2017

Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges

Richard Nilsen
Nova Southeastern University, rn380@nova.edu

NSUWorks Citation

Richard Nilsen. 2017. *Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1017)
https://nsuworks.nova.edu/gscis_etd/1017.

Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges

by

Richard K. Nilsen

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

College of Engineering and Computing
Nova Southeastern University

2017

We hereby certify that this dissertation, submitted by Rich Nilsen, 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

10/10/2017
Date

Dawn M. Beyer

Dawn Beyer, Ph.D.
Dissertation Committee Member

10/10/2017
Date

Steven R. Terrell, Ph.D.
Dissertation Committee Member

10/10/17
Date

Approved:

Yong X. Tao, Ph.D., P.E., FASME
Dean, College of Engineering and Computing

10/10/17
Date

College of Engineering and Computing
Nova Southeastern University

2017

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

Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges

by
Richard K. Nilsen
September 2017

Organizational information system users (OISU) that are victimized by cyber threats are contributing to major financial and information losses for individuals, businesses, and governments. Moreover, it has been argued that cybersecurity competency is critical for advancing economic prosperity and maintaining national security. The fact remains that technical cybersecurity controls may be rendered useless due to a lack of cybersecurity competency of OISUs. All OISUs, from accountants to cybersecurity forensics experts, can place organizational assets at risk. However, that risk is increased when OISUs do not have the cybersecurity competency necessary for operating an information system (IS). The main goal of this research study was to propose and validate, using subject matter experts (SME), a reliable hands-on prototype assessment tool for measuring the cybersecurity competency of an OISU. To perform this assessment, SMEs validated the critical knowledge, skills, and abilities (KSA) that comprise the cybersecurity competency of OISUs. Primarily using the Delphi approach, this study implemented four phases of data collection using cybersecurity SMEs for proposing and validating OISU: KSAs, KSA measures, KSA measure weights, and cybersecurity competency threshold. A fifth phase of data collection occurred measuring the cybersecurity competency of 54 participants.

Phase 1 of this study performed five semi-structured SME interviews before using the Delphi method and anonymous online surveys of 30 cybersecurity SMEs to validate OISU cybersecurity KSAs found in literature and United States government (USG) documents. The results of Phase 1 proposed and validated three OISU cybersecurity abilities, 23 OISU cybersecurity knowledge units (KU), and 22 OISU cybersecurity skill areas (SA). In Phase 2, two rounds of the Delphi method with anonymous online surveys of 15 SMEs were used to propose and validate OISU cybersecurity KSA measures. The results of Phase 2 proposed and validated 90 KSA measures for 47 knowledge topics (KT) and 43 skill tasks (ST). In Phase 3, using the Delphi method with anonymous online surveys, a group of 15 SMEs were used to propose and validate OISU cybersecurity KSA weights. The results of Phase 3 proposed and validated the weights for four knowledge categories (KC) and four skill categories (SC). When Phase 3 was completed, the MyCyberKSAs^{TM} prototype assessment tool was developed using the results of Phases 1-3, and Phase 4 was initiated. In Phase 4, using the Delphi method with anonymous online surveys, a group of 15 SMEs were used to propose and validate an OISU cybersecurity competency threshold (index score) of 80%, which was then integrated into the MyCyberKSAs^{TM} prototype tool. Before initiating Phase 5, the MyCyberKSAs^{TM}

prototype tool was fully tested by 10 independent testers to verify the accuracy of data recording by the tool. After testing of the MyCyberKSAs^{TM} prototype tool was completed, Phase 5 of this study was initiated. Phase 5 of this study measured the cybersecurity competency of 54 OISUs using the MyCyberKSAs^{TM} prototype tool. Upon completion of Phase 5, data analysis of the cybersecurity competency results of the 54 OISUs was conducted.

Data analysis was conducted in Phase 5 by computing levels of dispersion and one-way analysis of variance (ANOVA). The results of the ANOVA data analysis from Phase 5 revealed that annual cybersecurity training and job function are significant, showing differences in OISU cybersecurity competency. Additionally, ANOVA data analysis from Phase 5 showed that age, cybersecurity certification, gender, and time with company were not significant thus showing no difference in OISU cybersecurity competency.

The results of this research study were validated by SMEs as well as the MyCyberKSAs^{TM} prototype tool; and proved that the tool is capable of assessing the cybersecurity competency of an OISU. The ability for organizations to measure the cybersecurity competency of OISUs is critical to lowering risks that could be exploited by cyber threats. Moreover, the ability for organizations to continually measure the cybersecurity competency of OISUs is critical for assessing workforce susceptibility to emerging cyber threats. Furthermore, the ability for organizations to measure the cybersecurity competency of OISUs allows organizations to identify specific weaknesses of OISUs that may require additional training or supervision, thus lowering risks of being exploited by cyber threats.

Acknowledgements

Whenever someone is successful at achieving a goal, there's a good chance many people helped along the way. If I thanked everyone by name that helped me along the way to becoming a Ph.D., this dissertation would be nine million pages long. Seriously, it is a long list.

I've never officially thanked her, but I would like to thank Ms. Smith, my guidance councilor from Bloom Trail High School. It took her three years, but finally in the fourth quarter of my senior year, she single handedly convinced me to go to college. This was a decision that would change my life forever, thank you Ms. Smith!

I also need to thank my classmates, friends, and family for all of the help as well as encouragement throughout my studies. This study had five phases of data collection. I needed a lot of help to meet all of my data requirements, and you all were critical for me even being able to finish this study, thank you! I also have to thank the SMEs that participated in this study. I needed SMEs for four phases of data collection, and my Phase 2 instrument was enormous. Thank you for all of your time and patience!

I want to express my utmost appreciation to my dissertation committee, Dr. Steven Terrell and Dr. Dawn Beyer. All of your expertise was greatly appreciated, thank you! I cannot say thank you enough for all of the hard work you contributed, especially multiple reviews on a 300-page paper.

Then there is my dissertation chair, Dr. Yair Levy. My respect for Dr. Levy as an educator and a person could not be higher. I can honestly say that I have never met a person that works as hard as Dr. Levy. Thank you for the hundreds of hours you have invested in me and my dissertation. Thank you for all of the knowledge and expertise you have passed on, I won't waste it!

I have to thank my father and brothers, they have listened to me whine about schoolwork for the last 25 years! Not only that, growing up in my house, it was cool to be smart. No joke, due to a board game, we actually argued the accuracy and limitations of dictionaries. They were not always friendly arguments either, but they were all epic.

Last but not least, my wife Niki. I know I'm going to get a lot of kudos and congratulations for finishing my doctorate. I wish that credit could go to my wife instead, she worked just as hard as I did, if not more. At times, especially early on, I felt like an absentee dad and husband. I knew getting a doctorate would be hard, but it was even more difficult than I expected, which took a major time investment. While being a full time doctoral student I also worked full time, we had a baby, I coached my daughters softball team, completed Air Command and Staff College, and switched jobs. Niki was always very supportive about my goals and helped me see this thru. Sweetheart, I'm done with my homework! You finally have your husband back. Thank you for everything, honey. I could not have done this without you!!! How long is my honey-do list? And how long do I have to get it done?

For Madison, For Elinore

Madison and Elinore, always follow your dreams. One way to accomplish your dreams is by being educated. Maddie, if you want to be an animator for Disney, you have to go to college. Ellie, if you still want to become a "baby getting out doctor" when you get older, you too will have to go to college. And trust me, you both are more than capable of making it happen. I promise, mom and I will be there for you for any and all higher education goals that you may have in your lives. But education isn't the only way to accomplish your dreams. Follow your hearts and stay true to yourselves. Never live your lives trying to make other people happy, do what makes you happy! Be an individual, follow your own path, and everything will work out just fine, I promise!

Table of Contents

Chapters

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

The advent of cyberspace has transformed the methods of information delivery as well as information storage for individuals, businesses, and governments (Doneda & Almeida, 2015). Due to a minimally regulated digital infrastructure, the exploitation of cyberspace with malicious intent threatens the rights of individuals, privacy of individuals, assets of private enterprises, and even the security of nations (Paulsen, McDuffie, Newhouse, & Toth, 2012). Essentially, the infrastructure of cyberspace, mostly the Internet, is not secure or resilient (Garfinkel, 2012). Due to the dire need for cybersecurity, the Comprehensive National Cybersecurity Initiative (CNCI) explicitly stated that the Executive Branch of the United States (U.S.) government has been directed to work closely with all of the major actors in national cybersecurity (NSC, 2015). These actors include local governments, state governments, private industry, and academic institutes, whom will help to build a digital workforce for the 21st century (NSC, 2015). While businesses and governments spend billions of dollars on security technologies, the user of an information system (IS) remains one of the most critical cyber vulnerabilities (Huber, Kowalski, Nohlberg, & Tjoa, 2009; Lesk, 2011).

In an attempt to mitigate the IS user vulnerability in cybersecurity, organizations have provided security, education, training, and awareness (SETA) programs to employees (Han, Kim, & Kim, 2017; Warkentin, Straub, & Malimage, 2012). Such SETA programs are usually provided to all individuals that require access to organizational networks in an effort to reduce security breaches or loss of information due to IS user error, ignorance, malicious intent such as insider threat, or negligence (Abawajy, 2012; Choi & Song, 2016; D'Arcy, Hovav, & Galletta, 2009; DISA, 2015; Han et al., 2017). The Defense Information Systems Agency (DISA) offers cybersecurity awareness training, named the Cybersecurity Awareness Challenge, for the Department of Defense (DoD), non-DoD federal employees, and intelligence personnel (DISA, 2015). Furthermore, the DoD requires that both military personnel and federal civilians must annually complete the Cybersecurity Awareness Challenge with a passing score in order to maintain network access privileges.

A literature review on SETA programs in the U.S. government (USG) revealed an apparent lack of documentation regarding the programs, along with the validity and instrument development of measures of success (Behrens, Alberts, and Ruefle, 2012; Toth & Klein, 2013). Furthermore, a literature review on the measurement of cybersecurity competency revealed an apparent literature gap regarding how to define and measure cybersecurity competency (Burley, Eisenberg, & Goodman, 2014). Additionally, current literature acknowledges there is critical lack of information regarding the assessment of cybersecurity competency (Assante & Tobey, 2011; Evans & Reeder, 2010; Johnson, 2012). As such, there was a need to establish a definition and develop measurement of cybersecurity competency. Thus, this study proposed and validated a method for determining the combined necessary knowledge, skills, and abilities (KSA) of IS users to achieve cybersecurity competency for the attainment of organizational network access privileges.

Problem Statement

The research problem that this study addressed is significant financial, information, and intellectual property loses for organizations as well as governments as a result of inadequate cybersecurity competency of IS users (Barlow, Warkentin, Ormond, & Dennis, 2013; Choi, Levy, & Hovav, 2013; Shaw, Chen, Harris, & Huang, 2009). Cybersecurity as defined by the Association of Computing Machinery Joint Task Force (ACMJTF) on Cybersecurity Education (2016) is a "computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (p. 1). Competency is defined by Draganidis and Mentzas (2006) as:

> A specific, identifiable, definable, and measurable knowledge, skill, ability and/or other deployment-related characteristic (e.g. attitude, behaviour, physical ability) which a human resource may possess and which is necessary for, or material to, the performance of an activity within a specific business context. (p. 52)

Additionally, Alavi and Leidner (2001) defined knowledge as "a justified belief that increases an entity's capacity for taking effective action" (p. 109). Prager, Moran, and Sanchez (1997) defined ability as "the capacity to carry out physical and mental acts required by tasks" (p. 39). According to Boyatzis and Kolb (1995), skill is defined as a "goal-directed, well-organized behavior that is acquired through practice and performed with economy of effort" (p. 18). However, the use of the term behavior is problematic when describing skill since behavior is a specific psychological phenomenon that involves a decision process, while many aspects of cybersecurity involves users performing actions without thinking (Smith, 2015; Zipf, 2016). Boyatzis and Kolb (1995) also defined skill as “a combination of ability, knowledge, and experience that enables a person to do something well” (p. 4). This definition of skill is problematic as well by stating that skill is a combination of knowledge and ability, while other research contents knowledge and ability are separate measurables (Behrens et al., 2012; Draganidis & Mentzas, 2006; Toth & Klein, 2013). Combining the two definitions of skill by Boyatzis and Kolb (1995) appears to provide a sufficient definition of skill. Thus, skill is defined in this research study as a goal-directed, well-organized set of actions that is acquired through practice and performed with economy of effort, which enables a person to do something well (Boyatzis & Kolb, 1995).

Cybersecurity professionals are a vital component in combating cyber threats (Paulsen et al., 2012). Cybersecurity professionals are required to have a high level of combined KSAs (i.e. competency) to create and implement technologies, as well as manage human resources in order to: *identify* cyber threats and vulnerabilities, *protect* information and resources, *detect* the occurrences of cybersecurity events, *respond* to incidents, as well as *recover* from cybersecurity events (Paulsen et al., 2012; NIST, 2014). However, most IS users are not cybersecurity professionals, the majority of IS users are lacking awareness as well as training in information technology (IT) and cybersecurity (Happ, Melzer, & Steffgen, 2016; Hazari, Hargrave, & Clenney, 2008).

Lack of cybersecurity competency of IS users is a risk to organizational networks, which is of utmost importance since the exploitation of user technical incompetency is contributing to substantial financial losses for governments and organizations all over the world (Choi et al., 2013). To mitigate the cybersecurity KSA shortfalls of IS users, many companies and governments have instituted initiatives such as SETA programs or cyber awareness programs (D'Arcy, Hovav, & Galletta, 2009; DISA, 2015). However, there appeared to be a lack of scholarly literature and government documentation regarding how to measure the cybersecurity competency for an organizational IS user (OISU). Furthermore, there appeared to be a literature gap within the body of knowledge regarding how to quantify an acceptable cybersecurity competency level of an OISU. Therefore, additional research to establish such a way to quantify an acceptable cybersecurity competency level of an OISU was necessary (Johnson, 2012; O'Neil, Assante, & Tobey, 2012; Sabeil, Manaf, Ismail, & Abas, 2011).

Research Goals

The main goal of this research study was to propose and validate, using subject matter experts (SME), a reliable hands-on prototype assessment tool for measuring the combined necessary KSAs for cybersecurity competency of an OISU. This study intended to build on the work of Behrens et al. (2012), as well as Toth and Klein (2013), by developing a cybersecurity competency assessment tool. This assessment tool was in the form of a Website, with content that was validated by SMEs, that were used to measure a core set of required cybersecurity abilities, cybersecurity knowledge units, and cybersecurity skills that are necessary to pass a cybersecurity competency threshold, as illustrated in Figure 1.

