	Knowledge of organizational Information Technology (IT) user security policies (e.g., account creation, password rules, access control).
K0174	Knowledge of networking protocols.
K0177	Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0190	Knowledge of encryption methodologies.
K0205	Knowledge of basic system, network, and OS hardening techniques.
K0206	Knowledge of ethical hacking principles and techniques.
K0210	Knowledge of data backup and restoration concepts.
K0212	Knowledge of cybersecurity-enabled software products.
K0215	Knowledge of organizational training policies.
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0229	Knowledge of applications that can log errors, exceptions, and application faults and logging.
K0230	Knowledge of cloud service models and how those models can limit incident response.
K0255	Knowledge of network architecture concepts including topology, protocols, and components.
K0262	Knowledge of Personal Health Information (PHI) data security standards.
K0263	Knowledge of Information Technology (IT) risk management policies, requirements, and procedures.
K0302	Knowledge of the basic operation of computers.

ID	Knowledge Description
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).
K0363	Knowledge of auditing and logging procedures (including server-based logging).
K0375	Knowledge of wireless applications vulnerabilities.
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.
K0415	Knowledge of cyber operations terminology/lexicon.
K0424	Knowledge of denial and deception techniques.
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.
K0449	Knowledge of how to extract, analyze, and use metadata.
K0472	Knowledge of intrusion detection systems and signature development.
K0479	Knowledge of malware analysis and characteristics.
K0480	Knowledge of malware.
K0532	Knowledge of specialized target language (e.g., acronyms, jargon, technical terminology, code words).
K0540	Knowledge of target communication tools and techniques.
K0548	Knowledge of target or threat cyber actors and procedures.
K0555	Knowledge of TCP/IP networking protocols.
K0629	Knowledge of white/black listing.

Skills

ID	Skill Description
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
S0003	Skill of identifying, capturing, containing, and reporting malware.
S0005	Skill in applying and incorporating information technologies into proposed solutions.
S0006	Skill in applying confidentiality, integrity, and availability principles.
S0008	Skill in applying organization-specific systems analysis principles and techniques.
S0011	Skill in conducting information searches.
S0012	Skill in conducting knowledge mapping (e.g., map of knowledge repositories).
S0013	Skill in conducting queries and developing algorithms to analyze data structures.
S0015	Skill in conducting test events.
S0018	Skill in creating policies that reflect system security objectives.
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.
S0021	Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data).

ID	Skill Description
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
S0036	Skill in evaluating the adequacy of security designs.
S0040	Skill in implementing, maintaining, and improving established network security practices.
S0042	Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).
S0044	Skill in mimicking threat behaviors.
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
S0054	Skill in using incident handling methodologies.
S0056	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.
S0063	Skill in collecting data from a variety of cyber defense resources.
S0064	Skill in developing and executing technical training programs and curricula.
S0066	Skill in identifying gaps in technical capabilities.
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).
S0077	Skill in securing network communications.
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.
S0092	Skill in identifying obfuscation techniques.
S0097	Skill in applying security controls.
S0104	Skill in conducting Test Readiness Reviews.
S0107	Skill in designing and documenting overall program Test & Evaluation strategies.
S0112	Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.
S0114	Skill in performing sensitivity analysis.
S0137	Skill in conducting application vulnerability assessments.
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
S0174	Skill in using code analysis tools.
S0206	Skill in determining installed patches on various operating systems and identifying patch signatures.
S0208	Skill in determining the physical location of network devices.
S0243	Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).

ID	Skill Description
S0258	Skill in recognizing and interpreting malicious network activity in traffic.
S0259	Skill in recognizing denial and deception techniques of the target.
S0281	Skill in technical writing.
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
S0358	Skill to remain aware of evolving technical infrastructures.

Tasks:

ID	Task Description
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
T0016	Apply security policies to meet security objectives of the system.
T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.
T0024	Collect and maintain data needed to meet system cybersecurity reporting.
T0025	Communicate the value of Information Technology (IT) security throughout all levels of the organization stakeholders.
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.
T0073	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.
T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.
T0092	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).
T0133	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.
T0142	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.

ID	Tasks
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.
T0203	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.
T0233	Track and document cyber defense incidents from initial detection through final resolution.
T0285	Perform virus scanning on digital media.
T0309	Assess the effectiveness of security controls.
T0361	Develop and facilitate data-gathering methods.
T0381	Present technical information to technical and nontechnical audiences.
T0425	Analyze organizational cyber policy.
T0469	Analyze and report organizational security posture trends.
T0510	Coordinate incident response functions.
T0592	Provide input to the identification of cyber-related success criteria.
T0593	Brief threat and/or target current situations.
T0686	Identify threat vulnerabilities.
T0728	Provide input to or develop courses of action based on threat factors.
T0749	Monitor and report on validated threat activities.
T0845	Identify cyber threat tactics and methodologies.

Appendix B

Phase 1 Proposed CCF – Competency Instrument

A. Demographics

A1. What is your age range?

- 18-19
- 20-29
- 30-39
- 40-49
- 50-59
- Over 60

A2. What is your gender?

- Female
- Male
- Other

A3. What is your job function?

- Administrative/executive
- Cybersecurity/IT staff
- Engineer
- Manager
- Professional staff
- Academics/professor/faculty member
- Other

A4. How long have you been working in the field of IT/Cybersecurity?

- Under 1 year
- 1 – 5 years
- 6 – 10 years
- 11 – 15 years
- 16 – 20 years
- Over 20 years

A5. What is your highest level of education?

- High school diploma
- 2-year college (Associates degree)
- 4-year college (Bachelor degree)
- Master degree
- Doctorate (JD, Ph.D., MD, DO, etc.)

ID	Knowledge Description	←							→							
		Not Important							Extremely important							
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0049	Knowledge of Information Technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0059	Knowledge of new and emerging Information Technology (IT) and cybersecurity technologies.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0060	Knowledge of operating systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, current version (ITIL)).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0094	Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networking, content management systems, blogs).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0101	Knowledge of the organization's enterprise Information Technology (IT) goals and objectives.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0104	Knowledge of Virtual Private Network (VPN) security.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0110	Knowledge of adversarial tactics, techniques, and procedures.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0119	Knowledge of hacking methodologies.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0151	Knowledge of current and emerging threats/threat vectors.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0158	Knowledge of organizational Information Technology (IT) user security policies (e.g., account creation, password rules, access control).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0174	Knowledge of networking protocols.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ID	Knowledge Description	←							→								
		Not Important							Extremely important								
K0177	Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0190	Knowledge of encryption methodologies.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0205	Knowledge of basic system, network, and OS hardening techniques.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0206	Knowledge of ethical hacking principles and techniques.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0210	Knowledge of data backup and restoration concepts.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0212	Knowledge of cybersecurity-enabled software products.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0215	Knowledge of organizational training policies.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0229	Knowledge of applications that can log errors, exceptions, and application faults and logging.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0230	Knowledge of cloud service models and how those models can limit incident response.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0255	Knowledge of network architecture concepts including topology, protocols, and components.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0262	Knowledge of Personal Health Information (PHI) data security standards.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0263	Knowledge of Information Technology (IT) risk management policies, requirements, and procedures.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0302	Knowledge of the basic operation of computers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0363	Knowledge of auditing and logging procedures (including server-based logging).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0375	Knowledge of wireless applications vulnerabilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0415	Knowledge of cyber operations terminology/lexicon.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0424	Knowledge of denial and deception techniques.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0449	Knowledge of how to extract, analyze, and use metadata.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0472	Knowledge of intrusion detection systems and signature development.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0479	Knowledge of malware analysis and characteristics.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0480	Knowledge of malware.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0532	Knowledge of specialized target language (e.g., acronyms, jargon, technical terminology, code words).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0540	Knowledge of target communication tools and techniques.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0548	Knowledge of target or threat cyber actors and procedures.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0555	Knowledge of TCP/IP networking protocols.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K0629	Knowledge of white/black listing.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

C. Cybersecurity Skills Evaluation

Please evaluate the following cybersecurity *skills* for organizational users. Select from 1 “Not at all important” to 7 “Extremely important” to provide your feedback on the level of importance of each cybersecurity *skill* to the overall cybersecurity *skills* that all users must have when granted access to organizational systems.

Scale:

- 1 = Not at all important
- 2 = Low importance
- 3 = Slightly important
- 4 = Neutral
- 5 = Moderately important
- 6 = Very important
- 7 = Extremely important

C1. Skills

ID	Skill Description	←	→
		Not Important	Extremely important
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0003	Skill of identifying, capturing, containing, and reporting malware.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0005	Skill in applying and incorporating information technologies into proposed solutions.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0006	Skill in applying confidentiality, integrity, and availability principles.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0008	Skill in applying organization-specific systems analysis principles and techniques.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0011	Skill in conducting information searches.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0012	Skill in conducting knowledge mapping (e.g., map of knowledge repositories).	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0013	Skill in conducting queries and developing algorithms to analyze data structures.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0015	Skill in conducting test events.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0018	Skill in creating policies that reflect system security objectives.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0021	Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data).	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0036	Skill in evaluating the adequacy of security designs.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0040	Skill in implementing, maintaining, and improving established network security practices.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7

ID	Skill Description		
		← Not Important	→ Extremely important
S0042	Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0044	Skill in mimicking threat behaviors.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0054	Skill in using incident handling methodologies.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0056	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0063	Skill in collecting data from a variety of cyber defense resources.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0064	Skill in developing and executing technical training programs and curricula.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0066	Skill in identifying gaps in technical capabilities.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0077	Skill in securing network communications.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0092	Skill in identifying obfuscation techniques.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0097	Skill in applying security controls.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0104	Skill in conducting Test Readiness Reviews.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0107	Skill in designing and documenting overall program Test & Evaluation strategies.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0112	Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0114	Skill in performing sensitivity analysis.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0137	Skill in conducting application vulnerability assessments.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0174	Skill in using code analysis tools.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0206	Skill in determining installed patches on various operating systems and identifying patch signatures.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0208	Skill in determining the physical location of network devices.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0243	Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0258	Skill in recognizing and interpreting malicious network activity in traffic.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0259	Skill in recognizing denial and deception techniques of the target.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0281	Skill in technical writing.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7

ID	Skill Description	←	→
		Not Important	Extremely important
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
S0358	Skill to remain aware of evolving technical infrastructures.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7

D. Cybersecurity Task Evaluation

Please evaluate the following cybersecurity *tasks* for organizational users. Select from 1 “Not at all important” to 7 “Extremely important” to provide your feedback on the level of importance each cybersecurity *task* to the overall cybersecurity *tasks* that all users must be able to successfully complete before granted access to organizational systems.