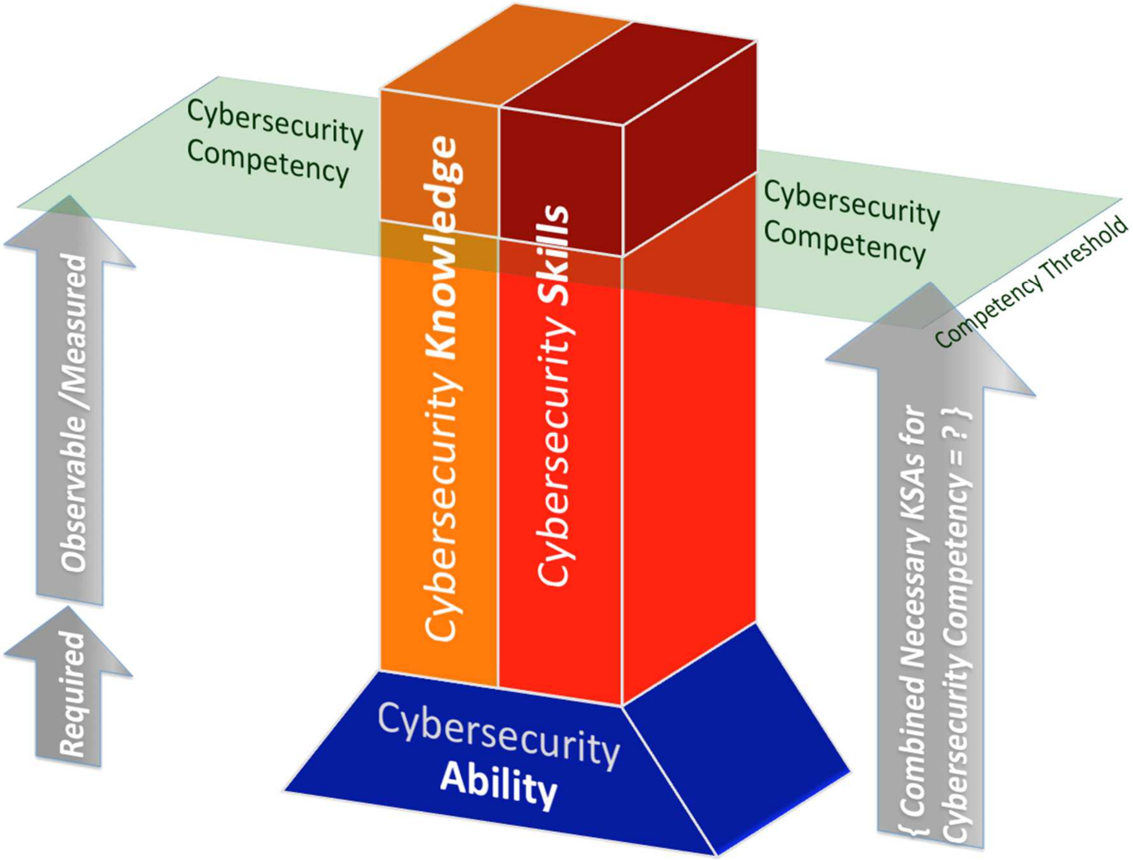


Figure 1. Model of Combined Necessary KSAs for Cybersecurity Competency Attainment for an Organizational Information System User

As such, when an individual possesses the required cybersecurity abilities, the increase in cybersecurity knowledge and skills will reach a certain level that can be identified as cybersecurity competency threshold. The intent of the cybersecurity competency threshold is to establish a minimum score that should be achieved when participating in a competency assessment (Ahmed, Ishman, Laeeq, & Bhatti, 2013; Jacob & Chalia, 2015). Behrens et al. (2012) proposed a Competency Lifecycle Roadmap (CLR) for developing and sustaining cybersecurity competencies. The CLR consists of five phases: assess, plan, acquire, validate, and test readiness. Moreover, Toth and Klein (2013) noted that all IS users within an organization are in need of continuous security awareness training. Toth and Klein (2013) also contended that all IS users are required to possess Cybersecurity Essentials competency. Toth and Klein (2013) also noted that Cybersecurity Essentials competency ensures an OISU possesses the desired applied KSA levels to protect information and systems. However, both studies, while indicating the importance of such a tool and the need for assessment of cybersecurity competency threshold level, do not provide a way to measure such KSAs or propose a minimum threshold level (Behrens et al., 2012; Toth & Klein, 2013).

To achieve the main goal, this study addressed five specific research goals. The first specific goal of this study was to identify the cybersecurity KSAs, validated by SMEs, which are required to assess cybersecurity competency of OISUs. The second specific goal of this study was to identify cybersecurity KSA measures, validated by SMEs, which are also necessary to assess cybersecurity competency of OISUs. The third specific goal of this study was to develop and validate, using SMEs, a reliable hands-on prototype assessment tool (MyCyberKSAs^{TM}) that will measure cybersecurity competency of OISUs using the validated KSAs measures. The fourth specific goal of this study was to determine the threshold, using SMEs, from the MyCyberKSAs^{TM} hands-on prototype assessment tool scoring at which cybersecurity competency of OISUs was reached. The fifth specific goal of this study was to measure the cybersecurity competency of 50 OISUs and report the results of such assessments.

Research Questions

The main research question that this study addressed is how can an assessment for cybersecurity competency be accomplished using KSAs and at what level of KSAs the cybersecurity competency threshold is established?

The five specific research questions that this research study addressed are:

RQ1. What are the specific SME approved *set of cybersecurity KSAs*, which need to be measured to assess the attainment of cybersecurity competency by OISUs for organizational network access?

RQ2. What are the SME approved cybersecurity *KSA measures*, which are needed to assess the attainment of cybersecurity competency by OISUs for organizational network access?

RQ3. What are the SME identified *weights of the cybersecurity KSA measures*, which are needed to assess the attainment of cybersecurity competency by OISUs for organizational network access to form the MyCyberKSAs^{TM} hands-on assessment prototype?

RQ4. What is the SME identified cybersecurity *competency threshold* for the combined *KSA measures*, which is the maximum needed for organizational network access as measured by the MyCyberKSAs^{TM} hands-on assessment prototype?

RQ5. What is the cybersecurity *competency level* as measured by the MyCyberKSAs^{TM} hands-on assessment prototype of a sample of 50 OISUs?

Relevance and Significance

Relevance

The relevance for this study was that the IS user's cybersecurity competency continues to be a problem (Behrens et al., 2012; Toth & Klein, 2013). Additionally, organizations may be under constant duress by advanced persistent threats, which continually attempt to exploit a large array of vulnerabilities for specific targets (Marchetti, Pierazzi, Colajanni, & Guido, 2016). Furthermore, regardless of which technical cybersecurity controls are in place, they can be negated by the IS users due to a lack of cybersecurity competency (Al Neaimi, Ranginya, & Lutaaya, 2015; Behrens et al., 2012; Toth & Klein, 2013). Phishing attacks are still one of the most effective vectors for infiltrating a secure system, due in large part to a lack of cybersecurity competency of IS users (Bowen, Devarajan, & Stolfo, 2012; Verma, Kantarcioglu, Marchette, Leiss, & Solorio, 2015). Additionally, recent studies show the need for the assessment of skills and competencies (Grus, Falender, Fouad, & Lavelle, 2016; Levy & Ramim, 2015). Moreover, the advent of new technologies introduces new vulnerabilities, which increases the need to continually and accurately assess cybersecurity competency (Johnson, 2012; Pittenger, 2016).

Significance

The USG contends that cybersecurity is critical for advancing economic prosperity and national security (Hoffman & Branlat, 2016; NIST, 2012). Additionally, cybersecurity competency is crucial for minimizing financial losses to organizations as well as threats to national security (Choi et al., 2013; NIST, 2014). Furthermore, cybersecurity competency contributes to compliance with laws, regulations, and Constitutional requirements (NIST, 2014).

Barriers and Issues

This research study contained several potential issues with conducting this type of exploratory research. First, as this study was dependent on SME responses, a low SME response rate would be problematic towards internal validity and adherence to the Delphi method. This study required a minimum of 15 SMEs for the first round of each phase of data collection. Thus, to minimize the probability of low response rates, this study contacted SMEs continuously per phase of data collection, until at the target number of responses were received.

An additional issue with this study was that the cybersecurity abilities of OISUs were not directly measured. The measurement of the identified OISU cybersecurity abilities was done via the surrogate measure of the individuals' education. Surrogating abilities significantly reduced the time commitment of MyCyberKSAs^{TM} prototype tool participants. To fully measure the defined cybersecurity abilities of OISUs, external tools would need to be employed. For example, measuring written comprehension could require the use of one or more of the following examination batteries: the Gray Oral Reading Test, the Qualitative Reading Inventory, the Woodcock–Johnson Passage Comprehension subtest, and/or the Peabody Individual Achievement Test Reading Comprehension subtest (Keenan, Betjemann, & Olson, 2008). Therefore, considering the estimated MyCyberKSAs^{TM} prototype tool size, surrogating for abilities was critical to maintain usability of the tool. The issue of surrogating the cybersecurity abilities of OISUs with education was additionally listed as a limitation of this study.

Another potential issue with this research study was the length of the data collection process. A long data collection process may contribute to non-response rates. This study conducted five phases of data collection from SMEs using the Delphi method. Therefore, the data collection instruments from Phases 1 and 2 were developed mostly from literature and USG documentation in order to negate the dependency of the SME to provide all of the KSAs and KSA measures.

Finally, the issue exists of SME bias based on their professional environment. While SMEs from government are concerned with access control by using access cards to log on to computers, SMEs from the private sector may be more concerned with strength of password. To resolve this potential issue, this study attempted to use an equal proportion of SMEs from government and from industry.

Assumptions, Limitations, and Delimitations

Assumptions

1. SMEs were honest with their responses.
2. Not all of the cybersecurity SMEs will participate in all four phases of SME required data collection.
3. An individual with a minimum of a high school diploma (or equivalent) possesses the required OISU cybersecurity abilities.

Limitations

A potential limitation of the Delphi method is the level of commitment exercised by the expert panel (Hill & Fowles, 1975). Level of commitment is essential because if a SME feels a survey is too long, they may have a low level of commitment, and therefore submit responses that are convenient/quick instead of accurate/detailed. Another potential limitation would be a bias introduced by selecting expert panel members from one specific USG agency or from one specific company. The surrogation of cybersecurity ability for education is a potential limitation of this study. Additionally, this study considers measuring skills with a Web-based tool as a limitation, as a live demonstration of the skill being performed would be most accurate/optimal measure.

Delimitations

A delimitation of this study was to inform each SME of the level of commitment necessary to participate in this study. Specifically, Phase 2 required emphasis regarding alerting the SMEs that at least an hour of time to complete may be needed without the ability to save responses. Another delimitation of this study was to select SMEs from multiple agencies/companies to serve on the expert panel.

Definitions of Terms

Ability – "the capacity to carry out physical and mental acts required by tasks" (Prager et al., 1997, p. 39).

Advanced persistent threat – "a form of cyber attack that is characterised by a high degree of technological and process sophistication mixed with a prolonged duration (Warren, 2015, p. 7).

Access control – “the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner” (Lopez, Oppliger, & Pernul, 2004, p. 580).

Antivirus software – “a program that attempts to identify, thwart and eliminate computer viruses and other malicious software” (Karantjias & Polemi, 2010, p. 60)

Behavior – “human interaction with the environment” **(**Lewin, 1943, p. 294).

Competency – “a specific, identifiable, definable, and measurable knowledge, skill, ability and/or other deployment-related characteristic (e.g. attitude, behaviour, physical ability) which a human resource may possess and which is necessary for, or material to, the performance of an activity within a specific business context” (Draganidis & Mentzas, 2006, p. 52).

Cookie usage - the storing of information generated from Internet browsing into a text file, that may contain unencrypted sensitive information or PII and may be used to track activity (DISA, 2015).

Cyber threats – any sources or circumstances that have the potential to compromise the confidentiality, integrity, and availability of an information system (Jung, Han, & Suh, 1999; Mejias & Balthazard, 2014).

Cyber vulnerabilities – “weaknesses or flaws, in terms of security and privacy” (Kalloniatis, Mouratidis, & Islam, 2013, p. 4).

Cybersecurity – a “computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (ACMJTF, 2016, p. 1).

Cybersecurity controls - technical, operational, and management controls that protect Availability, Integrity, and Confidentiality of information and information systems **(**Hassanzadeh, Modi, & Mulchandani, 2015; Saleh & Alfantookh, 2011).

Cybersecurity points of contact (POCs) – cybersecurity POCs include but are not limited to "computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information officers (CIOs), computer security program managers, and others who are responsible for preparing for, or responding to, security incidents" (Cichonski, Millar, Grance, & Scarfone, 2012, p .1)

Cybersecurity responsibilities – OISU cybersecurity responsibilities are protecting sensitive information, protecting information systems, protecting PII, providing physical security, and potentially updating software (Gross & Rosson, 2007; Karantjias & Polemi, 2010).

Cyberspace – "a computer-generated landscape, i.e. the virtual space of a global computer network, linking all people, computers, and sources of various information in the world through which one could navigate" (Jiang & Ormeling, 2000, p. 117).

Delphi method – "an iterative process to collect and distill the anonymous judgments of experts using a series of data collection and analysis techniques interspersed with feedback" (Skulmoski et al., 2007, p. 1).

Email encryption – "the process by which [email] is encoded so that only an authorized recipient can decode and consume the [email]" (Microsoft, 2016a).

Email Acceptable Use Policy – "An email acceptable use policy sets out your employees' responsibilities when using email in their day-to-day working activities" (NIBusinessInfo, 2016).

Event – "an unwanted incident or unauthorized intrusion that has occurred, is occurring, or may occur" (Garvey, Moynihan, & Servi, 2013, p. 2).

Exploit – "a particular instance of an attack on a computer system that leverages a specific vulnerability or set of vulnerabilities" (Barnum & McGraw, 2005, p. 78)

External validity - external validity "examines whether or not an observed causal relationship should be generalized to and across different measures, persons, settings, and times" (Calder et al., 1982, p. 240).

File Permissions – "grant or deny access to the files and folders" (Microsoft, 2016b).

Incident – "a security-related adverse event in which there is a loss of information confidentiality, disruption of information or system integrity, disruption or denial of system availability, or violation of any computer security policies" (Ng, Kankanhalli, & Xu, 2009, p. 815).

Incident reporting – the act of reporting suspicious individuals, worker misconduct, and all security incidents (Parsons et al., 2014).

Information handling – The access, creation, destruction, disposition, distribution, maintenance, receipt, storage, transmittal, and use of information (Bernard, 2007).

Information privacy – "the claim of individuals, groups, or institutions to determine when, and to what extent, information about them is communicated to others" (Lallmahamood, 2007, p. 7).

Information system – “a system to collect, process, store, transmit, and display information” (Avison & Wood-Harper, 1986, p. 175).

Insider threat – “a user who has appropriate permissions to access required resources of the system and misuses its privileges” (Saxena, Choi, & Lu, 2016, p. 907)

Intellectual property – “legally protected rights concerning ownership of specific intellectual assets such as patents, copyrights, trademarks, and trade secrets” (Hayton, 2005, p.141).

Internal validity - the likelihood that “observed effects could have been caused by or correlated with a set of unhypothesized and/or unmeasured variables” (Straub, 1989, p. 151).

Internet acceptable use policy – “guidelines for employees indicating both acceptable and unacceptable Internet usages, with the intention of controlling employee [behaviors] and actions which contribute to the incidence and severity of the [organization’s] Internet risks” (Lichtenstein & Swatman, 1997, p. 1).

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

KSAs - All possible knowledge, skills, and abilities required to perform a specific job function (Barnowski & Anderson, 2005).

Mobile computing – “using portable computers capable of wireless networking” (Johansson & Andersson, 2015, p. 1).

Password reuse – using the same password for multiple accounts (Ives, Walsh, & Schneider, 2004).

Personally Identifiable Information (PII) – “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information” (McCallister, Grance, & Scarfone, 2010, p. 7).

Phishing – “a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion” (Jakobsson & Myers, 2007, p. 1).

Physical security – “physical measures taken to safeguard personnel, to protect unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft” (Newsome & Jarmon, 2016, p. 322)

Policy compliance – adherence to a policy, where a policy is defined as “a course or principle of action adopted or proposed by a government, party, business, or individual” (Oxford, 2016, p.1).

Prototype – “a system constructed for evaluation purposes that has only limited function and performance” (Lowry, 1992, p. 74).

Psychological phenomenon – “the evolution of consciousness, the personal unfolding of ways of organizing experience that are not simply replaced as we grow but subsumed into more complex systems of mind” (Kegan, 1995, p. 9).

Reliability - “the extent to which a variable or set of variables is consistent in what it is intended to measure” (Straub et al., 2004, p. 70).

Resilient – “the capacity to move on in a positive way from negative, traumatic or stressful experiences” (Jackson, Firtko, & Edenborough, 2007, p. 2).

Secure – A system is secure when “the risk of unlawful interference is acceptable and collaborative support is enabled” (Hird, Hawley, & Machin, 2016, p. 487).

Security breach – “unauthorized access to or acquisition of computerized data” (Lesemann, 2016, p. 213).

Sensitive information – “protected information that the owner does not want to reveal to others and not to be divulged outside the [organization] as well as Information about an individual’s racial or ethnic origin, criminal record, sexual preferences or practices and other information that include political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, or a trade union” (Ajigini, Van der Poll, & Kroeze, 2012, p. 7).

Social engineering – “the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks” (Abraham & Chengalur-Smith, 2010, p. 183).

Social networking – “Web-based services allowing individuals to: (a) construct a profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and interact with their list of connections and those made by others within that system” (Weeden, Cooke, & McVey, 2013, p. 250).

Skill – a goal-directed, well-organized set of actions that is acquired through practice and performed with economy of effort, which enables a person to do something well (Boyatzis & Kolb, 1995).

Smart cards – "credit card-shaped devices incorporating an integrated circuit chip (memory, microprocessor, application-specific, etc.), although they can also take the form of tokens, keys, and non-credit card-shaped card-type devices" (Hester & Joseph, 1998, p. 54).

Spear-phishing – "a type of phishing attack that targets particular individuals, groups of people, or organizations" (DISA, 2015).

Spillage – "when information is spilled from a higher classification or protection level to a lower classification or protection level" (DISA, 2015).

Strong passwords – "having more than eight characters, at least one change of case, a number that is not at the end, and a non-alphanumeric character such as # or * that is also not at the end of the password" (Keller, Powell, Horstmann, Predmore, & Crawford, 2005, p. 13).

Subject matter expert (SME) – "a person with special knowledge or skills in a particular area of endeavor" (Kaplanski, 2010, p. 53).

Surrogate – "a substitute" (Plotkin, 2008, p. 401).

Threat – "a series of malicious computer activities that threaten and compromise the security & integrity of a computer/network system" (Mangla & Panda, 2013, p. 1439).

Vector – "a path by which a cyber criminal can pick up access to a network server or a computer in order to deliver a malicious effect" (Lemoudden, Bouazza, Ouahidi, & Bourget, 2013, p. 328)

Vulnerability – “a weakness that lets attackers gain entry to the system” (Arief, Adzmi, & Gross, 2015, p. 75)

Whaling – a form of spear-phishing that targets high-level personnel (DISA, 2015).

Summary

The research problem that this study addressed was significant financial, information, and intellectual property loses for organizations as well as governments are a result of inadequate cybersecurity competency of IS users (Barlow et al., 2013; Choi et al., 2013; Shaw et al., 2009). To address this research problem, this study set a main goal to propose and validate, using SMEs, a reliable hands-on prototype assessment tool for measuring the combined necessary KSAs for cybersecurity competency of an OISU. The SMEs that participated in this research study were cybersecurity experts, not end-users, and established the content needed to assess the cybersecurity competency of an OISU. This study conducted five phases of data collection. The first four phases conducted Delphi method data collection from 15-30 SMEs per phase. The fifth phase of data collection used the MyCyberKSAs^{TM} prototype assessment tool to collect cybersecurity competency data from 50 OISUs.

In the first phase of data collection, the SMEs proposed and validated existing KSAs found in literature and USG documentation. The second phase of data collection requested the SMEs propose and validate specific tasks from which KSAs will be measured. This study surrogated abilities at a required level (threshold of the ‘assumed abilities’) based on the individuals’ education indicated, which was collected via the demographics part of the prototype tool. In the third phase of data collection, the SMEs proposed and validated weights of the KSAs. These combined weighted KSAs constitute the cybersecurity competency of an OISU based on the SME determined competency threshold that was proposed and validated in the fourth phase of data collection. The fifth phase of this study tested the MyCyberKSAs^{TM} prototype assessment tool with 50 participants.

Chapter 2

Literature Review

Introduction

In this chapter, a review of the literature was performed to provide a theoretical foundation for this research study. While the literature review determined there was a need to assess the cybersecurity competency of OISUs, there appeared to be no established method to measure the cybersecurity competency of OISUs. Furthermore, there was a lack of information on how to quantify the threshold at which cybersecurity competency starts. Therefore, this literature review gathered the cybersecurity KSAs found in relevant peer reviewed literature and USG documentation. This chapter also presents elements of the cybersecurity KSAs of OISUs as to gain insight into performing accurate measurements.

Cybersecurity Competency

Ultimately, cybersecurity competency is required for meeting the five concurrent and continuous functions of the NIST Cybersecurity Framework: identify, protect, detect, respond, and recover (NIST, 2014). Competency is defined by Draganidis and Mentzas (2006) as:

> A specific, identifiable, definable, and measurable knowledge, skill, ability and/or other deployment-related characteristic (e.g. attitude, behaviour, physical ability) which a human resource may possess and which is necessary for, or material to, the performance of an activity within a specific business context. (p. 52)

An assessment of cybersecurity competency must be demonstrated, which can be accomplished by multiple methods, and should not be assumed solely based on previously earned academic degrees or professional certifications (Kay, Pudas, & Young, 2012; Tobey, 2015). Methods of measuring cybersecurity competency includes, but is not limited to, scoring game-based competitions or by scoring applied KSA tasks (Abawajy, 2014; Tobey, 2015). Tobey (2015) performed a game-based cybersecurity competency assessment for network defense where game content was collaborated by expert panels comprised of SMEs. Tobey (2015) then asked the SMEs to define competency models as well as develop a library of validated assessment questions, training curriculum, and simulation-based learning components.

While there is a limited amount of literature regarding the assessment of cybersecurity competencies, many competency assessment studies are available in other fields. Many medical studies have been performed using the Delphi method to assess competency (Bonner & Stewart, 2001; Czabanowska, Klemenc-Ketis, Potter, Rochfort, Tomasik, Csiszar, & Van den Bussche, 2012; Duffield, 1993; Sizer, Felstehausen, Sawyer, Dornier, Matthews, & Cook, 2007; Penciner, Langhan, Lee, Mcewen, Woods, & Bandiera, 2011; Staggers, Gassert, & Curran, 2002). The term competency has been leveraged in medical competency assessment studies as the threshold that must be reached when assessing a score of combined KSA measurements, or by treating each KSA as an individual competency (Czabanowska et al., 2012; Sizer et al., 2007).

Many Delphi competency studies (Czabanowska et al., 2012; Penciner et al., 2011) refer to all KSAs as independent competencies, other studies measure KSAs as a single competency where a defined threshold can be met or exceeded (Ahmed et al., 2013; Jacob & Chalia, 2015). Studies also refer to ‘competency threshold’ as ‘competency score’ and ‘competency level’ (Jacob & Chalia, 2015; Korndorffer, Scott, Sierra, Brunner, Dunne, Slakey, & Hewitt, 2005). Korndorffer et al. (2005) defined separate aggregate (variable) laparoscopic surgery competency threshold scores for each KSA. A different approach was used by Jacob and Chilia (2015) where SMEs defined a comprehensive partograph competency threshold of 70%.

While a competency assessment may be performed using a paper document, it has been shown that competency assessments should be accomplished using Web services due to simplified communication, information collection, and information sharing (Fetters, Motohara, Ivey, Narumoto, Sano, Terada, Tsuda, & Inoue, 2017; Haywood, Goode, Gao, Smith, Bronheim, Flocke, & Zyzanski, 2014). Furthermore, the measures of competency assessments should not be too broad; therefore, technical or functional competencies must be the focus of the assessment (Shippmann, Ash, Batjtsta, Carr, Eyde, Hesketh, Kehoe, Pearlman, Prien, & Sanchez, 2000; Succar, Sher, & Williams, 2013). Additionally, competency assessments should attempt to abbreviate the list of KSAs if at all possible in the interest of usability (Gebbie & Merrill, 2002). Most importantly, when assessing competency of an individual, the level of competency needs to be established (Garavan & McGuire, 2001). Specifically, competency assessments may be designed to measure a threshold level (minimum competency) or superior performance level (expert) (Garavan & McGuire, 2001; Shahidi, Ou, Telford, & Enns, 2015).

Knowledge, Skills, and Abilities (KSA)

The term KSAs encompasses all possible knowledge, skills, and abilities required to perform a specific job function (Barnowski & Anderson, 2005; Conklin, Cline, & Roosa, 2014). KSAs are also directly linked to specific actions that are required to complete job tasks (Baker, 2013; Barnowski & Anderson, 2005). Thus, measuring KSAs will identify the competency gaps that require additional training (Chen, Shore, Zaccaro, Dalal, Tetrick, & Gorab, 2014). In addition to identifying competency gaps, Baker (2013) stated that "KSAs are measures that specify the level of task performance" (p. 4). Therefore, as all combined KSAs form a competency, the competency measurement indicates if the combined KSAs are performed at a low or high level (Barnowski & Anderson, 2005; Chen et al., 2014; Conklin et al., 2014)

In the area of cybersecurity, there are numerous different jobs correlated to many different KSAs (Campbell, O'Rourke, & Bunting, 2015; Conklin et al., 2014). Certain jobs may require a high level of combined KSAs as to where others may require a low level of combined KSAs (Conklin et al., 2014; Lu, Guo, Luo, & Chen, 2015). Additionally, KSAs are not necessarily transferrable between career fields or job functions (Conklin et al., 2014). Therefore, measuring cybersecurity KSAs must focus on a foundational set of KSAs for all job functions or set of job tasks that requires an IS (Chen et al., 2014; Conklin et al., 2014). In regards to OISUs, job function is the large scope view of using an IS for work related purposes, or using an IS to complete work related tasks (Chen et al., 2014; Conklin et al., 2014). It is thus inferred that any job that requires the individual to use an IS, where the IS is Internet enabled, requires a baseline group of OISU cybersecurity KSAs. The baseline OISU cybersecurity KSAs do not need to be at the expert level; however, the minimum level of operational competency shall be required by all IS users (Besnard & Arief, 2004; Chen et al., 201; Marcolin, Compeau, Munro, & Huff, 2000; Toth & Klein, 2013).

Various theories have been applied to the study of KSAs. Grounded Theory has been applied to the proposal of development and operation KSAs (Bang, Chung, Choh, & Dupuis, 2013). Grounded Theory has also been applied to the development of curriculum KSAs (Phelan & Mills, 2010). KSAs have also been studied using Person-Environment Fit Theory (Jansen & Kristof-Brown, 2006). A study on KSAs using the Theory of Performance is of particular note as the argument is made that while an individual may possess a high level of KSAs, performance may still be substandard due to low motivation factors (Aryee, Walumbwa, Seidu, & Otaye, 2016).

The proposal and validation of KSAs for a certification or competency assessment may occur using SMEs (Wang, Schnipke, & Witt, 2005; Watson & Portenga, 2014). It is critical to ensure SMEs are qualified as experts within the field of study (Watson & Portenga, 2014). When KSAs are used to perform an assessment, it is critical that the KSA measures are weighted, as to prioritize importance (Honts, Prewett, Rahael, & Grossenbacher, 2012; Wang et al., 2005). A methodology for facilitating the use of SMEs is the Delphi method (Manley & Zinser, 2012). Weights can be determined by using the value-focused thinking approach (Keeney, 1999; Torkzadeh & Dhillon, 2002). The value-focused thinking approach allows the weights to be proposed and validated by dividing the KSAs into groups, then assigning 100 (percentage) points within each group to rate importance (Keeney, 1999; Smith, Wagner, Wallace, Pourabdollah, & Lewis, 2016).

Cybersecurity Abilities

Prager et al. (1997) defined ability as "the capacity to carry out physical and mental acts required by tasks" (p. 39). Ability includes the mental and/or physical capacity to apply knowledge and skills to perform a task (Tobey, 2015). Moreover, ability is the foundation for knowledge and skill application (Prager et al., 1997; Tobey, 2015).