Scale:

- 1 = Not at all important
- 2 = Low importance
- 3 = Slightly important
- 4 = Neutral
- 5 = Moderately important
- 6 = Very important
- 7 = Extremely important

D1. Tasks:

ID	Task Description	←	→
		Not Important	Extremely important
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0016	Apply security policies to meet security objectives of the system.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0024	Collect and maintain data needed to meet system cybersecurity reporting.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0025	Communicate the value of Information Technology (IT) security throughout all levels of the organization stakeholders.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0073	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	<input type="checkbox"/> 1	<input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7

T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0092	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0133	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0142	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0203	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0233	Track and document cyber defense incidents from initial detection through final resolution.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0285	Perform virus scanning on digital media.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0309	Assess the effectiveness of security controls.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0361	Develop and facilitate data-gathering methods.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0381	Present technical information to technical and nontechnical audiences.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0425	Analyze organizational cyber policy.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0469	Analyze and report organizational security posture trends.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0510	Coordinate incident response functions.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0592	Provide input to the identification of cyber-related success criteria.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0593	Brief threat and/or target current situations.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0686	Identify threat vulnerabilities.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0728	Provide input to or develop courses of action based on threat factors.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0749	Monitor and report on validated threat activities.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
T0845	Identify cyber threat tactics and methodologies.	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7

Appendix C

Phase 2 – Qualitative Data Collection Participant Letter

Dear Cybersecurity and Information Systems Expert,

Thank you for participating in Phase 1 of this research study. After collecting the input from all 42 Subject Matter Experts (SMEs), the quantitative data were analyzed for consensus. Thus, to identify the Knowledge Units (KUs), Skills, and Tasks (KSTs) that are most agreed upon in the context of cybersecurity competencies of end-users that organizations grant network access. The data analysis results indicated a total of 41 KUs, 32 Skills, and 31 Tasks, as indicated in the tables below, where the average rating and the percentage rating above 70% were retained, indicating the expert panel agreements.

In this round, you are receiving this Structured Interview Questionnaire because you participated in Phase 1, and I hope to get your honest feedback about the quantitative rankings. The goal of this round is to collect **your qualitative feedback** to understand the quantitative results to formulate the universal KSTs of the end-users.

Please provide your comments on the following questions on the KUs, Skills, and Tasks. The interview will take approximately 5-10 minutes to complete. Your participation will contribute to the current literature on Cybersecurity Competency and is significant in assisting organizations to have the minimum threshold for end-users when granted access to organizational Information Systems.

Section 1: Universal End-User Knowledge Units (KUs) Feedback

ID	Description	Average Rating	% Rated ≥ 5
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	85%	71%
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	85%	76%
K0004	Knowledge of cybersecurity and privacy principles.	88%	93%
K0005	Knowledge of cyber threats and vulnerabilities.	85%	86%
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	88%	86%
K0007	Knowledge of authentication, authorization, and access control methods.	81%	83%
K0009	Knowledge of application vulnerabilities.	84%	81%
K0026	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	80%	74%
K0040	Knowledge of Information Technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	84%	74%

ID	Description	Average Rating	% Rated ≥ 5
K0041	Knowledge of new and emerging Information Technology (IT) and cybersecurity technologies.	84%	71%
K0049	Knowledge of operating systems.	83%	74%
K0059	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP) and Internet Protocol (IP), Open System Interconnection Model (OSI), Information Technology Infrastructure Library, current version (ITIL)).	82%	74%
K0060	Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networking, content management systems, blogs).	84%	71%
K0101	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	85%	79%
K0104	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	84%	83%
K0106	Knowledge of adversarial tactics, techniques, and procedures.	81%	76%
K0107	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	86%	74%
K0110	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	83%	83%
K0113	Knowledge of hacking methodologies.	82%	74%
K0114	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	80%	79%
K0119	Knowledge of enterprise incident response program, roles, and responsibilities.	84%	74%
K0150	Knowledge of cyber defense and information security policies, procedures, and regulations.	82%	81%
K0151	Knowledge of organizational Information Technology (IT) user security policies (e.g., account creation, password rules, access control).	82%	88%
K0157	Knowledge of networking protocols.	84%	83%
K0158	Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	85%	90%
K0177	Knowledge of basic system, network, and OS hardening techniques.	83%	71%
K0205	Knowledge of data backup and restoration concepts.	79%	74%
K0210	Knowledge of organizational training policies.	84%	81%
K0212	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	84%	79%
K0215	Knowledge of applications that can log errors, exceptions, and application faults and logging.	80%	88%

ID	Description	Average Rating	% Rated ≥ 5
K0229	Knowledge of network architecture concepts including topology, protocols, and components.	80%	76%
K0262	Knowledge of the basic operation of computers.	81%	74%
K0263	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	82%	88%
K0302	Knowledge of auditing and logging procedures (including server-based logging).	85%	90%
K0362	Knowledge of wireless application vulnerabilities.	86%	81%
K0375	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).	82%	83%
K0392	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	81%	88%
K0395	Knowledge of cyber operations terminology/lexicon.	85%	71%
K0435	Knowledge of intrusion detection systems and signature development.	81%	79%
K0480	Knowledge of target communication tools and techniques.	83%	93%
K0548	Knowledge of white/black listing.	80%	79%

1a. After reviewing the above KUs results from the quantitative phase of this research study, what is your impression of the rankings? Do you agree/disagree with the results? Why/why not?

1b. What additional comments do you have about the KUs above in the context of cybersecurity competencies of end-users that organizations grant network access?

Section 2: Universal End-User Skills Feedback

ID	Description	Average Rating	% Rated ≥ 5
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	81%	76%
S0003	Skill of identifying, capturing, containing, and reporting malware.	86%	86%
S0005	Skill in applying and incorporating information technologies into proposed solutions.	88%	79%
S0006	Skill in applying confidentiality, integrity, and availability principles.	85%	88%
S0008	Skill in applying organization-specific systems analysis principles and techniques.	90%	81%
S0011	Skill in conducting information searches.	87%	90%
S0018	Skill in creating policies that reflect system security objectives.	84%	76%
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	88%	79%
S0036	Skill in evaluating the adequacy of security designs.	87%	74%
S0040	Skill in implementing, maintaining, and improving established network security practices.	88%	79%
S0042	Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).	87%	79%

ID	Description	Average Rating	% Rated ≥ 5
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).	86%	81%
S0054	Skill in using incident handling methodologies.	90%	83%
S0056	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	88%	71%
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	85%	88%
S0063	Skill in collecting data from a variety of cyber defense resources.	86%	71%
S0066	Skill in identifying gaps in technical capabilities.	84%	79%
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	87%	76%
S0077	Skill in securing network communications.	87%	74%
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	86%	74%
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	88%	79%
S0097	Skill in applying security controls.	84%	81%
S0137	Skill in conducting application vulnerability assessments.	86%	71%
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	88%	71%
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	88%	81%
S0206	Skill in determining installed patches on various operating systems and identifying patch signatures.	84%	71%
S0208	Skill in determining the physical location of network devices.	88%	71%
S0243	Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).	87%	74%
S0258	Skill in recognizing and interpreting malicious network activity in traffic.	84%	79%
S0259	Skill in recognizing denial and deception techniques of the target.	87%	76%
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	83%	90%
S0358	Skill to remain aware of evolving technical infrastructures.	90%	83%

2a. After reviewing the above Skills results from the quantitative phase of this research study, what is your impression of the rankings? Do you agree/disagree with the results? Why/why not?

2b. What additional comments do you have about the Skills above in the context of cybersecurity competencies of end-users that organizations grant network access?

Section 3: Universal End-User Tasks Feedback

ID	Description	Average Rating	% Rated ≥ 5
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	87%	86%
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	90%	90%
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	89%	81%
T0016	Apply security policies to meet security objectives of the system.	89%	83%
T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).	91%	76%
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	90%	71%
T0024	Collect and maintain data needed to meet system cybersecurity reporting.	92%	76%
T0025	Communicate the value of Information Technology (IT) security throughout all levels of the organization stakeholders.	86%	88%
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	90%	79%
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	87%	76%
T0073	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	88%	83%
T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	86%	76%
T0092	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	86%	81%
T0133	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	89%	74%
T0142	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	88%	86%
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	88%	83%
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	87%	88%
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	88%	86%
T0203	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	87%	79%
T0233	Track and document cyber defense incidents from initial detection through final resolution.	85%	79%

ID	Description	Average Rating	% Rated ≥ 5
T0285	Perform virus scanning on digital media.	88%	95%
T0309	Assess the effectiveness of security controls.	90%	83%
T0381	Develop and facilitate data-gathering methods.	84%	74%
T0425	Analyze organizational cyber policy.	86%	81%
T0469	Analyze and report organizational security posture trends.	85%	79%
T0510	Coordinate incident response functions.	85%	79%
T0592	Provide input to the identification of cyber-related success criteria.	86%	83%
T0686	Identify threat vulnerabilities.	88%	90%
T0728	Provide input to or develop courses of action based on threat factors.	92%	83%
T0749	Monitor and report on validated threat activities.	86%	81%
T0845	Identify cyber threat tactics and methodologies.	89%	81%

3a. After reviewing the above Tasks results from the quantitative phase of this research study, what is your impression of the rankings? Do you agree/disagree with the results? Why/why not?