Near vision, written communication, written expression, advanced written comprehension, and problem sensitivity are fundamental abilities that are required to function in many domains, including the cybersecurity of OISUs (Campbell et al., 2015; Trippe, Moriarty, Russell, Carretta, & Beatty, 2014). Near vision, or accurate near vision, is defined as "close-up viewing, usually defined for objects less than 2 feet or about 60 [centimeters] from the eyes" (Colman, 2015, p. 1). It is inferred that near vision is advised as a cybersecurity ability to be able to view computer screens. Problem sensitivity is defined as the "ability to tell when something is wrong or is likely to go wrong. It does not involve solving the problem, only recognizing there is a problem" (Trippe et al, 2014, p. 185). It is inferred that problem sensitivity is advised as a cybersecurity ability to be able to determine if an issue is or is not a cybersecurity incident. Advanced written comprehension is defined as the "ability to read and understand technical and/or government documents" (Trippe et al, 2014, p. 185). It is inferred that advanced written comprehension is advised as a cybersecurity ability to be able to read cybersecurity guidance and policies. Written communication is defined as the "transmission of [a] message in written symbols" (Terkan, 2013, p. 149). Poteet (1980) defined written expression as "a visible representation of thoughts, feelings, and ideas using symbols of the writer's language system for the purpose of communication or recording" (p. 88). It is inferred that written expression is advised as a cybersecurity ability to be able to write cybersecurity incident reports and communicate with a cybersecurity point of contact (POC) regarding issues. Table 1 presents the OISU cybersecurity abilities found in literature.

It appears the majority of literature regarding cybersecurity ability is classifying skills as ability. Rhee, Kim, and Ryu (2009) contended that understanding cybersecurity terminology is an ability. The contention of Rhee et al. (2009) is supported by Siponen, Mahmood, and Pahnila (2014) when noting that the ability to understand cybersecurity terminology is foundational for the ability to adhere to as well as apply cybersecurity policies and procedures. However, other studies in literature have shown that understanding terminology is a skill (Nguyen, 1998; Yule, Flin, Paterson-Brown, Maran, & Rowley, 2006).

Hagen and Albrechtsen (2009) noted that the three main abilities critical to ensure cybersecurity are: the ability to anticipate, monitor, and respond to cybersecurity challenges. However, it can be argued that the abilities noted by Hagen and Albrechtsen (2009) should be classified as skills. Using the definition of skill as defined by this research study, the abilities noted by Hagen and Albrechtsen (2009) are skills because they are organized goal-directed actions that are acquired through practice and performed with economy of effort.

Table 1

Summary of OISU Cybersecurity Ability Literature

OISU Abilities	**Source**
Oral comprehension	Campbell et al., 2015; Trippe et al., 2014
Near vision	Campbell et al., 2015; Trippe et al., 2014
Problem sensitivity	Campbell et al., 2015; Trippe et al., 2014
Written communication	Campbell et al., 2015; Trippe et al., 2014
Advanced written comprehension	Campbell et al., 2015; Trippe et al., 2014
Written expression	Campbell et al., 2015; Trippe et al., 2014

Cybersecurity Knowledge

The definition of knowledge is not clear and has been researched since as early as Plato (Shulman, 1987). A philosophical definition of knowledge can simply be 'what is known' (Shulman, 1987). Alavi and Leidner (2001) defined knowledge as "a justified belief that increases an entity's capacity for taking effective action" (p. 109). Cognitive psychologists have presented evidence that knowledge is the combination of declarative knowledge and procedural knowledge (Camerer & Hogarth, 1999). Bassellier, Reich, and Benbasat (2001) noted that in the field of IS research, knowledge can be separated into explicit knowledge and tacit knowledge. They elucidate that explicit knowledge is knowledge that can be taught, while tacit knowledge is knowledge that is gained from experience and is not easily transferrable. An example of tacit knowledge is the knowledge that a surgeon possesses to perform surgical skills (Alavi & Leidner, 2001). Dienes and Perner (1999) noted that explicit knowledge is unambiguous and easily measurable. As stated by Nonaka (1991), “explicit knowledge is formal and systematic” (p. 98). Additionally, explicit knowledge can be transferred by various forms of communication and media (Becerra-Fernandez & Sabherwal, 2001).

Nonaka (1994) posited that there are four modes of explicit and tacit knowledge creation: combination, externalization, internalization, and socialization. Combination is the conversion of explicit knowledge to explicit knowledge (Bratianu, 2016; Jou, Lin, & Wu, 2016). An example of knowledge combination is when two individuals collaborate explicit knowledge during a study (Nonaka & Konno, 1998). Externalization is the conversion of tacit knowledge to explicit knowledge (Bratianu, 2016; Nonaka, 1994). An example of knowledge externalization is when an individual is able to express an idea in a form such as words, concepts, visuals, and figurative language (Nonaka & Konno, 1998; Zhao, Ha, & Widdows, 2016). Internalization is the conversion of explicit knowledge into tacit knowledge (Bratianu, 2016; Jou et al., 2016). Essentially, internalization is learning-by-doing, such as learning that snow is cold when it is touched for the first time (Nonaka & Konno, 1998). Socialization is the conversion of tacit knowledge from tacit knowledge (Jou et al., 2016; Zhao et al., 2016). An example of socialization would be a medical residency when an inexperienced medical doctor gains tacit knowledge from on-the-job with other more experienced medical doctors (Nonaka & Konno, 1998).

Numerous studies have been conducted regarding IS user knowledge as well as knowledge gaps in IS user awareness. Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) defined the following OISU cybersecurity knowledge units: email use, incident reporting, information handling, Internet use, mobile computing, password management, social networking site use, and strong passwords. Gross and Rosson (2007) listed the following IS user cybersecurity knowledge units: access control, antivirus software, cybersecurity POCs, cybersecurity responsibilities, cyber threats, cyber vulnerabilities, email encryption, file permissions, phishing, policy compliance, privacy, sensitive information, and social engineering. Dlamini, Eloff, and Eloff (2009) as well as Ives et al. (2004) additionally noted physical security and smart cards using public key infrastructure (PKI) security as cybersecurity knowledge units. Password reuse has also shown to be an OISU cybersecurity knowledge unit (Ives et al., 2004).

Lopez, Oppliger, and Pernul (2004) defined access control as "the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner" (p. 580). For OISUs, access control is the protection of their computer and the information accessible from the computer by external or unauthorized sources. Gross and Rosson (2007) noted that the knowledge regarding access controls that OISUs should possess is: avoid reusing passwords, periodically change passwords, keep passwords secret, lock the computer while away, physically protect computers, understand access control to a computer is an individual responsibility, verify identities by phone if email phishing is suspected, and contact IT [or cybersecurity POCs] if access control has been compromised.

Studies have shown that users had difficulty understanding who owned the responsibility of updating antivirus software (Arnold, Erner, Möckel, & Schläffer, 2010; Gross & Rosson, 2007). Antivirus software is defined by Karantjias and Polemi (2010) as "a program that attempts to identify, thwart and eliminate computer viruses and other malicious software" (p. 60). Studies have shown that some users may not be aware if antivirus software exists on their computers or how to update it (Arnold et al., 2010; Gross & Rosson, 2007).

Studies have shown that users have issues reporting security incidents to cybersecurity POCs (Gross & Rosson, 2007; Parsons et al., 2014). Cybersecurity POCs are defined as “computer security incident response teams (CSIRT), system and network administrators, security staff, technical support staff, chief information officers (CIO), computer security program managers, and others who are responsible for preparing for, or responding to, security incidents” (Cichonski, Millar, Grance, & Scarfone, 2012, p .1). Furthermore, it appears that some users do not feel responsible to contact cybersecurity POCs for issues (Gross & Rosson, 2007).

OISUs need to have knowledge regarding their cybersecurity responsibilities (Gross & Rosson, 2007). OISU cybersecurity responsibilities include protecting sensitive information, protecting information systems, protecting personally identifiable information (PII), providing physical security, reporting security incidents, and potentially updating software (Cichonski et al., 2012; Gross & Rosson, 2007; Karantjias & Polemi, 2010). OISUs cybersecurity responsibilities may lead to a breach that affects the whole organization (Gross & Rosson, 2007). Gross and Rosson (2007) noted that users expressed the perception that they had no responsibilities in regards to cybersecurity citing reasons such as “it’s not my job” and “I don’t know” (p. 9).

OISUs require knowledge regarding cyber threats (Barlow et al., 2013; Bulgurcu, B., Cavusoglu, & Benbasat, 2010). Cyber threats can be defined as any sources or circumstances that have the potential to compromise the confidentiality, integrity, and availability of an information system (Jung, Han, & Suh, 1999; Mejias & Balthazard, 2014). Specific threats applicable to OSIUs are: hackers, insider attacks, malware, phishing, social engineering, spyware, and viruses (Barlow et al., 2013; Gross & Rosson, 2007; Mbanaso & Dandaura, 2015; Nagarajan, Allbeck, Sood, & Janssen, 2012). While users do display knowledge of threat names or classes, there appears to be a lack of knowledge regarding the damage that the threat may inflict (Gross & Rosson, 2007; Bulgurcu et al., 2010).

Knowledge of cyber vulnerabilities is critical for OISUs (Barlow et al., 2013; Behrens et al., 2012). Cyber vulnerabilities are defined as “weaknesses or flaws, in terms of security and privacy” (Kalloniatis, Mouratidis, & Islam, 2013, p. 4). OISUs require knowledge of the following cyber vulnerabilities: antivirus that has not been updated, email that does not filter spam, information posted to social networking sites, misconfigured or disabled firewalls, misconfigured or disabled antivirus, not installing software patches/updates, not using antivirus software, password sharing, personnel lacking cybersecurity competency, physical security failures, reused passwords on multiple accounts, reused passwords on the same account, unencrypted email, using default passwords, and weak passwords (Barlow et al., 2013; Behrens et al., 2012; Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Bulgurcu et al., 2010; Dlamini et al., 2009; Gross & Rosson, 2007; Ives et al., 2004; Nagarajan et al., 2012; Newsome & Jarmon, 2016; Parsons et al., 2014; Toth & Klein, 2013; Weeden et al., 2013).

Gross and Rosson (2007) contend that users lack of knowledge of email encryption. Email encryption is defined as “the process by which [email] is encoded so that only an authorized recipient can decode and consume the [email]” (Microsoft, 2016a). Specifically, it has been shown that users have knowledge and skill deficiencies in determining when an email needs to be encrypted (Puhakainen & Siponen, 2010).

Parsons et al. (2014) noted email use as a knowledge topic for OISUs. OISUs require the knowledge to avoid dangerous cybersecurity email behaviors such as: downloading of malicious codes and viruses, forwarding of unnecessary emails such as jokes and chain mail, personal use, and sending sensitive information without encryption (DISA, 2015). OISUs also require the knowledge not to use organizational email to create and send SPAM (Parsons et al., 2014).

OISUs need to possess knowledge regarding using file permissions (Gross & Rosson, 2007; Dye & Scarfone, 2014). File permissions are used to “grant or deny access to the files and folders” (Microsoft, 2016b). Properly implementing file permissions may enhance security by limiting which users or groups are able to read sensitive information (Dye & Scarfone, 2014; Zhauniarovich, Russello, Conti, Crispo, & Fernandes, 2014). However, file permissions are not totally secure, an administrator or root user can override restrictive file permissions (Dye & Scarfone, 2014; Parkinson, Somaraki, & Ward, 2016).

OISUs require the knowledge of cybersecurity incident reporting (Imgraben, Engelbrecht, & Choo, 2014; Parsons et al., 2014). Incident reporting is the act of reporting threats to IS security such as suspicious individuals, worker misconduct, and all security incidents (Imgraben, Engelbrecht, & Choo, 2014; Parsons et al., 2014). Incident reporting is critical to ensure unauthorized personnel do not gain access to sensitive information (Ab Rahman & Choo, 2015; Parsons et al., 2014). In regards to system security, it has been shown that organizations have displayed issues regarding incident reporting to protect the reputation of the company (Lagazio, Sherif, & Cushman, 2014; Parsons et al. 2014). Similarly, while not found in literature, it is assumed that employees may resist reporting cybersecurity incidents if they feel the incident may result in job loss for themselves or friends.

It has been shown that OIUSs require knowledge of information handling (Arpaci, Kilicer, & Bardakci, 2015; Parsons et al., 2014). Information handling is the access, creation, destruction, disposition, distribution, maintenance, receipt, storage, transmittal, and use of information (Bernard, 2007). Specific examples of OISU information handling issues due to lack of knowledge include: not properly destroying removable media (CDs, DVDs, etc.) that contain sensitive information, losing removable media that contains sensitive information, the writing and dissemination of malicious code, posting sensitive information to public domains, and inserting USB devices (such as thumb drives) that may contain malicious code (Arpaci et al., 2015; Parsons et al., 2014). USB devices are also under consideration as removable media in cybersecurity (DISA, 2015).

OISU knowledge regarding information privacy continues to be a problem (Bulgurcu et al., 2010; Gross & Rosson, 2007). Information privacy is defined as “the claim of individuals, groups, or institutions to determine when, and to what extent, information about them is communicated to others” (Lallmahamood, 2007, p. 7). Studies have shown that information privacy knowledge by OISUs appears to be neither comprehensive nor sufficient (Gross & Rosson, 2007). Specifically, OISUs need to have knowledge of the legal aspects of information privacy laws and identifying sensitive information for protection (DISA, 2015; Gross & Rosson, 2007).

OISUs require knowledge regarding the Internet use (DISA, 2015; Parsons et al., 2014). OISUs should possess the knowledge to avoid browsing the Internet for personal use, for ethical as well as security reasons (Parsons et al. 2014; Shepherd & Mejias, 2016). Additionally, OISUs should possess the knowledge to avoid downloading unapproved software, using peer-to-peer (P2P) software, and visiting suspicious Websites (DISA, 2015; Parsons et al. 2014).

While not all OISUs have an immediate need to possess mobile computing knowledge, those that do must be knowledgeable regarding sending sensitive information and checking work email while connected to mobile networks (DISA, 2015; Levy & Ramim, 2016; Parsons et al., 2014). Johansson and Andersson (2015) defined mobile computing as “using portable computers capable of wireless networking” (p. 1). Mobile computing is applicable to OISU knowledge because employees travel with laptops for company business and also work from home (Ahn, Lee, & Kim, 2016; DISA, 2015). Moreover, wireless capabilities of mobile computing devices can lead to cyber criminal stealing PII when unencrypted information is transmitted (Levy & Ramim, 2016).

OISU knowledge regarding the security ramifications of password reuse is a serious problem (Gross & Rosson, 2007; Ives et al., 2004). Password reuse is using the same password for multiple accounts or using the same password repeatedly for the same account (DISA, 2015; Ives et al., 2004). As noted by Ives et al. (2004), when password reuse occurs by using the same password on multiple accounts, the password is only as strong as the weakest system in which it is used.

It is critical that OISUs have knowledge regarding phishing, as phishing continues to be a major issue (Bowen, Devarajan, & Stolfo, 2012; Verma, et al., 2015). Phishing is defined as “a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion” (Jakobsson & Myers, 2007, p. 1). Phishing attacks via email are one of the single most effective vectors for infiltrating a secure system (Bowen et al., 2012; Verma et al., 2015).