3b. What additional comments do you have about the Tasks above in the context of cybersecurity competencies of end-users that organizations grant network access?

Section 4: Overall Feedback and Demographics

4a. What additional overall comments you would like to share about the rankings for the KUs, Skills, and Tasks (KSTs) as part of the cybersecurity competencies for end-users that organizations grant network access?

4b. What is your age range?

- 18-19
- 20-29
- 30-39
- 40-49
- 50-59
- Over 60

4c. What is your gender?

- Female
- Male
- Other

4d. What is your job function?

- Administrative/executive
- Cybersecurity/IT staff
- Engineer

- Manager
- Professional staff
- Academics/professor/faculty member
- Other

4e. How long have you been working in the field of IT/Cybersecurity?

- Under 1 year
- 1 – 5 years
- 6 – 10 years
- 11 – 15 years
- 16 – 20 years
- Over 20 years

4f. What is your highest level of education?

- High school diploma
- 2-year college (Associates degree)
- 4-year college (Bachelor's degree)
- Master degree
- Doctorate (JD, Ph.D., MD, DO, etc.)
- Other

4g. Which cybersecurity certifications do you possess?

Appendix D

Phase 2 – Structured Interview Protocol

Step 1

Noting the date.

Step 2

Noting the participant ID.

Step 3

Introduce myself to establish a rapport and honest comments.

Step 4

Welcome the participant to feel comfortable and get the participant to share their cybersecurity experiences.

Step 5

Read a brief overview of the interview and its purpose.

Step 6

Read the verbal consent before the start of the interview.

Step 7

Seek permission to move forward with the interview after reading the verbal consent.

Step 8

Start recording the interview.

Step 9

Start showing the Knowledge Units table via Zoom.

1. Start asking Questions 1a and 1b.
2. Document the answers in a Word file.

Step 10

Start showing the Skills table via Zoom.

1. Start asking Questions 2a and 2b.
2. Document the answers in a Word file.

Step 11

Start showing the Tasks table via Zoom.

1. Start asking Questions 3a and 3b.
2. Document the answers in a Word file.

Step 12

Start asking question 4a about the overall comments on the rankings for the KSTs.

Document the answers in a Word file.

Step 13

Start asking the demographic questions 4b through 4f.

Document the answers in a Word file.

Step 14

Conclusion of the interview and thank the participant for their time.

Step 15

End the recording.

Appendix E

Phase 2 – Invitation Letter to Participate in Semi-Structured Interview

Dear Cybersecurity Expert,

Last Fall 2021, you completed the survey for Phase 1 data collection for my research study. Thank you.

I am inviting you to complete a questionnaire. The goal of this questionnaire is to collect qualitative data to understand the ranking of the quantitative results and solicit your feedback. Would you mind answering the following questions to ascertain your eligibility to complete the questionnaire?

1. Did you complete the Phase 1 survey in Summer/Fall 2021? [Circle yes/no]
2. Are you comfortable communicating and being recorded through Zoom? [Circle yes/no]
3. The recording is optional. You can email the completed questionnaire if you are not comfortable with the Zoom recording.

Based on your response [YES] to both questions, I will email you a Portable Document Format(pdf) copy of the questionnaire to complete.

Sincerely,

Patricia Baker, Ph.D. Candidate
Nova Southeastern University
3301 College Ave
Davie, FL, 33301

Appendix F

Phase 3 Proposed CCF – Aggregated Score Development Instrument

Dear Cybersecurity Expert,

Below please find the survey instrument to determine the aggregated score for the CCF. You are asked to help us by allocating between 0 to 100% for the knowledge units, skills, and tasks.

Also, to identify the threshold level to distinguish between competency and incompetency.

Weights Allocation

In order to develop an aggregated score of the universal Cybersecurity Competency Framework (CCF), this research study will integrate all three competency components of the score: Knowledge Units (KUs), Skills, and Tasks (KSTs). However, the level of importance (weight) of each competency component may not be the same. As such, please think about the overall score of an aggregated CCF for organizational users and think about the percentage (out of 100%) that you find appropriate for each set of the three competency components (i.e., KUs, Skills, & Tasks).

Kindly provide your designated percentage to each of the three competency components and ensure that the total of all three adds up to 100%:

1. The allocated weight (importance) for Knowledge Units: _____ %
2. The allocated weight (importance) for Skills: _____ %
3. The allocated weight (importance) for Tasks: _____ %

Please calculate the total and ensure it adds up to 100% for all three competency components above.

4. Is there any other feedback you would like to submit regarding the above weights?

Threshold Level for the CCF

With the integration of the weights provided above and the making of the aggregated score of the universal Cybersecurity Competency Framework (CCF), please provide the minimum level (threshold) of the overall score that will distinguish between competency and incompetency of organizational users' cybersecurity out of 100%:

1. What is the threshold to distinguish between competency and incompetency? _____%
2. Is there any other feedback you would like to submit regarding the threshold level?

Appendix G

Institutional Review Board Approval Letter



MEMORANDUM

To: Patricia Baker
College of Engineering and Computing

From: Ling Wang, Ph.D.
College Representative, College of Engineering and Computing

Date: April 30, 2021

Subject: IRB Exempt Initial Approval Memo

TITLE: A Universal Cybersecurity Competency Framework for Organizational Users– NSU
IRB Protocol Number 2021-165

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **April 30, 2021**. You may proceed with your study.

Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Annual Status of Research Update: You are required to notify the IRB Office annually if your

Page 1 of 2

research study is still ongoing via the *Exempt Research Status Update xForm*.

Final Report: You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm*.

Translated Documents: No

Please retain this document in your IRB correspondence file.

CC: Ling Wang, Ph.D.

Yair Levy, Ph.D

References

- Ab Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45-69. <https://doi.org/10.1016/j.cose.2014.11.006>
- Abuadbbba, A., & Khalil, I. (2017). Walsh-Hadamard-based 3-D steganography for protecting sensitive information in point-of-care. *IEEE Transactions on Biomedical Engineering*, *64*(9), 2186-2195. <https://doi.org/10.1109/TBME.2016.2631885>
- Abualoush, S. H., Obeidat, A. M., Tarhini, A., Masa'deh, R. E., & Al-Badi, A. (2018). The role of employees' empowerment as an intermediary variable between knowledge management and information systems on employees' performance. *VINE Journal of Information and Knowledge Management Systems*, *48*(2), 217-237. <https://doi.org/10.1108/vjikms-08-2017-0050>
- Aihie, V. U., & Ikuabe, M. (2018). Evaluation of cost estimation techniques in DRC valuation: A comparative assessment of valuers and quantity surveyors in Lagos State. *Baltic Journal of Real Estate Economics and Construction Management*, *6*(1), 175-192. <https://doi.org/10.2478/bjreecm-2018-0014>
- Akram, J., & Ping, L. (2020). How to build a vulnerability benchmark to overcome cyber security attacks. *IET Information Security*, *14*(1), 60-71. <https://doi.org/10.1049/iet-ifs.2018.5647>
- Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, *25*(1), 107-136. <https://doi.org/10.2307/3250961>
- Aldawood, H., & Skinner, G. (2020). Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions. *IEEE Access*, *8*, 67321-67329. <https://doi.org/10.1109/access.2020.2983280>
- Alhogail, A. (2020). Enhancing information security best practices sharing in virtual knowledge communities. *VINE Journal of Information and Knowledge Management Systems*, (ahead-of-print). <https://doi.org/10.1108/vjikms-01-2020-0009>
- Al-Matari, O. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2018, October 1-2). *Cybersecurity tools for IS auditing* [Paper presentation]. Sixth International Conference on Enterprise Systems, Limassol, Cyprus. <https://doi:10.1109/ES.2018.00040>
- Alonge, O., Rao, A., Kalbarczyk, A., Maher, D., Gonzalez Marulanda, E. R., Sarker, M., Ibisomi, L., Dako-Gyeke, P., Mahendradhata, Y., Launois, P., & Vahedi, M. (2019). Developing a framework of core competencies in implementation research for low/middle-

- income countries. *BMJ Global Health*, 4(5), e001747. <https://doi.org/10.1136/bmjgh-2019-001747>
- Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. *Computers & Security*, 77, 565-577. <https://doi.org/10.1016/j.cose.2018.05.009>
- Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information and Computer Security*, 26(1), 91-108. <https://doi.org/10.1108/ics-09-2016-0073>
- Alstete, J. W., & Meyer, J. P. (2020). Intelligent agent-assisted organizational memory in knowledge management systems. *VINE Journal of Information and Knowledge Management Systems*, (ahead-of-print). <https://doi.org/10.1108/vjikms-05-2019-0063>
- Amagoh, F. (2009). Leadership development and leadership effectiveness. *Management Decision*, 47(6), 989-999. <https://doi.org/10.1108/00251740910966695>
- Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, 21(1), 2-35. <https://doi.org/10.1108/JSIT-02-2018-0028>
- Archer, D., & Cameron, A. (2009). Tough times call for collaborative leaders. *Industrial and Commercial Training*, 41(5), 232-237. <https://doi.org/10.1108/00197850910974776>
- Arling, P. A., & Chun, M. W. (2011). Facilitating new knowledge creation and obtaining KM maturity. *Journal of Knowledge Management*, 15(2), 231-250. <https://doi.org/10.1108/13673271111119673>
- Armstrong, M. E., Jones, K. S., Namin, A. S., & Newton, D. C. (2018). The knowledge, skills, and abilities used by penetration testers: Results of interviews with cybersecurity professionals in vulnerability assessment and management. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62(1), 709-713. <https://doi.org/10.1177/1541931218621161>
- Assante, M. J., & Tobey, D., H. (2011). Enhancing the cybersecurity workforce. *IT Professional*, 13(1), 12-15. <https://doi.org/10.1109/mitp.2011.6>
- Auffret, J.-P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., Sokol, L., Allor, P., & Warweg, P. (2017). Cybersecurity leadership: Competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks*, 17(01), 1-20. <https://doi.org/10.1142/s0219265917400011>

- Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies*, *11*, 305-321. <https://doi.org/10.28945/3561>
- Bartram, D. (2005). The great eight competencies: A criterion-centric approach to validation. *Journal of Applied Psychology*, *90*(6), 1185-1203. <https://doi.org/10.1037/0021-9010.90.6.1185>
- Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15* (5/6), 337-346. <https://doi.org/10.1108/09576050210447019>
- Bassellier, G., Reich, B. H., & Benbasat, I. (2001). Information technology competence of business managers: A definition and research model. *Journal of Management Information Systems*, *17*(4), 159-182. <https://doi.org/10.1080/07421222.2001.11045660>
- Bastian, N. D., Lunday, B. J., Fisher, C. B., & Hall, A. O. (2020). Models and methods for workforce planning under uncertainty: Optimizing U.S. Army cyber branch readiness and manning. *Omega*, *92*. <https://doi.org/10.1016/j.omega.2019.102171>
- Bazeley, P. (2004). Issues in mixing qualitative and quantitative approaches to research. *Applying Qualitative Methods to Marketing Management Research*, *141*, 156.
- Beaty, R. E., Kenett, Y. N., Christensen, A. P., Rosenberg, M. D., Benedek, M., Chen, Q., Fink, A., Qiu, J., Kwapil, T. R., Kane, M. J., & Silvia, P. J. (2018). Robust prediction of individual creative ability from brain functional connectivity. *Proceedings of the National Academy of Sciences*, *115*(5), 1087-1092. <https://doi.org/10.1073/pnas.1713532115>
- Bechtsoudis, A., & Sklavos, N. (2012). Aiming at higher network security through extensive penetration tests. *IEEE Latin American Transactions*, *10*(3), 1752-1756.
- 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>
- Bender, M., L'Ecuyer, K., & Williams, M. (2019). A clinical nurse leader competency framework: Concept mapping competencies across policy documents. *Journal of Professional Nursing*, *35*(6), 431-439. <https://doi.org/10.1016/j.profnurs.2019.05.002>
- Beuran, R., Tang, D., Pham, C., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security*, *78*, 43-59. <https://doi.org/10.1016/j.cose.2018.06.001>

- Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2019). Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems*, 1–12. <https://doi.org/10.1080/08874417.2019.1579076>
- Bleed, P. (2008). Skill matters. *Journal of Archaeological Method and Theory*, 15(1), 154-166. <https://doi.org/10.1007/s10816-007-9046-0>
- Boak, G. (1991). *Developing managerial competences*. Pitman.
- Borba, B. S. M. C., Fortes, M. Z., Bitencourt, L. A., Ferreira, V. H., Maciel, R. S., Guimaraens, M. A. R., Lima, G. B. A., Barboza, E. U., Henriques, H. O., Bergaiante, N. C. R., & Moreira, B. S. (2019). A review on optimization methods for workforce planning in electrical distribution utilities. *Computers & Industrial Engineering*, 135, 286-298. <https://doi.org/10.1016/j.cie.2019.06.002>
- Boyatzis, R. E. (1982). *The competent manager: A model for effective performance*. John Wiley.
- Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology*, 11(3-4), 279-295. <https://doi.org/10.1080/0144341910110305>
- Boyer, L., Pepin, J., Dubois, S., Descôteaux, R., Robinette, L., Déry, J., Robinette, L., Dery, J., Burnet, F., Bolduc, J., & Deschênes, M. F. (2020). Adaptation and validation of a nursing competencies framework for clinical practice on a continuum of care from childhood to adulthood: A Delphi study. *Nurse Education Today*, 93, 1-8. <https://doi.org/10.1016/j.nedt.2020.104530>
- Bracewell, R. J., & Witte, S. P. (2016). Tasks, ensembles, and activity. *Written Communication*, 20(4), 511-559. <https://doi.org/10.1177/0741088303260691>
- Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, 88, 1-13. <https://doi.org/10.1016/j.cose.2019.101607>
- Brunner, M., Sauerwein, C., Felderer, M., & Brey, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. *Computers & Security*, 92, 1-32. <https://doi.org/10.1016/j.cose.2020.101776>
- Burley, D. L., & Lewis, A. H. (2019). Cybersecurity curricula 2017 and Boeing: Linking curricular guidance to professional practice. *Computer*, 52(3), 29-37. <https://doi.org/10.1109/mc.2018.2883567>

- Burlig, F. (2018). Improving transparency in observational social science research: A pre-analysis plan approach. *Economics Letters*, 168, 56-60. <https://doi.org/10.31222/osf.io/qemkz>
- Buthelezi, M. P., Van Der Poll, J. A., & Ochola, E. O. (2016, December). *Ambiguity as a barrier to information security policy compliance: A content analysis* [Conference session]. International Conference on Computational Science and Computational Intelligence. <https://doi.org/10.1109/CSCI.2016.253>
- Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. *Proceedings of the IEEE SoutheastCon 2015*, 1-7. Fort Lauderdale, Florida. <https://doi.org/10.1109/SECON.2015.7132932>
- Carlton, M., & Levy, Y. (2017). Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management*, 5(2), 16–28. [https://doi.org/10.36965/ojakm.2017.5\(2\)16-28](https://doi.org/10.36965/ojakm.2017.5(2)16-28)
- Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*, 27(1), 101-121. <https://doi.org/10.1108/ics-11-2016-0088>
- Carpenter, H. L. (2017). Philanthropy: Evidence in favor of a profession. *The Foundation Review*, 9(4). <https://doi.org/10.9707/1944-5660.1388>
- Carroll, J. B. (1993). *Human cognitive abilities: A survey of factor-analytic studies*. Cambridge University Press.
- Castro, F. G., Kellison, J. G., Boyd, S. J., & Kopak, A. (2010). A methodology for conducting integrative mixed methods research and data analyses. *Journal of Mixed Methods Research*, 4(4), 342-360. <https://doi.org/10.1177/1558689810382916>
- Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, 5(1), 1-19. <https://doi.org/10.1093/cybsec/tyz001>
- Cavusoglu, H., Cavusoglu, H., Son, J., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, 52(4), 385–400. <https://doi.org/10.1016/j.im.2014.12.004>
- The Center for Strategic Studies (2011). Cybersecurity two years later. *A report of the CSIS commission on cybersecurity for the 44th Presidency*.

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf

- Charoensap-Kelly, P., Broussard, L., Lindsly, M., & Troy, M. (2016). Evaluation of soft skills training program. *Business and Professional Communication Quarterly*, 79(2), 154-179. <https://doi.org/10.1177/2329490615602090>
- Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability. *Journal of Hospitality and Tourism Technology*, 9(2), 223–234. <https://doi.org/10.1108/jhtt-07-2017-0044>
- Chen, T. Y. (2018). Medical leadership: An important and required competency for medical students. *Tzu Chi Medical Journal* 30(2), 66-70. https://doi.org/10.4103/tcmj.tcmj_26_18
- Chenail, R. J. (2012). Conducting qualitative data analysis: Reading line-by-line, but analyzing by meaningful qualitative units. *Qualitative Report*, 17(1), 266-269. <https://doi.org/10.46743/2160-3715/2012.1817>
- Choudhury, E. H. (2007). Workforce planning in small local governments. *Review of Public Personnel Administration*, 27(3), 264-280. <https://doi.org/10.1177/0734371X06297464>
- Clark, M. A., Espinosa, J. A., & Butina, M. (2018). Cybersecurity knowledge networks. *American University*, 23, 1-11.
- Cobb, M. J. (2018). Plugging the skills gap: The vital role that women should play in cybersecurity. *Computer Fraud & Security*, 2018(1), 5-8. [https://doi.org/10.1016/s1361-3723\(18\)30004-6](https://doi.org/10.1016/s1361-3723(18)30004-6)
- Coffelt, T. A., Grauman, D., & Smith, F. L. M. (2019). Employers' perspectives on workplace communication skills: The meaning of communication skills. *Business and Professional Communication Quarterly*, 82(4), 418-439. <https://doi.org/10.1177/2329490619851119>
- Collins, J. W., Levy, J., Stefanidis, D., Gallagher, A., Coleman, M., Cecil, T., Ericsson, A., Motrie, A., Wiklund, P., Ahmed, K., Pratsckke, J., Casali, G., Ghazi, A., Gomez, M., Hung, A., Arnold, A., Dunning, J., Martino, M., Vaz, C., ... Satava, R. M. (2019). Utilising the Delphi process to develop a proficiency-based progression train-the-trainer course for robotic surgery training. *European Urology*, 75(5), 775-785. <https://doi.org/10.1016/j.eururo.2018.12.044>
- Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organizational culture, procedural countermeasures, and employee security behavior: A qualitative study. *Information & Computer Security*, 25(2), 118–136. <https://doi.org/10.1108/ics-03-2017-0013>