OISUs must have knowledge of physical security (DISA, 2015; Newsome & Jarmon, 2016). Physical security is defined as the “physical measures taken to safeguard personnel, to protect unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft” (Newsome & Jarmon, 2016, p. 322). Physical security is a critical practice that is a basic principal to all computer systems (Dlaminia et al., 2009; Gross & Rosson, 2007). While physical security policies vary between organizations, OISUs should possess the knowledge to report suspicious activity within the workplace (DISA, 2015; Newsome & Jarmon, 2016).

It is critical that OISUs possess knowledge of policy compliance (Mohammed, Mariani, & Mohammed, 2015; Safa, Von Solms, & Furnell, 2016). Policy compliance is the adherence to a policy, where a policy is defined as “a course or principle of action adopted or proposed by a government, party, business, or individual” (Oxford, 2016, p.1). The perception exists that OISUs, in general, know very little about policies and that these policies need to be reasonable in order for trust to be established (Gross & Rosson, 2007; Safa et al., 2016). An Information Security Policy (ISP) is a common policy where OISU knowledge is critical (Safa et.al, 2016). An Email Acceptable Use Policies (EAUP) is another common policy where OISU knowledge is needed (Parsons et al., 2014). An EAUP is defined as a policy that “sets out your employees' responsibilities when using email in their day-to-day working activities” (NIBusinessInfo, 2016, p. 1). An Internet Acceptable Use Policy (IAUP) is another common policy where OISU knowledge is critical (Lichtenstein & Swatman, 1997). IAUPs are implemented as “guidelines for employees indicating both acceptable and unacceptable Internet usages, with the intention of controlling employee behaviours and actions which contribute to the incidence and severity of the [organization’s] Internet risks” (Lichtenstein & Swatman, 1997, p. 1). These policies vary from organization-to-organization. Therefore, assessing knowledge on specific IAUPs, ISPs, and EAUPs is not possible. However, having OISUs possess the knowledge to follow cybersecurity policy parameters as well as ascertain the ramifications of policy compliance violations is extremely important to minimizing cybersecurity risks (Mohammed et al., 2015; Safa et al. 2016).

Knowledge of protecting sensitive information and PII is critical for OISUs to adhere to security polices and procedures (Gross & Rosson, 2007; Parsons et al., 2014). Ajigini, Van der Poll, and Kroeze (2012) defined sensitive information as:

> Protected information that the owner does not want to reveal to others and not to be divulged outside the [organization] as well as Information about an individual’s racial or ethnic origin, criminal record, sexual preferences or practices and other information that include political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, or a trade union (p. 7).

PII can be considered as a subset of sensitive information, but is often treated independently (DISA, 2015). McCallister, Grance, and Scarfone (2010) defined PII as:

> Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (p. 7)

Social engineering is a concern that is very common amongst OISUs (Gross & Rosson, 2007; Nagarajan et al., 2012). Social engineering is defined as "the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks" (Abraham & Chengalur-Smith, 2010, p. 183). Studies have shown that OISUs have displayed a lack of familiarity with 'social engineering', but did possess knowledge about certain forms of social engineering such as phishing (Bowen et al., 2012; Gross & Rosson, 2007). OISUs should posses the knowledge to avoid social engineering attempts such as taking telephone surveys, also known as vishing (DISA, 2015; Gross & Rosson, 2007). OISUs should also have the knowledge to avoid giving away information regarding their computer, network information, and sensitive personal information (Bowen et al., 2012; DISA, 2015).

Social networking usage is an area where OISUs are prone to errors, such as posting PII, that lead to cybersecurity incidents (DISA, 2015; Parsons et al., 2014). Social networking is defined as "Web-based services allowing individuals to: (a) construct a profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and interact with their list of connections and those made by others within that system" (Weeden, Cooke, & McVey, 2013, p. 250). Facebook$^{©}$, Twitter$^{©}$, and Instagram$^{©}$ are examples of social networking Websites. OISUs appear to post PII and sensitive information to social networks accidentally, as well as intentionally (DISA, 2015; Parsons et al., 2014). OISUs at times have appeared to post PII and sensitive information to social networks due in part to a knowledge deficit where OISUs believe they cannot be fired for something they have posted on a social networking site (Parsons et al., 2014).

It is necessary for OISUs to have knowledge of smart cards, even if they are not actively using smart cards, so they will be better prepared to use smart cards if/when needed (Ardiley, 2012; DISA, 2015; Ives et al., 2004). Smart cards are defined as "credit card-shaped devices incorporating an integrated circuit chip (memory, microprocessor, application-specific, etc.), although they can also take the form of tokens, keys, and non-credit card-shaped card-type devices" (Hester & Joseph, 1998, p. 54). Smart cards employ a Public Key Infrastructure (PKI) to provide authentication to one or many services using public key cryptography (Ardiley, 2012; Ives et al., 2004). Congress mandated that the DoD implement smart card technology for all military and civilian personnel (Ardiley, 2012; DISA, 2015). The smart cards used by the DoD are referred to as common access cards (CACs) that are capable of performing authentication using a fingerprint, personal identification number (PIN), or a photograph that is printed on the card (Ardiley, 2012). Therefore, OISUs should possess the knowledge about physically securing a smart card and the PIN associated with the card, as a lost smart card may be used for malicious purposes (Ardiley, 2012; DISA, 2015; Ives et al., 2004).

The knowledge to use strong passwords is critical for OISUs (Cox, 2012; Parsons et al., 2014). A strong password can be defined as a password "having more than eight characters, at least one change of case, a number that is not at the end, and a non-alphanumeric character such as # or * that is also not at the end of the password" (Keller, Powell, Horstmann, Predmore, & Crawford, 2005, p. 13). When OISUs do not choose strong passwords it increases the probability of an information security breech (Cox, 2012;). While it has been noted that the decision to not choose a strong password is a behavior (Parsons et al., 2014), the assumption is made that this behavior occurs due to a lack of knowledge as well as a lack of technical controls forcing the OISU to create a strong password.

OISUs require the knowledge to securely use Webmail (Ahmad & Bamnote, 2013; Broucek & Turner, 2005; Symantec, 2016). Webmail is defined as "web application that allows users to read and write e-mail on the Internet through a web interface" (Ioannou & Hannafin, 2008, p. 47). OISUs need to have the knowledge that using Webmail to send sensitive information and PII without encryption can lead to a security compromise (Ahmad & Bamnote, 2013). OISUs also need to have the knowledge to use strong passwords and to regularly change passwords (Symantec, 2016). OISUs additionally need to have the knowledge to avoid password reuse on Webmail accounts (Broucek & Turner, 2005). It is critical that OISUs possess the knowledge that public computers are not secure systems and should not be trusted for Webmail use (Symantec, 2016). Specially, public computers may contain key loggers that may be used to steal Webmail login usernames and passwords (Symantec, 2016). A summary of all OISU cybersecurity knowledge requirements are listed in Table 2.

Table 2

Summary of OISU Cybersecurity Knowledge Literature

OISU Knowledge	Source
Access control	Gross & Rosson, 2007; Ifinedo, 2012
Antivirus software	Arnold et al., 2010; Gross & Rosson, 2007;
Cyber threats	Gross & Rosson, 2007; Bulgurcu et al., 2010
Cyber vulnerabilities	Gross & Rosson, 2007; Bulgurcu et al., 2010
Cybersecurity POCs	Gross & Rosson, 2007; Parsons et al., 2014
Cybersecurity responsibilities	Gross & Rosson, 2007
Email encryption	Gross & Rosson, 2007; Puhakainen & Siponen, 2010
Email use	Parsons et al., 2014; Barlow et al., 2013
File permissions	Gross & Rosson, 2007; Dye & Scarfone, 2014
Incident reporting	Imgraben et al., 2014; Parsons et al., 2014
Information handling	Arpaci et al., 2015; Parsons et al., 2014
Information privacy	Bulgurcu et al., 2010; Gross & Rosson, 2007
Internet usage	DISA, 2015; Parsons et al., 2014
Mobile computing	DISA, 2015; Levy & Ramim, 2016; Parsons et al., 2014
Password reuse	Ives et al., 2004; Gross & Rosson, 2007
Phishing	Bowen et al., 2012; Verma et al., 2015
Physical security	DISA, 2015; Newsome & Jarmon, 2016
Policy compliance	Mohammed et al., 2015; Safa et al. 2016
Sensitive information	Gross & Rosson, 2007; Parsons et al. 2014
Social engineering	Cox, 2012; Gross & Rosson, 2007
Social networking	DISA, 2015; Parsons et al., 2014
Smart cards	Ardiley, 2012; DISA, 2015; Ives et al., 2004
Strong password	Cox, 2012; Parsons et al., 2014
Webmail	Ahmad & Bamnote, 2013; Broucek & Turner, 2005; Symantec, 2016

Cybersecurity Skills

Skill has been defined by this research as a goal-directed, well-organized set of actions that is acquired through practice and performed with economy of effort, which enables a person to do something well (Boyatzis & Kolb, 1995). Cybersecurity skills are defined as "the skills one possess to prevent damage to IT via the Internet" (Carlton & Levy, 2016, p. 1). In regards to cybersecurity, defining a universal skill set is challenging as cybersecurity encompasses a massive and rapidly changing collection of capabilities (Dodge, Toregas, & Hoffman, 2012). Therefore, cybersecurity skills correlate to specific sets of actions or tasks required (Conklin et al, 2014; Dodge et al., 2012). When cybersecurity skills belong to a engineering or scientific cyber position, the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework noted that formal training is required (Nagarajan et al., 2012; Carlton & Levy, 2015). However, regardless of career field and cybersecurity expertise, all federal employees are required to complete annual cybersecurity awareness training to gain/maintain access to government networks (DISA, 2015; Nagarajan et al., 2012; NIST, 2014). The intent of such cybersecurity awareness programs is to increase skill levels thru practice and close the cybersecurity skills gap that is created due to lack of experience and skill (Mbanaso & Dandaura, 2015; Nagarajan et al., 2012). Therefore, an assessment of skills both demonstrated and practiced in cybersecurity awareness literature appears to be lacking, but significantly critical and needed to gather the necessary skills needed to determine cybersecurity competency of an OISU.

The DISA Cybersecurity Awareness Challenge is a game type simulation that allows the user to react to ethical and cybersecurity situations from a first person perspective (DISA, 2015). While cybersecurity certification examinations typically only assess knowledge, simulations may be designed to assess skill (Tobey, 2015). Moreover, game type simulations are accurate measures of skill since the application of the skill is observable (Cankaya, 2015; Tobey, 2015). The DoD version of the Cybersecurity Awareness Challenge defined a threshold of 70% of the weighted points needed to pass the challenge (DISA, 2015). The DoD Cybersecurity Awareness Challenge training focuses on the following three topics: situational awareness, securing government furnished equipment (GFE), and telework (DISA, 2015).

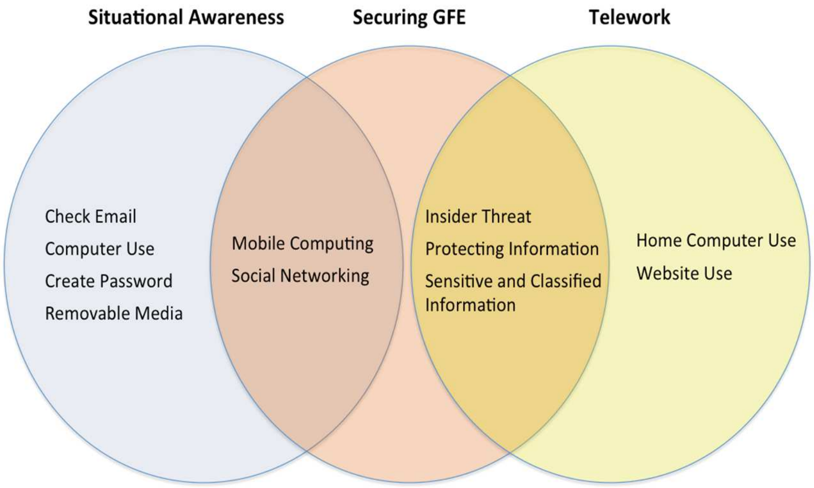


Figure 2. DoD Cybersecurity Awareness Challenge topics and skill categories

Figure 2 represents the training topics with their skill categories that are common to all versions of the Cybersecurity Awareness Challenge. Not all of the skills listed within the skill categories apply to the cybersecurity competency of OISUs. The skills applicable to OISUs are listed in Table 3.

Table 3

Summary of OISU Cybersecurity Skills Approved by DISA

Computer Use
Peer-to-peer software usage
Cookie usage
Internet usage
Malicious code avoidance

Table 3

Summary of OISU Cybersecurity Skills Approved by DISA (continued)

Create Password
Strong password usage
Check Email
Email security
Phishing avoidance
Spear-phishing avoidance
Whaling avoidance
Insider Threat
Physical security
Removable Media
Removable media usage
Removable media protection
Protecting Information
Protecting sensitive information
Sensitive information identification
Spillage avoidance
Strong password usage
Social Networking
Social engineering avoidance

To ensure access control is maintained within an organization, OISUs must possess skill in preventing unauthorized access to an IS by controlling access to systems (Gross & Rosson, 2007; Ifinedo, 2012). Proper access control will reduce the probability that an external or unauthorized entity will gain access to sensitive information or PII (DISA, 2015; Gross & Rosson, 2007). OISUs must be able to perform several tasks to prevent unauthorized access to an IS by controlling access to systems (Gross & Rosson, 2007; Ifinedo, 2012). OISUs must be able to demonstrate the following tasks: avoid password reuse, use strong passwords, keep passwords confidential, lock (disable) the computer while away, physically protect computer, and contact IT [or cybersecurity POCs] if access control has been compromised (Gross & Rosson, 2007).

Skill regarding antivirus software is necessary to maximize the protection provided by antivirus software (Dhepe & Akarte, 2013; Gross & Rosson, 2007; Ifinedo, 2012). While many organizations have the ability to automatically update antivirus software for users (or configure systems to auto-update), there may be times where an OISU is needed to facilitate the update (Dhepe & Akarte, 2013). OISUs must have skill in using an antivirus application to properly update the software when notified that antivirus requires an update (Gross & Rosson, 2007). Therefore, OISUs need to be able to demonstrate the task of updating antivirus software when notified that an antivirus software update is available (Dhepe & Akarte, 2013; Gross & Rosson, 2007).

Skills regarding cookie usage are necessary because cookies may contain unencrypted sensitive information or PII and may be used to track activity (DISA, 2015). Therefore, OISUs must have skill in managing cookie settings and usage (DISA, 2015; Park & Sandhu, 2000). OISUs must be able to demonstrate the task of adjusting their Internet browser setting to prompt each time a site wants to store a cookie (DISA, 2015; Park & Sandhu, 2000). Furthermore, OISUs need to be able to demonstrate the task of only accepting cookies from reputable sites (DISA, 2015; Park & Sandhu, 2000). OISUs also need to demonstrate the task of cookie use only while the Internet browser is using an encrypted link (DISA, 2015). An encrypted link can be confirmed when ‘https’ is in the Web address and the encryption icon is working (DISA, 2015).