- Contech, N.Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31-38. <https://doi.org/10.1108/ics-03-2017-0013>
- Conti, G., & Fanelli, R. (2019). How could they not: Thinking like a state cyber threat actor. *The Cyber Defense Review*, 4(2), 49-64. <https://doi.org/10.2307/26843892>
- Cornford, I., & Athanasou, J. (1995). Developing expertise through training. *Industrial and Commercial Training*, 27(2), 10-18. <https://doi.org/10.1108/00197859510082861>
- Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced mixed methods research designs. *Handbook of mixed methods in social and behavioral research*, 209(240), 209-240. Thousand Oaks, CA: Sage publications.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, mixed methods approaches (4th ed.)*, Thousand Oaks, CA: Sage publications.
- Creswell J. W., & Poth C. N. (2018). *Designing and conducting mixed methods research (3rd ed.)*, Thousand Oaks, CA: Sage publications.
- Crumpler, W., & Lewis, J. A. (2019). Cybersecurity workforce gap. *Center for Strategic and International Studies (CSIS)*, 1-10.
- Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. *IEEE Engineering Management Review*, 47(3), 79-86.
- Cunningham, D. J., Ascher, M. T., Viola, D., & Visintainer, P. F. (2007). Baseline assessment of public health informatics competencies in two Hudson Valley health departments. *Public Health Reports*, 122(3), 302-310. <https://doi.org/10.1177/003335490712200303>
- D'Arcy, J., Hovav, A., & Galetta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 1-20. <https://doi.org/10.1287/isre.1070.0160>
- Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.
- David, D. P., Keupp, M. M., & Mermoud, A. (2020). Knowledge absorption for cyber-security. *Computers in Human Behavior*, 106, 106255. <https://doi.org/10.1016/j.chb.2020.106255>
- Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Front Psychology*, 9, 1-12. <https://doi.org/10.3389/fpsyg.2018.00744>

- De Faveri, C., Moreira, A., & Amaral, V. (2018). Multi-paradigm deception modeling for cyber defense. *Journal of Systems and Software, 141*, 32-51.
<https://doi.org/10.1016/j.jss.2018.03.031>
- Deka, L., & Barua, G. (2014). Consistent online backup in transactional file systems. *IEEE Transactions on Knowledge and Data Engineering, 26*(11), 2676-2688.
<https://doi.org/10.1109/TKDE.2014.2302297>
- Dell'Amico, M., Michiardi, P., & Roudier, Y. (2010, March). *Password strength: An empirical analysis* [Conference session]. IEEE SoutheastCon 2010, Concord, NC, United States.
- D'Elia, D. C., Coppa, E., Palmaro, F., & Cavallaro, L. (2020). On the dissection of evasive malware. *IEEE Transactions on Information Forensics and Security, 15*, 2750-2765.
<https://doi.org/10.1109/tifs.2020.2976559>
- Diedrich, A., & Guzman, G. (2015). From implementation to appropriation: Understanding knowledge management system development and introduction as a process of translation. *Journal of Knowledge Management, 19*(6), 1273-1294.
<https://doi.org/10.1108/jkm-02-2015-0055>
- Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security, 92*, 1-21.
<https://doi.org/10.1016/j.cose.2020.101747>
- Dimov, D. (2017). Competency profile of the innovative enterprises. *International Scientific Journals of Scientific Technical Union of Mechanical Engineering, 2*(3), 135-138.
<https://stumejournals.com/journals/i4/2017/3/135.full.pdf>
- Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic, and digital determinants affect diverse safety practices. *Computers & Security, 86*, 75-91. <https://doi.org/10.1016/j.cose.2019.05.023>
- Downey, J. P., McMurtrey, M. E., & Zeltmann, S. M. (2008). Mapping the MIS curriculum based on critical skills of new graduates: An empirical examination of IT professionals. *Journal of Information Systems Education, 19*(3), 351.
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology, 6*, 323-337. <https://doi.org/10.28945/3325>
- Engeström, Y. (2000). Activity theory as a framework for analyzing and redesigning work. *Ergonomics, 43*(7), 960-974. <https://doi.org/10.1080/001401300409143>

- Englander, R., Cameron, T., Ballard, A. J., Dodge, J., Bull, J., & Aschenbrener, C. A. (2013). Toward a common taxonomy of competency domains for the health professions and competencies for physicians. *Academic Medicine*, 88(8), 1088-1094. <https://doi.org/10.1097/ACM.0b013e31829a3b2b>
- European Committee for Standardization. (2019). *The what, how and why guide to e-CF*. <https://www.ecompetences.eu/>
- Evers, F. T., Rush, J. C., & Berdrow, I. (2010). *The bases of competence: Skills for lifelong learning and employability*. Jossey-Bass.
- Executive Order No. 13636, Improving critical infrastructure cybersecurity, DCPD-201300091, February 12, 2013. <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>
- Executive Order No. 13800, Strengthening the cybersecurity of federal networks and critical infrastructure, DCPD-201710004, May 11, 2017. <https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf>
- Fara, M. (2008). Masked abilities and compatibilism. *Mind*, 117(468), 843-865. <https://doi.org/10.1093/mind/fzn078>
- Farcas, M. A., & Azzie, G. (2020). Performance assessment - The knowledge, skills and attitudes of surgical performance. *Seminars in Pediatric Surgery*, 29(2), 1-4. <https://doi.org/10.1016/j.sempedsurg.2020.150903>
- Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs—principles and practices. *Health Services Research*, 48(6pt2), 2134-2156. <https://doi.org/10.1111/1475-6773.12117>
- Fink, A. (2020). *Conducting research literature reviews: From the internet to paper*. Sage.
- Fonseca, P., & Picoto, W. N. (2020). The competencies needed for digital transformation. *Online Journal of Applied Knowledge Management*, 8(2), 53-70. [https://doi.org/10.36965/ojakm.2020.8\(2\)53-70](https://doi.org/10.36965/ojakm.2020.8(2)53-70)
- Fox, J., Murray, C., & Warm, A. (2003). Conducting research using web-based questionnaires: Practical, methodological, and ethical considerations. *International journal of social research methodology*, 6(2), 167-180. <https://doi.org/10.1080/13645570210142883>
- Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalizing data saturation for theory-based interview studies. *Psychology and Health*, 25, 1229-1245. <https://doi.org/10.1080/08870440903194015>

- Francis, K. A., & Ginsberg, W. (2016). *The federal cybersecurity workforce: Background and congressional oversight issues for the Departments of Defense and Homeland Security*. 1-25.
- Franklin, N. & Melville, P. (2015). Competency assessment tools: An exploration of the pedagogical issues facing competency assessment for nurses in the clinical environment. *The Australian Journal of Nursing Practice, Scholarship Research*, 22(1), 25-31. <https://doi.org/10.1016/j.colegn.2013.10.005>
- Franzese, L. G., Fioroni, M., Pinheiro, L., & Soares, J. E. (2006). *Allocating field service teams with simulation in energy/utilities environment*. [Conference presentation]. Proceedings of the 2006 Winter Simulation Conference, Monterey, CA, United States. <https://doi.org/10.1109/wsc.2006.323124>
- Fugard, A. J., & Potts, H. W. (2015). Supporting thinking on sample sizes for thematic analyses: A quantitative tool. *International Journal of Social Research Methodology*, 18(6), 669-684. <https://doi.org/10.1080/13645579.2015.1005453>
- Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cybersecurity skills. *Computer Fraud & Security*, 2017(2), 5–10. [https://doi.org/10.1016/s1361-3723\(17\)30013-1](https://doi.org/10.1016/s1361-3723(17)30013-1)
- Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1), 27-35. <https://doi.org/10.1016/j.cose.2005.12.004>
- Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20(9), 1408. <https://doi.org/10.1016/j.cose.2005.12.004>
- Gander, S. L. (2006). Beyond mere competency: Measuring proficiency with outcome proficiency indicator scales. *Performance Improvement*, 45(4), 38-44. <https://doi.org/10.1002/pfi.2006.4930450409>
- Ganguly, A., Talukdar, A., & Chatterjee, D. (2019). Evaluating the role of social capital, tacit knowledge sharing, knowledge quality and reciprocity in determining innovation capability of an organization. *Journal of Knowledge Management*, 23(6), 1105-1135. <https://doi.org/10.1108/jkm-03-2018-0190>
- Garcia, V. J., Bernardon, D. P., Abaide, A., & Fonini, J. (2014, September 2-5). *Evaluating multicriteria scenarios to schedule emergency orders in electric distribution utilities* [Conference presentation]. 2014 49th International Universities Power Engineering Conference, Cluj-Napoka, Romania. <https://doi.org/10.1109/upec.2014.6934780>
- Garvin, D. A., Wagonfeld, A. B., & Kind, L. (2013). Google's project oxygen: Do managers

matter. *Harvard Business School Review*

Gorlatykh, A., & Zapechikov, S. (2018). Building secure multidimensional data management system. *Procedia Computer Science*, 145, 232-237.

<https://doi.org/10.1016/j.procs.2018.11.044>

Gourisetti, S. N., Mylrea, M., Gervais, E., & Bhadra, S. (2017). Multi-scenario use case based demonstration of buildings cybersecurity framework webtool. *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, 1-8. <https://doi.org/10.1109/ssci.2017.8285240>

Gravill, J. I., Compeau, D. R., & Marcolin, B. L. (2006). Experience effects on the accuracy of self-assessed user competence. *Information & Management*, 43(3), 378-394.

<https://doi.org/10.1016/j.im.2005.10.001>

Guzys, D., Dickson-Swift, V., Kenny, A., & Threlkeld, G. (2015). Gadamerian philosophical hermeneutics as a useful methodological framework for the Delphi technique. *International Journal of Qualitative Studies on Health and Well-Being*, 10(1), 26291.

<https://doi.org/10.3402/qhw.v10.26291>

Hanus, B., & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1), 2–16.

<https://doi.org/10.1080/10580530.2015.1117842>

Hasson, F., & Keeney, S. (2011). Enhancing rigor in the Delphi technique research.

Technological Forecasting and Social Change, 78(9), 1695–1704.

<https://doi.org/10.1016/j.techfore.2011.04.005>

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, 32(4), 1008-1015. <https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x>

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept.

Computers & Security, 73, 102-113. <https://doi.org/10.1016/j.cose.2017.10.008>

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers.

International Journal of Information Management, 43, 165-172.

<https://doi.org/10.1016/j.ijinfomgt.2018.07.013>

Havelka, D., & Merhout, J. W. (2009). Toward a theory of Information technology professional competence. *Journal of Computer Information Systems*, 50(2), 106-116.

<https://doi.org/10.1080/08874417.2009.11645389>

- Heckman, K. E., Walsh, M. J., Stech, F. J., O'boyle, T. A., Dicato, S. R., & Herber, A. F. (2013). Active cyber defense with denial and deception: A cyber-wargame experiment. *Computers & Security, 37*, 72-77. <https://doi.org/10.1016/j.cose.2013.03.015>
- Hemenway, D. (2001). The public health approach to motor vehicles, tobacco, and alcohol, with applications to firearms policy. *Journal of Public Health Policy, 22*(4), 381-402. <https://doi.org/10.2307/3343157>
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. <https://doi.org/10.1057/ejis.2009.6>
- Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically building cybersecurity workforce. *IEEE Security & Privacy Magazine, 10*(2), 33-39. <https://doi.org/10.1109/msp.2011.181>
- Hogarth, R. M. (1978). A note on aggregating opinions. *Organizational Behavior and Human Performance, 21*(1), 40-46. [https://doi.org/10.1016/0030-5073\(78\)90037-5](https://doi.org/10.1016/0030-5073(78)90037-5)
- Holm, H. (2012). Performance of automated network vulnerability scanning at remediating security issues. *Computers & Security, 31*(2), 164-175. <https://doi.org/10.1016/j.cose.2011.12.014>
- Horsman, G., Laing, C., & Vickers, P. (2014). A case-based reasoning method for locating evidence during digital forensic device triage. *Decision Support Systems, 61*, 69-78. <https://doi.org/10.1016/j.dss.2014.01.007>
- Horton, S. (2000). Introduction – The competency movement: Its origins and impact on the public sector. *International Journal of Public Sector Management, 13*(4), 306-318. <https://doi.org/10.1108/09513550010350283>
- Hong, Q. N., Pluye, P., Fàbregues, S., Bartlett, G., Boardman, F., Cargo, M., ... & Vedel, I. (2019). Improving the content validity of the mixed methods appraisal tool: a modified e-Delphi study. *Journal of clinical epidemiology, 111*, 49-59. <https://doi.org/10.1016/j.jclinepi.2019.03.008>
- Hsu, C., & Sabherwal, R. (2012). Relationship between intellectual capital and knowledge management: An empirical investigation. *Decision Sciences, 43*(3), 489-524. <https://doi.org/10.1111/j.1540-5915.2012.00357.x>
- Huang, W., Boateng, A., & Newman, A. (2016). Capital structure of Chinese listed SMEs: An agency theory perspective. *Small Business Economics, 47*(2), 535–550.

- Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering*, 45(4), 3171-3189. <https://doi.org/10.1007/s13369-019-04319-2>
- Ikeda, K., Marshall, A., & Zaharchuk, D. (2019). Agility, skills and cybersecurity: Critical drivers of competitiveness in times of economic uncertainty. *Strategy & Leadership*, 47(3), 40-48. <https://doi.org/10.1108/sl-02-2019-0032>
- Internet Crime Compliant Center (2018). *Internet crime report*. https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf
- Internet Crime Compliant Center (2019). *Internet crime report*. https://pdf.ic3.gov/2019_IC3Report.pdf
- Internet Crime Complaint Center (2022). Internet crime report. <https://www.ic3.gov/Media/Y2022/PSA220504>
- Ioannou, M., Stavrou, E., & Bada, M. (2019, June 3-4). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination [Conference paper]. *2019 International Conference on Cyber Security and Protection of Digital Services*, Oxford, United Kingdom.
- Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field Methods*, 18(1), 3-20. <https://doi.org/10.1177/1525822X05282260>
- Jajodia, S., Park, N., Pierazzi, F., Pugliese, A., Serra, E., Simari, G. I., & Subrahmanian, V. S. (2017). A probabilistic logic of cyber deception. *IEEE Transactions on Information Forensics and Security*, 12(11), 2532-2544. <https://doi.org/10.1109/tifs.2017.2710945>
- James, L. (2018). Making cyber-security a strategic business priority. *Network Security*, 2018(5), 6-8. [https://doi.org/10.1016/s1353-4858\(18\)30042-4](https://doi.org/10.1016/s1353-4858(18)30042-4)
- James, T., Nottingham, Q., & Kim, B. C. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information Technology and Management*, 14(2), 69–89. <https://doi.org/10.1007/s10799-012-0147-4>
- Jeris, L., & Johnson, K. (2004, March 4-7). *Speaking of "competence": Toward a cross-translation for Human Resource Development and Continuing Professional Education*. Academy of Human Resource Development Annual Conference, Austin, TX, United States.
- Ji, X., Wang, B., Liu, D., Dong, Z., Chen, G., Zhu, Z., Zhu, X., & Wang, X. (2016). Will electrical cyber–physical interdependent networks undergo first-order transition under

random attacks? *Physical A: Statistical Mechanics and Its Applications*, 460, 235-245.
<https://doi.org/10.1016/j.physa.2016.05.017>

Johnson, G., Scholes, K. & Whittington, R. (2008). *Exploring corporate strategy*.
 Prentice Hall.

Joint Task Force on Cybersecurity Education. (2017). *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity*.
<https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school. *ACM Transactions on Computing Education*, 18(3), 1-12. <https://doi.org/10.1145/3152893>

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *British journal of applied science & technology*, 7(4), 396.
<https://doi.org/10.9734/BJAST/2015/14975>

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75–87.
<https://doi.org/10.1016/j.chb.2016.09.012>

Karafili, E., Wang, L., & Lupu, E. C. (2020). An argumentation-based reasoner to assist digital investigation and attribution of cyber-attacks. *Forensic Science International: Digital Investigation*, 32, 1-9. <https://doi.org/10.1016/j.fsidi.2020.300925>

Karie, N. M., Kebande, V. R., & Venter, H. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy*, 1, 61-67. <https://doi.org/10.1016/j.fsisyn.2019.03.006>

Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & Security*, 93, 1-18.
<https://doi.org/10.1016/j.cose.2020.101782>

Keeney, R. L. (1999). The value of Internet commerce to the customer. *Management Science*, 45(4), 533-542. <https://doi.org/10.1287/mnsc.45.4.533>

Khodabakhshi, F., Sajad, N. K. & Shiargar, M. (2013). The impact of knowledge management on innovation with the mediating role of empowerment. *Life Science Journal*, 10(2), 1385-1390. <https://doi.org/10.7537/marslsj100213.190>

Klein, J. D. (2013, September). Design and development research: A rose by another name?

- [Conference session]. *AERA Design-Based Research Conference*, Athens, GA, United States.
- Kost, R. G., & da Rosa, J. C. (2018). Impact of survey length and compensation on validity, reliability, and sample characteristics for ultrashort-, short-, and long-research participant perception surveys. *Journal of Clinical and Translational Science*, 2(1), 31-37. <https://doi.org/10.1017/cts.2018.18>
- Kouttis, S. (2016). Improving security knowledge, skills, and safety. *Computer Fraud & Security*, 2016(4), 12–14. [https://doi.org/10.1016/s1361-3723\(16\)30037-9](https://doi.org/10.1016/s1361-3723(16)30037-9)
- Krogh, G. V., Nonaka, I., & Ichijo, K. (1997). Develop knowledge activists! *European Management Journal*, 15(5), 475-483. [https://doi.org/10.1016/s0263-2373\(97\)00028-5](https://doi.org/10.1016/s0263-2373(97)00028-5)
- Kriz, D. (2011, June 1-2). Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity. [Conference session]. 2011 *Second Worldwide Cybersecurity Summit*, London, United Kingdom.
- Lane, J.S., (2019). Creating the competency in social justice action scale (CSJAS) [Doctoral dissertation, North Carolina State University]. <https://repository.lib.ncsu.edu/bitstream/handle/1840.20/36593/etd.pdf?sequence=1&isAllowed=y>
- Le Deist, F. D., & Winterton, J. (2005). What is competence? *Human Resource Development International*, 8(1), 27-46. <https://doi.org/10.1080/1367886042000338227>
- Levy, Y. (2005). A case study of management skills comparison in online and on-campus MBA programs. *International Journal of Information and Communication Technology Education*, 1(3), 1-20. <https://doi.org/10.4018/jicte.2005070101>
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Information Science Publishing.
- Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education*, 51(4), 1664-1675. <https://doi.org/10.1016/j.compedu.2008.04.003>
- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: The International Journal of an Emerging Transdiscipline*, 9, 181–212. <https://doi.org/10.28945/479>
- Levy, Y., & Ramim, M. M. (2015). An assessment of competency-based simulations on e-learners' management skills enhancements. *Interdisciplinary Journal of e-Skills and Life-Long Learning*, 11, 179-190. <https://doi.org/10.28945/2309>

- Liang, S., Zhang, Y., Li, B., Guo, X., Jia, C., & Liu, Z. (2018). Secureweb: Protecting sensitive information through the web browser extension with a security token. *Tsinghua Science and Technology*, 23(5), 526-538. <https://doi.org/10.26599/tst.2018.9010015>
- Lin, H. F., & Lee, G. G. (2005). Impact of organizational learning and knowledge management factors on e-business adoption. *Management Decision*, 23(2), 0025-1747. <https://doi.org/10.1108/00251740510581902>
- Lin, P., Chang, Y., Lin, H., & Hong, H. (2017). Fostering college students' creative capacity through computer-supported knowledge building. *Journal of Computers in Education*, 4(1), 43-56. <https://doi.org/10.1007/s40692-016-0063-4>
- Longo, M. C., & Giaccone, S. C. (2017). Struggling with agency problems in open innovation ecosystem: Corporate policies in innovation hub. *The Total Quality Management Journal*, 29(6), 881-898.
- Lucia, A. D., & Lepsinger, R. (1999). *The art and science of competency models: Pinpointing critical success factors in organizations*. Jossey-Bass/Pfeiffer.
- MacLean, P., Gregory S. Anderson, D., & Cahillane, M. (2015). The human factor in learning design, research, policy, and practice. *International Journal of Information and Learning Technology*, 32(3), 182-196. <https://doi.org/10.1108/ijilt-12-2014-0029>
- McCleskey, J. A. (2014). Situational, transformational, and transactional leadership and leadership development. *Journal of Business Studies Quarterly*, (5), 4, 117-130.
- Mailloux, L. O., & Grimaila, M. (2018). Advancing cybersecurity: The growing need for a cyber-resiliency workforce. *IEEE Access*, 20(3), 23-30.
- Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, 27(2), 233-272. <https://doi.org/10.1108/ics-03-2018-0031>
- Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32-44. <https://doi.org/10.1016/j.chb.2018.01.028>
- Markus, M. L. (2001). Toward a theory of knowledge reuse: Types of knowledge reuse situations and factors in reuse success. *Journal of Management Information Systems*, 18(1), 57-93. <https://doi.org/10.1080/07421222.2001.11045671>

- Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. [Conference paper]. 2017 *European Intelligence and Security Informatics Conference*, Athens, Greece.
- McCrudden, M. T., & McTigue, E. M. (2019). Implementing integration in an explanatory sequential mixed methods study of belief bias about climate change with high school students. *Journal of Mixed Methods Research*, 13(3), 381-400. <https://doi.org/10.1177/1558689818762576>
- Meadows, N., Webb, D., McRobbie, D., Antoniou, S., Bates, I., & Davies, G. (2004). Developing and validating a competency framework for advanced pharmacy practice. *The Pharmaceutical Journal*, 273, 789-792. <https://discovery.ucl.ac.uk/id/eprint/1368463>
- Mehra, A., Langer, N., Bapna, R., & Gopal, R. (2014). Estimating returns to training in the knowledge economy: A firm-level analysis of small and medium enterprises. *MIS Quarterly*, 38(3), 757-771. <https://doi.org/10.25300/misq/2014/38.3.06>
- Menges, F., & Pernul, G. (2018). A comparative analysis of incident reporting formats. *Computers & Security*, 73, 87-101. <https://doi.org/10.1016/j.cose.2017.10.009>
- Merhia, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior*, 92, 37-46. <https://doi.org/10.1016/j.chb.2018.10.031>
- Meyer, G. J., Lorz, T., Wehner, R., Jaeger, J., Dauer, M., & Krebs, R. (2020). Hybrid fuzzy evaluation algorithm for power system protection security assessment. *Electric Power Systems Research*, 189, 1-7. <https://doi.org/10.1016/j.epsr.2020.106555>
- Meyer, M. A. (2019). Competencies required for healthcare improvement positions. *International Journal of Health Care Quality Assurance*, 32(1), 281-295. <https://doi.org/10.1108/IJHCQA-12-2017-0236>
- Molinaro, K. A., & Boltona, M. L. (2018). Evaluating the applicability of the double system lens model to the analysis of phishing email judgments. *Computers & Security*, 77, 128-137. <https://doi.org/10.1016/j.cose.2018.03.012>
- Momin, W. Y. M., & Mishra, K. (2015). HR analytics as a strategic workforce planning. *International Journal of Applied Research*, 1(4), 258-260.
- Mora, H., Pujol-López, F. A., Mendoza-Tello, J. C., & Morales-Morales, M. R. (2018). An education-based approach for enabling the sustainable development gear. *Computers in Human Behavior*, 107, 1-11. <https://doi.org/10.1016/j.chb.2018.11.004>

- Mullen, P. M. (2003). Delphi: Myths and reality. *Journal of Health Organization and Management*, 17(1), 37-52. <https://doi.org/10.1108/14777260310469319>
- Mylrea, M., Gourisetti, S. N. G., & Nicholls, A. (2017, November 27-December 1). *An introduction to buildings cybersecurity framework* [Symposium presentation]. 2017 IEEE Symposium Series on Computational Intelligence, Honolulu, HI, United States
- National Initiative for Cybersecurity Education (NICE) (2017), *National Cybersecurity Workforce Framework*, 2. <https://www.nist.gov/file/359261>
- National Institute of Standards and Technology (NIST). (2014). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- National Institute of Health (NIH), Office of Human Resources. (2019). *Competency Proficiency Scale*. <https://hr.nih.gov/working-nih/competencies/competencies-proficiency-scale>.
- Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, 92, 101731. <https://doi.org/10.1016/j.cose.2020.101731>
- Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication*, 800(2017), 181, 1-130. <https://doi.org/10.6028/NIST.SP.800-181>
- Nilsen, R. K., Levy, Y., & Terrell, S. R. (2017). A developmental study on assessing the cybersecurity competency of organizational information system users. *Journal of Cybersecurity Education, Research and Practice*, 2017(2), 1-36. <https://digitalcommons.kennesaw.edu/ccerp/2017/research/1>
- Nonaka, I. (1991). The knowledge-creating company. *Harvard Business Review*, 85(7/8), 96-104.
- Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, 5(1), 14-37. <https://doi.org/10.4777/0898/94/0501/0014>
- Nyanchama, M. (2005). Enterprise vulnerability management and its role in information security management. *Information Systems Security*, 14(3), 29-56. <https://doi.org/10.1201/1086.1065898x/45390.14.3.20050701/89149.6>
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & management*, 42(1), 15-29.

<https://doi.org/10.1016/j.im.2003.11.002>

- Onwubiko, C., & Ouazzane, K. (2020). SOTER: A playbook for cybersecurity incident management. *IEEE Transactions on Engineering Management*, 1-21. <https://doi.org/10.1109/tem.2020.2979832>
- Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, 88, 1-14. <https://doi.org/10.1016/j.cose.2019.101608>
- Parsons, D. (2010). Medical-workforce planning: An art or science? *Human Resource Management International Digest*, 18(5), 36-38. <https://doi.org/10.1108/09670731011060289>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, 42, 165-176. <https://doi.org/10.1016/j.cose.2013.12.002>
- Pătrascu, A., & Patriciu, V. (2013, May 23-25). *Beyond digital forensics. A cloud computing perspective over incident response and reporting* [Symposium presentation]. 2013 IEEE 8th International Symposium on Applied Computational Intelligence and Informatics, Timișoara, Romania. <https://doi.org/10.1109/saci.2013.6609018>
- Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy*, 10(3), 76-79.
- 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. <https://doi.org/10.6028/NIST.SP.800-181rl-draft>
- Petterson, I. B., Åmo, B. W., van der Lingen, E., Håvåg Voldsund, K., & Johnstad Bragelien, J. (2019). Developing engineering students' willingness and ability to perform creative tasks. *Education + Training*, 61(9), 1138-1150. <https://doi.org/10.1108/et-10-2018-0219>
- Philip, M., & Lindley, P. (2006). People are our greatest asset: A model of real workforce development to turn rhetoric into reality. *The Journal of Mental Health Training, Education and Practice*, 1(1), 37-41. <https://doi.org/10.1108/17556228200600006>
- Podmetina, D., Soderquist, K. E., Petraite, M., & Teplov, R. (2018). Developing a competency model for open innovation. *Management Decision*, 56(6), 1306-1335. <https://doi.org/10.1108/MD-04-2017-0445>

- Popper, M., & Lipshitz, R. (1993). Putting leadership theory to work: A conceptual framework for theory based leadership development. *Leadership & Organization Development Journal*, 14(7), 23-27. <https://doi.org/10.1108/01437739310047001>
- Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, 20(1), 121-139. <https://doi.org/10.1287/isre.1080.0174>
- Raponi, S., & Pietro, R. D. (2020). A longitudinal study on web-sites password management (in) security: Evidence and remedies. *IEEE Access*, 8, 52075-52090. <https://doi.org/10.1109/access.2020.2981207>
- Renauda, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsabilization of the cyber security risk reasonable and judicious? *Computer & Security*, 78, 198–211. <https://doi.org/10.1016/j.cose.2018.06.006>
- Rojewski, J. W., Choi, I., Hill, J. R., Ko, Y., Walters, K. L., Kwon, S., & McCauley, L. (2019). Career orientation and perceived professional competence among clinical research coordinators. *Journal of Clinical and Translational Science*, 3(5), 234-244. <https://doi.org/10.1017/cts.2019.385>
- Rowe, G., Wright, G., & Bolger, F. (1991). Delphi: A reevaluation of research and theory. *Technological Forecasting and Social Change*, 39(3), 235-251. [https://doi.org/10.1016/0040-1625\(91\)90039-I](https://doi.org/10.1016/0040-1625(91)90039-I)
- Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Jeimy, J. (2019). An effective cybersecurity training model to support an organizational awareness program: The cybersecurity awareness training model (CATRAM). A case study in Canada. *Journal of Cases on Information Technology*, 21(3), 1–14. <https://doi.org/10.4018/JCIT.2019070102>
- Salah, K., & Kahtani, A. (2009). Improving snort performance under Linux. *IET Communications*, 3(12), 1883-1895. <https://doi.org/10.1049/iet-com.2009.0114>
- Saleh, S., Qadir, J., & Ilyas, M. U. (2018). Shedding light on the dark corners of the Internet: A survey of tor research. *Journal of Network and Computer Applications*, 114, 1-28. <https://doi.org/10.1016/j.jnca.2018.04.002>
- Salkind, N. J. (2018). *Exploring research*. Pearson Education Limited.
- Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organizational cybersecurity: A knowledge-problem perspective. *Journal of Intellectual Capital*, 20(4), 581–597. <https://doi.org/10.1108/JIC-03-2019-0041>