It is critical that OISUs have skill specific to email security (DISA, 2015; Parsons et al., 2014). The main objective of email security is to protect sensitive information and

PII, as well as to prevent the propagation of malicious code (Carlton, Levy, Ramim, & Terrell, 2015; DISA, 2015; Wang, Li, & Cheng, 2014). Therefore, OISUs must have skill in configuring and using Email in a manner that prevents sensitive information and PII loss (DISA, 2015; Parsons et al., 2014). Thus, OISUs must be able to demonstrate the task of preventing the downloading of malicious code or viruses, as well as the task of sending sensitive information or PII with encryption (Barlow et al., 2013; DISA, 2015). Additionally, OISUs must demonstrate the task of avoiding using email for personal use (DISA, 2015). An OISU must also demonstrate the task of configuring email programs to only view email messages in plain text, as well disabling the preview pane (DISA, 2015). Additionally, OISUs must be able to demonstrate the task of digitally signing emails to provide added security (DISA, 2015; Foster, Larson, Masich, Snoeren, Savage, & Levchenko, 2015). OISUs must also demonstrate the task of scanning all email attachments before use (DISA, 2015; Tan, Chua, & Chang, 2014).

OISUs must have skill in cybersecurity incident reporting to ensure unauthorized personnel do not gain access to sensitive information or PII (Imgraben et al., 2014; Parsons et al., 2014). OISUs need to be able to identify suspicious individuals that may be attempting to compromise security, as well as recognize personal mistakes that need to be reported (Parsons et al., 2014). A specific threat that may require skill with incident reporting is worker misconduct (Parsons et al., 2014). An OISU must be able to demonstrate the task of reporting all incidents that may be perceived as a possible security incident, such as coworker conduct/misconduct that is in violation of company cybersecurity policies (Parsons et al., 2014).

It is critical that OISUs possess skill in avoiding suspicious or malicious Websites when using the Internet at work (Carlton et al., 2015; DISA, 2015; Parsons et al., 2014). An OISU must be able to demonstrate the task of being able to avoid clicking on malicious pop-up windows (DISA, 2015; Kumar, Chaudhary, & Kumar, 2015). An example of a malicious popup window is one that warns "your computer is infected, click here to remove viruses", as this is possibly a malicious code attack (DISA, 2015; Kumar et al., 2015). OISUs also need to be able to demonstrate the task of avoiding dubious and pornographic Websites (DISA, 2015; Parsons et al., 2014). Additionally, it is crucial that OISUs demonstrate the task of being able to refrain from making credit card transactions on non-secured Websites (Carlton et al., 2015).

It is vital that OISUs have skill in avoiding actions that increase exposure to malicious code downloading or execution (Barlow et al., 2013; DISA, 2015). Malicious code is capable of giving hackers access to a network or system, erase hard drives, and corrupt files (DISA, 2015). Examples of malicious code are viruses, worms, Trojan horses, spyware, and scripts (DISA, 2015). Malicious code can be spread as email attachments, downloaded files, or even just by visiting a Webpage (DISA, 2015). OISUs must be able to demonstrate the task of avoiding clicking hyperlinks within emails (DISA, 2015). Additionally, OISUs must be able to demonstrate the task of configuring their Internet browser to disable automatic downloading. OISUs must also be able to demonstrate the task scanning all external files before transferring to their computer (DISA, 2015). OISUs must additionally demonstrate the task of avoiding the forwarding of infected files (DISA, 2015). OISUs should ideally be able to demonstrate the task of executing legitimate ActiveX controls and avoiding suspicious ActiveX controls (DISA, 2015). However, ActiveX controls are operating system specific and do not need to be considered for OISU cybersecurity competency assessment.

While all OISUs might not travel for work purposes, or telework, skill in securely operating mobile computing devices may prove valuable in case the need arises (DISA, 2015). OISUs must demonstrate the task of locking their mobile computing device when not in use (DISA, 2015; Parsons et al., 2014). OISUs must also demonstrate the task of disabling wireless capabilities when the device is using a LAN (Botha, Furnell, & Clarke, 2009; DISA, 2015). OISUs must additionally demonstrate the task of disabling wireless capabilities when the mobile device is not in use (Botha et al., 2009; DISA, 2015). Moreover, OISUs must also demonstrate the task of encrypting sensitive information or PII when using a mobile device such as a laptop (DISA, 2015; Parsons et al., 2014).

The avoidance of password reuse is a skill needed by OISUs (DISA, 2015; Ives et al., 2004). OISUs must possess skill in creating using unique passwords for all user accounts and logins (Gross & Rosson, 2007; DISA, 2015). DISA (2015) noted that it is critical that the same password is not used between personal and professional accounts. Thus, it is critical that OISUs demonstrate the task of creating unique passwords on multiple user accounts or logins (Gross & Rosson, 2007; DISA, 2015).

Peer-to-peer is defined as “technology that enables two or more peers to collaborate spontaneously in a network of equals (peers) by using appropriate information and communication systems without the necessity for central coordination” (Schoder & Fischbach, 2003, p. 27). Thus, peer-to-peer software enables small and large groups of computers to connect directly with each other for file sharing. While peer-to-peer software at times can be a security liability because it may allow unauthorized access to data or copyrighted files, peer-to-peer software is still necessary to perform specific job functions for some occupations (Bishop, 2003; DISA, 2015). Thus, OISUs require skill in peer-to-peer software usage without exploitation by transferring copyrighted materials, sensitive information, or PII. Therefore, OISUs must demonstrate the task of not using peer-to-peer software to illegally transfer copyrighted materials, sensitive information, or PII (Bishop, 2003; DISA, 2015).

OISUs require skill in avoiding phishing attempts of sensitive information and PII (Carlton et al., 2015; DISA, 2015; Furnell, Tsaganidi, & Phippen, 2008). OISUs must demonstrate the task of not divulging sensitive information or PII to a phishing attempt (DISA, 2015; Furnell et al., 2008). If an email appears to be a phishing attempt, but may be legitimate, the OISU must demonstrate the task of verifying the identity of an email sender to prevent the divulging of sensitive information or PII to a phishing attempt (DISA, 2015).

A targeted form of phishing is called spear-phishing (Botha et al., 2009). Spear-phishing is defined as “a type of phishing attack that targets particular individuals, groups of people, or organizations” (DISA, 2015). OISUs require skill in avoiding spear-phishing attempts of sensitive information and PII (Botha et al., 2009; DISA, 2015; Luo, Zhang, Burd, & Seazzu, 2013). An OISU must demonstrate the task of not divulging sensitive information or PII to a spear-phishing attack that mimics someone from within their organization or related organization (DISA, 2015; Luo et al., 2013). Additionally, OISUs must demonstrate the task of not divulging sensitive information or PII to a spear-phishing attack that states their name (DISA, 2015; Luo, Zhang, Burd, & Seazzu, 2013)

Whaling is a form of spear-phishing that targets high-level personnel (DISA, 2015; Furnell et al., 2008; Hong, 2012). Whaling attacks typically resemble a legitimate message and attempt to exploit relevant issues or topics (DISA, 2015; Nagarjuna, & Sujatha, 2013). OISUs must have skill in avoiding whaling attempts of sensitive information and PII (DISA, 2015; Hong, 2012). OISUs must demonstrate the task of not divulging sensitive information or PII to a whaling attempt (DISA, 2015; Furnell et al., 2008; Hong, 2012).

Physical security is a primary cybersecurity concern for OISUs and organizations (Dlaminia et al., 2009). Many organizations carry policies regarding gaining entry to secure/sensitive locations or systems (DISA, 2015; Gross & Rosson, 2007; Hinduja & Kooi, 2013). OISUs require skill in physically protecting an IS from an unauthorized user (DISA, 2015; Dlaminia et al., 2009; Hinduja & Kooi, 2013). At a minimum, OISUs must demonstrate the task of reporting an unauthorized person on an IS to IT or cybersecurity POCs (DISA, 2015; Dlaminia et al., 2009; Hinduja & Kooi, 2013).

It is critical that OISUs have skill in using authorized systems for sensitive information and PII data processing as well as transmissions (Carlton et al., 2015; DISA, 2015; Knapp & Ferrante, 2012). OISUs must demonstrate the task of not using an unauthorized system when dealing with sensitive information and PII (DISA, 2015; Posthumus & Von Solms, 2004). This includes not transmitting, processing, or storing sensitive information and PII on non-sensitive systems (DISA, 2015; Posthumus & Von Solms, 2004). OISUs must also demonstrate the task of not using non-secured text message to transmit sensitive information or PII (DISA, 2015; Puhakainen & Siponen, 2010).

OISUs require skill in labeling removable media that contains sensitive information or PII (Da Veiga & Eloff, 2010; DISA, 2015). Thus, OISUs must demonstrate the task of labeling any removable media that contains sensitive information or PII (DISA, 2015; Gaurav, Kumar, Venkatesan, & Babu, 2015). Labeling is necessary to identify which organizational policies need to be followed when sanitizing, storing, purging, discarding, and destroying removable media that may contain sensitive information as well as PII (DISA, 2015; Gaurav et al., 2015; Medlin & Cazier, 2011).

OISUs need to have skill in using encryption to store data on approved removable media (Da Veiga & Eloff, 2010; DISA, 2015). Many organizations have very strict policies restricting or prohibiting the use of certain forms of removable media (DISA, 2015; Sugii & Nojiri, 2015). Such restrictions exist due to thumb drives, CD's, etc. that contain hidden malicious software such as viruses (Arpaci et al., 2015; DISA, 2015; Parsons et al., 2014). Therefore, OISUs must demonstrate the task of using approved/appropriate removable media (DISA, 2015; Sugii & Nojiri, 2015). For approved forms of removable media, OISUs must demonstrate the task of encrypting data sensitive information and PII when using removable media (DISA, 2015).

It is crucial that OISUs have skill in identifying sensitive information and PII (DISA, 2015; Puhakainen & Siponen, 2010). OISUs need the skill to identify sensitive information and PII such as: financial information, private health information, payroll or personal information, or protected business intellectual properties (DISA, 2015). Having the skill of sensitive information and PII identification is critical for many reasons, such as knowing when to encrypt emails or when printed documents need to be shredded (DISA, 2015; Puhakainen & Siponen, 2010). Therefore, OISUs must demonstrate the task of identifying an address and phone number as PII (DISA, 2015; Puhakainen & Siponen, 2010). OISUs must also demonstrate the task of identifying proprietary information as sensitive information (DISA, 2015; Puhakainen & Siponen, 2010). Additionally, sensitive information and PII identification is beneficial when reviewing documents for spillage (Deshpande, Joshi, Dewan, Murthy, Mohania, & Agrawal, 2015; DISA, 2015).

Spillage occurs “when information is spilled from a higher classification or protection level to a lower classification or protection level” (DISA, 2015). An example of spillage would be writing a memo for publication that accidentally contains sensitive information or PII of customers. OISUs require skill in identifying the spillage of sensitive information and PII (Deshpande et al., 2015; DISA, 2015; Sugii, & Nojiri 2015). Thus, OISUs must demonstrate the task of reporting a spillage incident (Deshpande et al., 2015; DISA, 2015; Sugii & Nojiri, 2015).

OISUs require skill in avoiding social engineering attempts of sensitive information and PII (DISA, 2015; Gross & Rosson, 2007). OISUs must demonstrate the task of identifying and avoiding social engineering attempts by text messages (DISA, 2015; Gross & Rosson, 2007). OISUs are also required to demonstrate the task of identifying and avoiding social engineering by vishing surveys (DISA, 2015; Gross & Rosson, 2007). Additionally, OISUs must demonstrate the task of identifying and avoiding social engineering by public conversations (DISA, 2015; Gross & Rosson, 2007).

DISA proposed that social networking at home is relevant to OISUs work responsibilities (DISA, 2015). This is supported by Parsons et al. (2014) when they noted that OISUs did not realize their employment could be terminated due negative interactions with social media. OISUs must have skill in using social networking without divulging sensitive information and PII (Carlton et al., 2015; DISA, 2015; Parsons et al., 2014). Therefore, OISUs must demonstrate the task of using a social network without divulging PII (DISA, 2015; Parsons et al., 2014). Additionally, OISUs must demonstrate the task of using a social network without divulging sensitive information or PII. Furthermore, OISUs need to use strong passwords for social networking sites (DISA, 2015; Lorentzen, Fiedler, & Johnson, 2013). While not found in literature, the assumption can be made that the avoidance of password reuse applies to social networking as well.

It is critical that OISUs have skill in creating strong passwords (Da Veiga & Eloff, 2010; DISA, 2015; Mujeye & Levy, 2013). DISA (2015) noted that the skill of using strong passwords involves memorizing the passwords. OISUs should also have to skill to choose letter combinations that do not form common words or phrases (DISA, 2015; Mujeye & Levy, 2013). Thus, OISUs are required to demonstrate the task of creating strong passwords for user accounts or logins (Da Veiga & Eloff, 2010; DISA, 2015).

OISUs need skill in using encryption to transmit sensitive information and PII when using Webmail (Ahmad & Bamnote, 2013; Broucek & Turner, 2005; Symantec, 2016). OISUs must demonstrate the task to use encryption when sending sensitive information or PII with Webmail (Ahmad & Bamnote, 2013; Broucek & Turner, 2005; Symantec, 2016). Additionally, OISUs need to have the skill to use strong passwords as well as regularly changing passwords for Webmail accounts (Symantec, 2016).

Furthermore, OISUs need to have the skill to use unique passwords for their Webmail accounts to avoid password reuse (Broucek & Turner, 2005).

As shown in this section of the review of the literature, there are numerous cybersecurity skills required by OISUs. A lack of skill with any of the OISU cybersecurity skills shown in this section can cause catastrophic losses for an organization. The skills presented in this section, as well as the knowledge and abilities in previous sections, were required to be measured to determine cybersecurity competency of OISUs. At this time, a review of the literature did not reveal a method for measuring the cybersecurity competency of OISUs. A summary of all OISU cybersecurity skills are listed in Table 4.