- Sandelowski, M. (1995). Sample size in qualitative research. *Research in Nursing & Health*, *18*(2), 179–183
- Sandelowski, M. (2000). Whatever happened to qualitative description?. *Research in Nursing & Health*, *23*(4), 334-340.
- Sarker, I. H., Colman, A., Han, J., Khan, A. I., Abushark, Y. B., & Salah, K. (2019). BehavDT: A behavioral decision tree learning to build user-centric context-aware predictive model. *Mobile Networks and Applications*, *25*(3), 1151-1161. <https://doi.org/10.1007/s11036-019-01443-z>
- Sarnikar, S., & Deokar, A. V. (2017). A design approach for process-based knowledge management systems. *Journal of Knowledge Management*, *21*(4), 693-717. <https://doi.org/10.1108/jkm-09-2016-0376>
- Schneider, J. K., & Deenan, A. (2004). Reducing quantitative data errors: Tips for clinical researchers. *Applied Nursing Research*, *17*(2), 125-129. <https://doi.org/10.1016/j.apnr.2004.02.001>
- Schrimmer, K., Williams, N., Mercado, S., Pitts, J., & Polancich, S. (2019). Workforce competencies for healthcare quality professionals: Leading quality-driven healthcare. *Journal for Healthcare Quality*, *41*(4), 259-265. <https://doi.org/10.1097/JHQ.0000000000000212>
- Seele, H., & Eberl, P. (2020). Newcomers' reactions to unfulfilled leadership expectations: An attribution theory approach. *European Management Journal*. <https://doi.org/10.1016/j.emj.2020.02.007>
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (6th Ed.). John Wiley & Sons Ltd.
- Shah, M., Maitlo, A., Jones, P., & Yusuf, Y. (2019). An investigation into agile learning processes and knowledge sharing practices to prevent identity theft in the online retail organisations. *Journal of Knowledge Management*, *23*(9), 1857-1884. <https://doi.org/10.1108/jkm-06-2018-0370>
- Shaikh, I. A., & O'Connor, G. C. (2020). Understanding the motivations of technology managers in radical innovation decisions in the mature R&D firm context: An agency theory perspective. *Journal of Engineering and Technology Management*, *55*, 101553. <https://doi.org/10.1016/j.jengtecman.2020.101553>
- Sharevski, F., Trowbridge, A., & Westbrook, J. (2018, March 10). *Novel approach for cybersecurity workforce development: A course in secure design* [Conference session]. IEE Integrated STEM Conference, Princeton, NJ, United States.

- Sharma, R. K., Issac, B., & Kalita, H. K. (2019). Intrusion detection and response system inspired by the defense mechanism of plants. *IEEE Access*, 7, 52427-52439. <https://doi.org/10.1109/access.2019.2912114>
- Shoemaker, D. (2015). The NICE framework: Why you need to understand this important initiative. *The EDP Audit, Control, and Security*, 51(6), 1-7. <https://doi.org/10.1080/07366981.2015.1054241>
- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, 177-191. <https://doi.org/10.1016/j.cose.2015.01.002>
- Shulman, L. (1987). Knowledge and teaching: Foundations of the new reform. *Harvard Educational Review*, 57(1), 1-23.
- Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems*, 37, 31-63. <https://doi.org/10.17705/1cais.03702>
- Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education: Research*, 6(1), 1-21. <https://doi.org/10.28945/199>
- Smith, G. (2018). The intelligent solution: Automation, the skills shortage and cyber-security. *Computer Fraud & Security*, 2018(8), 6-9. [https://doi.org/10.1016/s1361-3723\(18\)30073-3](https://doi.org/10.1016/s1361-3723(18)30073-3)
- Solms, B. V., & Solms, R. V. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, 26(1), 2-9. <https://doi.org/10.1108/ics-04-2017-0025>
- Somayyeh, S. & Morteza, P. (2015). Investigation the role of knowledge management in staff empowerment. *International Journal of Review in Life Sciences*, 5(4), 163-168.
- Soundaram, M. N., & Pon-Rek, D. M. (2018). A study on core competency levels of IT employees vs. size of the company – A special reference to Chennai. *International Journal of Research and Analytical Reviews*, 5(2), 2008-2011. http://ijrar.com/upload_issue/ijrar_issue_1130.pdf
- Spink, A., & Sollenberger, M. (2004). Elicitation purposes and tasks during mediated information search. *Journal of Documentation*, 60(1), 77-91. <https://doi.org/10.1108/00220410410516662>

- Sternberg, R. J. (1998). Abilities are forms of developing expertise. *Educational Researcher*, 27(3), 11-20. <https://doi.org/10.2307/1176608>
- Sternberg, R. J., & Detterman, D. K. (1986). *What is intelligence? Contemporary viewpoints on its nature and definition*. Norwood, NJ. Ablex Publishing Corporation.
- Sternberg, R. J., & Kaufman, J. C. (1998). Human abilities. *Annual Review of Psychology*, 49(1), 479-502.
- Sussman, L. L. (2018). Exploring Non-Technical Knowledge, Skills, and Abilities (KSA) that May Expand the Expectations of the Cyber Workforce. *Investigating Framework Adoption, Adaptation, or Extension National CyberWatch Center Digital Press ID NCC-2020-CSJ-02 csj. nationalcyberwatch.org*, 19.
- Tashakkori, A., & Creswell, J. W. (2007). The new era of mixed methods. *Journal of Mixed Methods Research*, 1(1), 3-7. <https://doi.org/10.1177/2345678906293042>
- Telha, A., Rodrigues, A., Páscoa, C., & Tribolet, J. (2016). The competency architecture as error limiting element and efficiency enhancer in business processes. *Procedia Computer Science*, 100, 665–670. <https://doi.org/10.1016/j.procs.2016.09.209>
- Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructure: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans* 40(4), 853-865. <https://doi.org/10.1109/TSMCA.2010.2048028>
- Terrell, S. R. (2015). *Writing a proposal for your dissertation: Guidelines and examples*. New York, NY. Guilford Publications.
- Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, 32(10), 1014-1023. <https://doi.org/10.1080/0144929x.2013.763860>
- Tobey, D. H., Gandhi, R. A., Watkins, A. B., & O'Brien, C. W. (2018). Competency is not a three letter word: A glossary supporting competency-based instructional design in cybersecurity. *Cybersecurity Skills Journal: Practice and Research*, 20, 32-38.
- Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computer & Security*, 79, 68–79. <https://doi.org/10.1016/j.cose.2018.08.007>
- Vargas-Halabi, T., Mora-Esquivel, R., & Siles, B. (2017). Intrapreneurial competencies: Development and validation of a measurement scale. *European Journal of Management and Business Economics*, 26(1), 86-111. <https://doi.org/10.1108/ejmbe-07-2017-006>

- Urias, V. E., Leeuwen, B. V., Stout, W. M., & Lin, H. W. (2017, April 25-26). *Dynamic cybersecurity training environments for an evolving cyber workforce*. [Conference session]. 2017 IEEE International Symposium on Technologies for Homeland Security, Waltham, MA, United States. <https://doi.org/10.1109/ths.2017.7943509>
- Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, 4(2), 32–46. <https://www.salusjournal.com>
- Walker, A. M., & Selfe, J. (1996). The Delphi method: A useful tool for the allied health researcher. *British Journal of Therapy and Rehabilitation*, 3(12), 677-681. <https://doi.org/10.12968/bjtr.1996.3.12.14731>
- Wan, H., Chen, F. F., & Kuriger, G. W. (2011). An intelligent decision support system for workforce forecast. Texas University at San Antonio. <https://doi.org/10.21236/ada537920>
- Wegner, D. M. (1987). Transactive memory: A contemporary analysis of the group mind. *Theories of Group Behavior*, 185-208. https://doi.org/10.1007/978-1-4612-4634-3_9
- Wei, F., Wan, Z., & He, H. (2020). Cyber-attack recovery strategy for smart grid based on deep reinforcement learning. *IEEE Transactions on Smart Grid*, 11(3), 2476-2486. <https://doi.org/10.1109/tsg.2019.2956161>
- Whitman, M., & Mattord, H. J. (2018). *Principles of information security*. Cengage Learning Inc.
- Wilkerson, J. W. (2020). An alumni assessment of MIS related job skill importance and skill gaps. *Journal of Information Systems Education*, 23(1), 85-97.
- Wilson, R. D., & Klein, J. D. (2012). Design, implementation, and evaluation of a nursing simulation: A design and development research study. *The Journal of Applied Instructional Design*, 2(1), 57-68. http://myweb.fsu.edu/jklein/articles/Wilson_Klein_2012.pdf
- Wirojanagud, P., Gel, E. S., Fowler, J. W., & Cardy, R. (2007). Modelling inherent worker differences for workforce planning. *International Journal of Production Research*, 45(3), 525-553. <https://doi.org/10.1080/00207540600792242>
- Woodruffe, C. (1991). Competent by any other name. *Personnel Management*, 30-33.
- Xiong, B., Yang, K., Zhao, J., & Li, K. (2017). Robust dynamic network traffic partitioning against malicious attacks. *Journal of Network and Computer Applications*, 87, 20-31. <https://doi.org/10.1016/j.jnca.2016.04.013>

- Yagan, O., Qian, D., Zhang, J., & Cochran, D. (2012). Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. *IEEE Transactions on Parallel and Distributed Systems*, 23(9), 1708-1720. <https://doi.org/10.1109/tpds.2012.62>
- Yang, Z., Sun, J., Zhang, Y., & Wang, Y. (2015). Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. *Computers in Human Behavior*, 45, 254–264. <https://doi.org/10.1016/j.chb.2014.12.022>
- Zhang, L., Wei, W., & Hua, N. (2019). Impact of data breach locality and error management on attitude and engagement. *International Journal of Hospitality Management*, 78, 159–168. <https://doi.org/10.1016/j.ijhm.2018.12.001>
- Zhang, M., Martin, P., Powley, W., & Chen, J. (2018). Workload management in database management systems: A taxonomy. *IEEE Transactions on Knowledge and Data Engineering*, 30(7), 1386-1402. <https://doi.org/10.1109/tkde.2017.2767044>