Table 4

Summary of OISU Cybersecurity Skill Literature

OISU Skills	**Source(s)**
Skill in preventing unauthorized access to an IS by controlling access to systems	Gross & Rosson, 2007; Ifinedo, 2012
Skill in using an antivirus application to properly update the software when notified that antivirus requires an update	Dhepe & Akarte, 2013; Gross & Rosson, 2007; Ifinedo, 2012
Skill in managing cookie settings and usage	DISA, 2015; Park & Sandhu, 2000
Skill in configuring and using Email in a manner that prevents sensitive information and PII loss	DISA, 2015; Gross & Rosson, 2007
Skill in cybersecurity incident reporting	Imgraben et al., 2014; Parsons et al., 2014
Skill in avoiding suspicious and malicious Websites when using the Internet at work	Carlton et al., 2015; DISA, 2015; Parsons et al., 2014
Skill in securely operating mobile computing devices	Botha et al., 2009; DISA, 2015; Parsons et al., 2014
Skill in avoiding actions that increase exposure to malicious code downloading or execution	Barlow et al., 2013; DISA, 2015

Table 4

Summary of OISU Cybersecurity Skill Literature (continued)

OISU Skills	**Source**
Skill in creating using unique passwords for all user accounts and logins	DISA, 2015; Ives et al., 2004
Skill in peer-to-peer software usage without exploitation by transferring copyrighted materials, sensitive information, or PII	Bishop, 2003; DISA, 2015
Skill in avoiding a phishing attempts of sensitive information and PII	Carlton et al., 2015; DISA, 2015; Furnell et al., 2008
Skill in physically protecting an IS from an unauthorized user	DISA, 2015; Dlaminia et al., 2009; Hinduja & Kooi, 2013
Skill in using authorized systems for sensitive information and PII data processing as well as transmissions	Carlton et al., 2015; DISA, 2015; Knapp & Ferrante, 2012
Skill in labeling removable media that contains sensitive information or PII	Da Veiga & Eloff, 2010; DISA, 2015
Skill in using encryption to store data on approved removable media	Da Veiga & Eloff, 2010; DISA, 2015
Skill in identifying sensitive information and PII	DISA, 2015; Puhakainen & Siponen, 2010
Skill in avoiding social engineering attempts of sensitive information and PII	DISA, 2015; Parsons et al., 2014
Skill in using social networking without divulging sensitive information and PII	Carlton et al., 2015; DISA, 2015; Gross & Rosson, 2007
Skill in avoiding a spear-phishing attempts of sensitive information and PII	Botha et al., 2009; DISA, 2015; Luo et al., 2013
Skill in identifying the spillage of sensitive information and PII	Deshpande et al., 2015; DISA, 2015; Sugii & Nojiri, 2015
Skill in creating strong passwords	Da Veiga & Eloff, 2010; DISA, 2015; Mujeye & Levy, 2013
Skill in using encryption to transmit sensitive information and PII when using Webmail	Ahmad & Bamnote, 2013; Broucek & Turner, 2005; Symantec, 2016
Skill in avoiding a whaling attempts of sensitive information and PII	DISA, 2015; Furnell et al., 2008; Hong, 2012

Summary of What is Known and Unknown in Research Literature

A review of the literature was performed to provide a foundation for this research study of OISU cybersecurity competency assessment. This literature review lead to the discovery of what is known and what is unknown about the cybersecurity competency of OISUs. Literature has shown that any competency can be determined by establishing an assessment where the combined weighted KSA measures scored by an individual must meet or exceed the competency threshold level (Ahmed et al., 2013; Jacob & Chalia, 2015; Korndorffer et al., 2005). In the case of OISU cybersecurity competency, it appears no such assessment method or tool exists. The DISA Cyber Awareness Challenge does partially measure the cybersecurity awareness of OISUs, but it is not a competency assessment tool (DISA, 2015).

The assessment of OISU cybersecurity competency requires the proposal and validation of: OISU cybersecurity KSAs, OISU cybersecurity KSA measures, weights for the OISU cybersecurity KSA measures, and the OISU cybersecurity competency threshold; all of which were unknown before this research study. The initial list of KSAs was compiled using applicable OISU KSAs, found in literature and USG documents, which are shown in Tables 1 - 4. However, this list of KSAs is not valid in and of itself, the initial KSA list needed to be validated. Furthermore, the proposed OISU cybersecurity KSA measures, weights for the OISU cybersecurity KSA measures, and the OISU cybersecurity competency threshold needed to be validated.

Literature has presented various options for proposing and validating research content and measures. Grounded Theory is approach that can be used for proposal and validation studies (Bang et al., 2013). Person-Environment Fit Theory has also been applied to proposal and validation research (Jansen & Kristof-Brown, 2006). Theory of Performance is another method for proposal and validation research (Aryee, Walumbwa, Seidu, & Otaye, 2016). However, it appears the Delphi method is an effective method for using SMEs to propose and validate content and measures (Manley & Zinser, 2012).

Competency assessments may be accomplished using printed documents or using computer software (Fetters et al., 2017; Haywood et al., 2014). However, literature has shown that it is recommended for competency assessments to be accomplished using Web services due to simplified communication and information sharing (Draganidis & Mentzas, 2006). Additionally, competency assessments measurements should be technical or functional KSA measures (Shippmann et al., 2000; Succar et al., 2013). Furthermore, competency assessments should abbreviate the list of KSAs to ensure a usable tool (Gebbie & Merrill, 2002). It is also important that when assessing non-experts, competency assessments should establish a threshold level (Shahidi et al., 2015).

Chapter 3

Methodology

Overview

This study was developmental, in terms of developing the MyCyberKSAs^{TM} cybersecurity competency assessment prototype tool. This research study was conducted with Institutional Review Board (IRB) approval as shown in Appendix M. This study used the Delphi method with an expert panel of cybersecurity SMEs to propose and validate the content that comprised the prototype MyCyberKSAs^{TM} cybersecurity competency assessment prototype tool. The first step of Phase 1 was to conduct interviews with 5 SMEs from government and industry to quality check the initial KSA list, identified from literature as well as USG documents, for accuracy/thoroughness. For Phases 1 thru 4, qualitative and quantitative data collection occurred by using Google® Forms electronic surveys to gather the expertise of at least 15 SMEs per phase. The first Google® Forms survey instrument is shown in Appendix C. When using the Delphi method, each method of each phase builds on the previously administered instrument. The Google® Forms instruments were administered to SMEs from government and industry for each Delphi iteration. This study attempted to use the same SMEs for the duration of data collection. However, due to anonymity, it was not possible to confirm which SMEs participated in each phase. Phase 5 of this study used a sample of 54 OISUs from government and industry to test the prototype MyCyberKSAs^{TM} cybersecurity competency assessment prototype tool.

The main research question that this study addressed is: How can an assessment for cybersecurity competency of OISUs be accomplished using KSAs and at what level of KSAs the cybersecurity competency threshold is established? The theoretical model to address the main research question is shown in the Figure 1. Additionally, the research design of this study is shown in Figure 3.

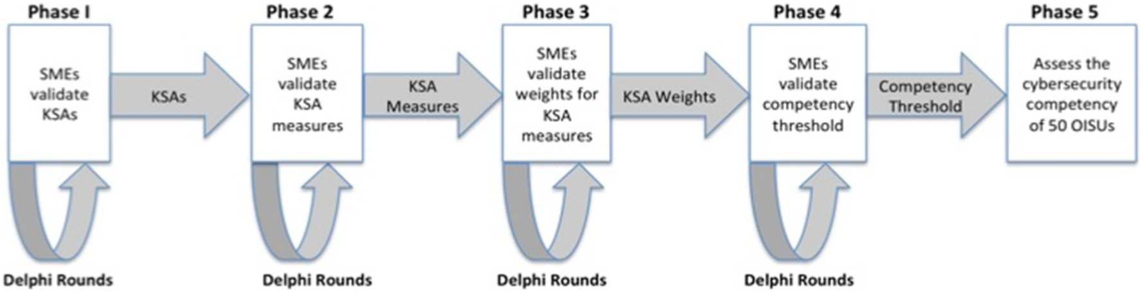


Figure 3. Research design for the development of MyCyberKSAs^{TM} prototype

To meet the specific goals that will address the main research question, this study conducted five phases of research as shown in Figure 3. Phases 1 thru 4 were performed using new instances of the Delphi method, building upon the previous phase. Each phase had the potential to conduct additional rounds of data collection, where each round supplied the data for the next round, until a consensus is achieved. A consensus was achieved when at least 70% of the panelists are in agreement, as recommended by Sumsion (1998). For this study, a 7-point Likert scale was used to collect SME inputs. To accept an item with a SME consensus, 70% of SME responses had to be at least (5) “moderately acceptable.” SMEs were required to provide reasoned arguments (feedback) to add or modify any constructs in Phases 1 thru 4. The Phase 1 thru 4 instruments were designed to also collect qualitative data from the SMEs, to allow the ability to submit feedback on every item on each instrument. The qualitative data from each phase (and round if applicable) was analyzed in conjunction with the quantitative data. In Phase 2, when a SME rated a survey item less than (5) “moderately acceptable”, feedback was required so that item may be reworked based on the SME identified deficiencies. For each phase of this study, once a consensus was achieved on each instrument item, the study initiated the next phase of data collection. Phase 5 of this study required a minimum of 50 participants from government and industry to test the MyCyberKSAs^{TM} prototype assessment tool. When the results for at least 50 participants were recorded, the final phase of data collection was complete and this study proceeded to data analysis.

Delphi Method

The Delphi method is an expert panel methodology that was developed in the 1950s by the RAND Corporation (Dalkey & Helmer, 1963). Skulmoski, Hartman, and Krahn (2007) stated that "the Delphi method is an iterative process to collect and distill the anonymous judgments of experts using a series of data collection and analysis techniques interspersed with feedback" (p. 1). Linstone and Turoff (1975) stated that the Delphi method is characterized as "a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem" (p. 3). This communication process typically occurs in the form of anonymous questionnaires or surveys interspersed with controlled opinion feedback (Skinner, Nelson, Chin, & Land, 2015).

The Delphi method refers to the each iteration of the process as a chronologically numbered 'round' (Worrell, Di Gangi, & Bush, 2013). A study performed using the Delphi method will typically iterate through one to six rounds (Worrell et al., 2013). Each round will use a measurement instrument such as a survey, which often is developed based on the results of the previous surveys (Skulmoski et al., 2007). In the communication process, Dalkey and Helmer (1963) noted that anonymity is a key factor as it eliminates direct confrontation. Moreover, Dalkey and Helmer (1963) argued the need to remove the element of direct confrontation by stating:

> Direct confrontation, on the other hand, all too often induces the hasty formulation of preconceived notions, an inclination to close one's mind to novel ideas, a tendency to defend a stand once taken, or, alternatively and sometimes alternately, a predisposition to be swayed by persuasively stated opinions of others. (p. 2)

Each round iterates until the goal is achieved or a research question has been answered (Worrell et al., 2013). This may occur when consensus is reached, theoretical saturation is achieved, or when sufficient information has been exchanged (Skinner et al., 2015; Skulmoski et al., 2007).

The Delphi method has proven to be highly effective in IS research (Grisham, 2009). Specifically, the Delphi method is beneficial when accurate information is not available and there exists a need for inputs based on human judgment (Ramim & Lichvar, 2014). Furthermore, a wide range of doctoral dissertations using the Delphi method have been conducted in the field of IS (Skulmoski et al., 2007). Okoli and Pawlowski (2004) noted that the Delphi method is effective in IS research due to the four specific ways it relates to theory building. First, the Delphi method assists with the identification of the variables of interest as well as generating propositions (Okoli & Pawlowski, 2004). Second, the Delphi method assists with producing a generalizable theory that will be valid across different domains (Okoli & Pawlowski, 2004). Third, the Delphi method assists with understanding the causal relationships between factors if the experts are required to provide their reasoning within feedback (Okoli & Pawlowski, 2004). Fourth, the expert panel in the Delphi method assists with construct validity (Okoli & Pawlowski, 2004).

The proposal and validation of KSAs using the Delphi method has occurred in numerous studies. Studies have shown that literature reviews have been used to build an initial list of KSAs for the SMEs to evaluate (Kay & Moncarz 2004; Manley & Zinser, 2012; Weber, Crawford, Rivera, & Finley, 2011). The number of SMEs used in studies varies, ranging from 10 to 475 SMEs (Kay & Moncarz 2004; Weber et al., 2011). SME evaluations are facilitated using surveys delivered as: paper documents, electronic documents, and Websites (Brill, Bishop, & Walker, 2006; Manley & Zinser, 2012; Weber et al., 2011). SME data collection using digital surveys may be designed to ensure anonymity, as suggested by the Delphi method process (Dalkey & Helmer, 1963; Higgins, Veech, MacFarlane, Borders, LeRoy, & Callanan, 2012). For SMEs to evaluate each KSA, studies have used Likert scales to validate the importance of each proposed KSA (Kay & Moncarz 2004; Manley & Zinser, 2012; Weber et al., 2011). During the SME evaluation process, SMEs may add additional KSAs that were not presented in the initial KSA list (Weber et al., 2011). A summary of literature in which KSAs are proposed and validated using the Delphi method is shown in Table 5.

Table 5

Summary of KSA Proposal and Validation Literature

Study	**Methodology**	**Sample**	**Instruments or Constructs**	**Main Finding or Contribution**
Brill, Bishop, & Walker, 2006	Empirical study via survey using the Delphi Expert methodology	147	Project manager KSAs	Reported project manager KSAs and demonstrated the effectiveness of a Web-based Delphi technique

Table 5

Summary of KSA Proposal and Validation Literature (continued)

Study	**Methodology**	**Sample**	**Instruments or Constructs**	**Main Finding or Contribution**
Higgins, Veech, MacFarlane, Borders, LeRoy, & Callanan, 2012	Empirical study via survey using the Delphi Expert methodology	74	Genetic councilor KSAs	Data analysis yielded six genetic councilor KSA domains
Manley & Zinzer, 2012	Empirical study via survey using the Delphi Expert methodology	475	CTE teacher KSAs	Level of importance and degree of consensus in the re-validation of existing KSAs
Thompson, Repko, & Staggers, 2003	Empirical study via questionnaire using the Delphi Expert methodology	198	US Air Force surgical nurse KSAs	Assessment of surgical nurse KSAs in a mobility environment

Research Phases

To meet the previously described goals that addressed the main research question, this study conducted five phases of research as shown in Figure 3. Each phase was performed using new instances of the Delphi Method, building upon the previous phase. When a consensus was required by the SMEs, the consensus was achieved when at least 70% of the panelists were in agreement. Once a consensus was achieved, the study proceeded to the next phase.

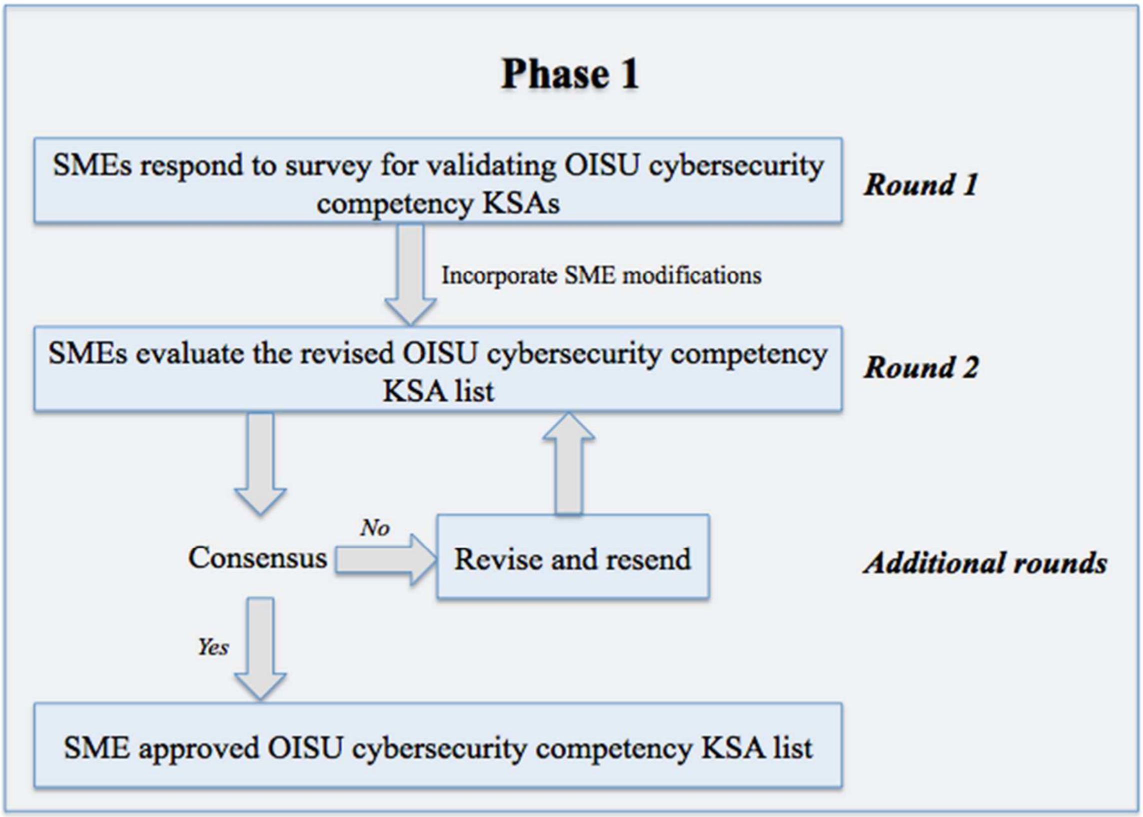

Phase 1
SMEs respond to survey for validating OISU cybersecurity competency KSAs
Round 1
Incorporate SME modifications
SMEs evaluate the revised OISU cybersecurity competency KSA list
Round 2
Consensus
No
Revise and resend
Additional rounds
Yes
SME approved OISU cybersecurity competency KSA list

Figure 4. Phase 1 Research design to propose and validate cybersecurity KSAs for OISUs

Before starting the Phase 1 Survey, this study performed five semi-structured SME interviews for evaluation of the initial list of KSAs as identified from literature review. The intent of performing five semi-structured SME interviews was to collect qualitative data regarding the KSAs found in literature and USG documents. Specifically, the semi-structured SME interviews determined if any KSAs were missed by the literature review, or if any KSAs found in literature were not critical enough to be included in the OISU cybersecurity competency assessment. To suggest the addition(s) of new KSA(s) to the initial list, a SME must have provided reasoned argument(s) as to why the KSA(s) should be added. To suggest the removal of existing KSA(s) from the initial list, the SME needed to provide reasoned argument(s) as to why the KSA(s) should be removed. If qualitative data did not provide compelling evidence (which will be asserted with literature) to remove a KSA, or is not marked for removal by at least 60% of the SMEs, the KSA remained on the initial KSA for evaluation by the 30 SME expert panel in the Phase 1 Survey. The instrument for the semi-structured SME interviews is shown in Appendix A.

The Phase 1 Survey used a Google® Forms survey (Appendix C) consisting of all KSAs found in literature and USG documents that are applicable to the cybersecurity competency of an OISU. The Phase 1 Survey targeted responses from 30 SMEs from government and industry. Each KSA required inputs from the SMEs in order to validate all of the KSAs. For each survey item, the SMEs were presented with a seven-point Likert scale ranging from (1) “not at all important” to (7) as “extremely important”. Additionally, the instrument allowed the SMEs to provide qualitative optional feedback for each item in the survey. At the end of the instrument, SMEs had the ability to critique the round, which included the ability to add additional KSAs for further evaluation. The research design for Delphi method portion of Phase 1 is shown in Figure 4. When the required number of SMEs submitted their responses, the qualitative data was assessed to determine if an additional round was required. Since a second round was not needed, the first specific goal of this study was met and RQ1 was addressed. Thus, Phase 1 was complete and the study initiated Phase 2.

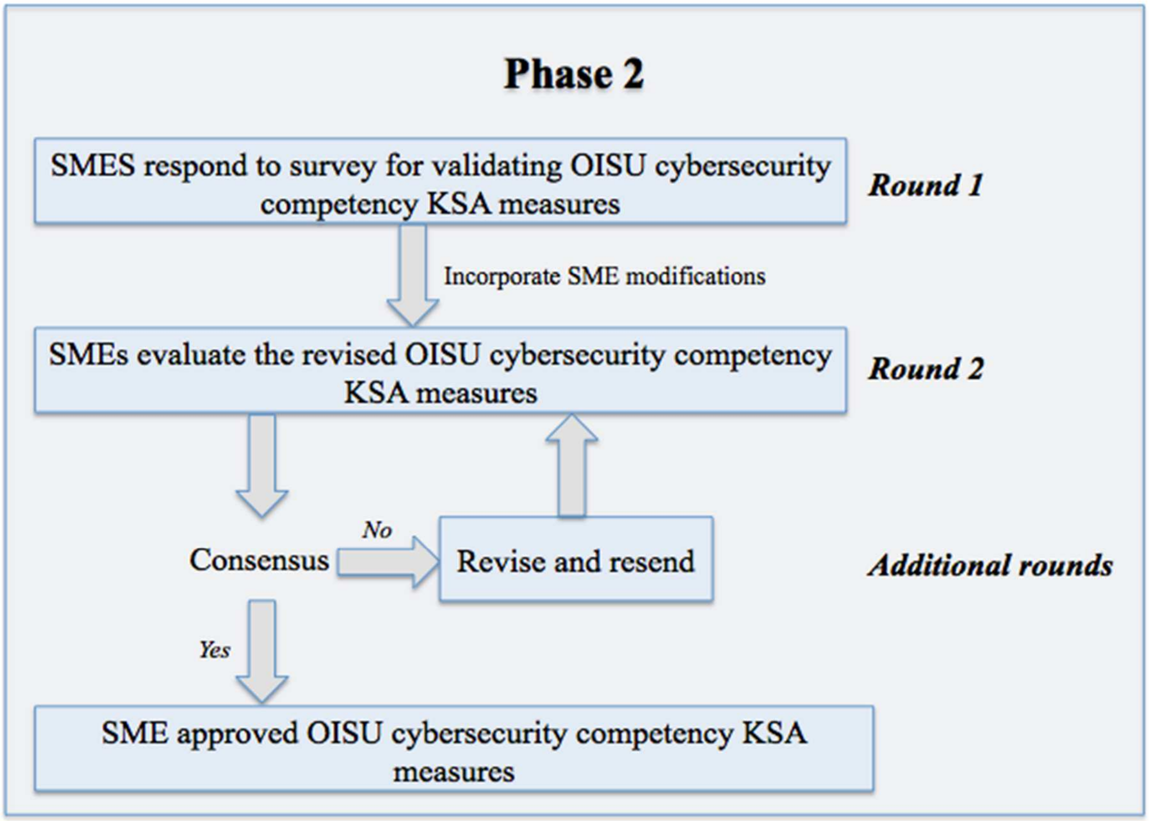

Phase 2
SMES respond to survey for validating OISU cybersecurity competency KSA measures
Round 1
Incorporate SME modifications
SMEs evaluate the revised OISU cybersecurity competency KSA measures
Round 2
Consensus
No
Revise and resend
Additional rounds
Yes
SME approved OISU cybersecurity competency KSA measures

Figure 5. Phase 2 Research design to propose and validate cybersecurity KSA assessment measures for OISUs

Phase 2 Round 1 used a Google® Forms survey (Appendix E) consisting of KSA measures based on all of the KSAs validated in Phase 1. Each KSA measure required inputs from the SMEs in order to validate all of the proposed KSA measures applicable to the cybersecurity competency of an OISU. The Phase 2 Round 1 survey required responses from at least 15 SMEs from government and industry. For each survey item, the SMEs were presented with a seven-point Likert scale ranging from (1) “totally unacceptable” to (7) “perfectly acceptable”. Wherever possible, the KSA measures were developed by researching like or similar content found in literature and public training materials. Additionally, the instrument allowed the SMEs to critique each KSA measure that was presented in the round, which included the ability to add additional assessment questions or vignettes for existing KSAs. The research design for Phase 2 is shown in Figure 5. Consensus for each round was determined by computing the response values based on the Likert scale number. For each round, if 70% of the SMEs responses are greater than or equal to 5.0, the measure is accepted. When compelling qualitative data was submitted for a survey item, even if the 70% acceptance criteria was met, the survey item was added to the Phase 2 Round 2 (Appendix F) instrument for adjustments and further evaluation. The Phase 2 Round 2 survey required responses from at least 7 SMEs from government and industry. Phase 2 Round 2 only displayed the KSA measures that were not accepted in Phase 2 Round 1. When a consensus was achieved on all proposed KSA measures, the second specific goal was met and RQ2 was addressed. Thus, Phase 2 of this study was complete and the study initiated Phase 3.

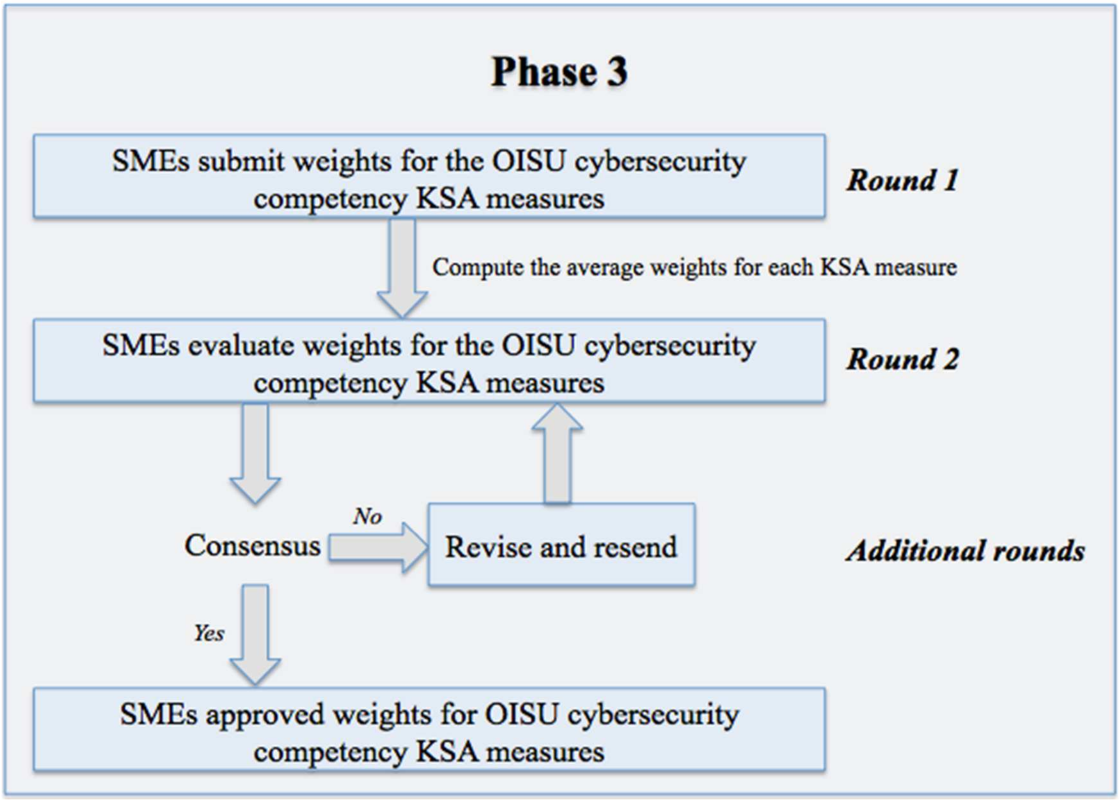

Phase 3
SMEs submit weights for the OISU cybersecurity competency KSA measures
Round 1
Compute the average weights for each KSA measure
SMEs evaluate weights for the OISU cybersecurity competency KSA measures
Round 2
Consensus
No
Revise and resend
Additional rounds
Yes
SMEs approved weights for OISU cybersecurity competency KSA measures

Figure 6. Phase 3 Research design to weight cybersecurity KSA assessment measures for OISUs

The Phase 3 Survey used a Google® Forms survey (Appendix H) consisting of all validated KSAs, which were assigned to Knowledge Category (KC) and Skill Category (SC) groups. Each KC and SC required inputs from the SMEs to assign weights for the cybersecurity competency KSAs of an OISU. The survey required responses from at least 15 SMEs from government and industry. SMEs were asked to allocate 100 points among the four KCs, which were used to compute weighted averages for each KC. The four KCs are: Application Security Knowledge Category (ASKC), Information Security Knowledge Category (ISKC), Internet and Network Security Knowledge Category (INSKC), and Physical Security Knowledge Category (PSKC). SMEs were also asked to allocate 100 points among the four SCs, which were used to compute weighted averages for each SC. The four SCs are: Application Security Skill Category (ASSC), Information Security Skill Category (ISSC), Internet and Network Security Skill Category (INSSC), and Physical Security Skill Category (PSSC). SMEs are asked to allocate 100 points between Overall Knowledge (OK) and Overall Skills (OS) that were used to compute weighted averages. The approach of dividing the KSAs into groups and assigning weights is replicating the approach shown by Keeney (1999). The SMEs were not asked to provide weights for OISU abilities. While abilities are essential requirements for cybersecurity competency, they are assumed in this study based on education. The Phase 3 Survey instrument allowed the SMEs to critique the round. The research design for Phase 3 is shown in Figure 6. The weighted averages were computed by dividing the weighted total of responses for a measure by the total number of SME responses for the measure. Additional rounds would have been required if compelling qualitative data was submitted necessitating further SME evaluation. When the required number of SME responses were received, and the weights were computed, the third specific goal was met and RQ3 had been addressed. All of the assessment weights were incorporated into MyCyberKSAs^{TM} and the study proceeded to Phase 4.

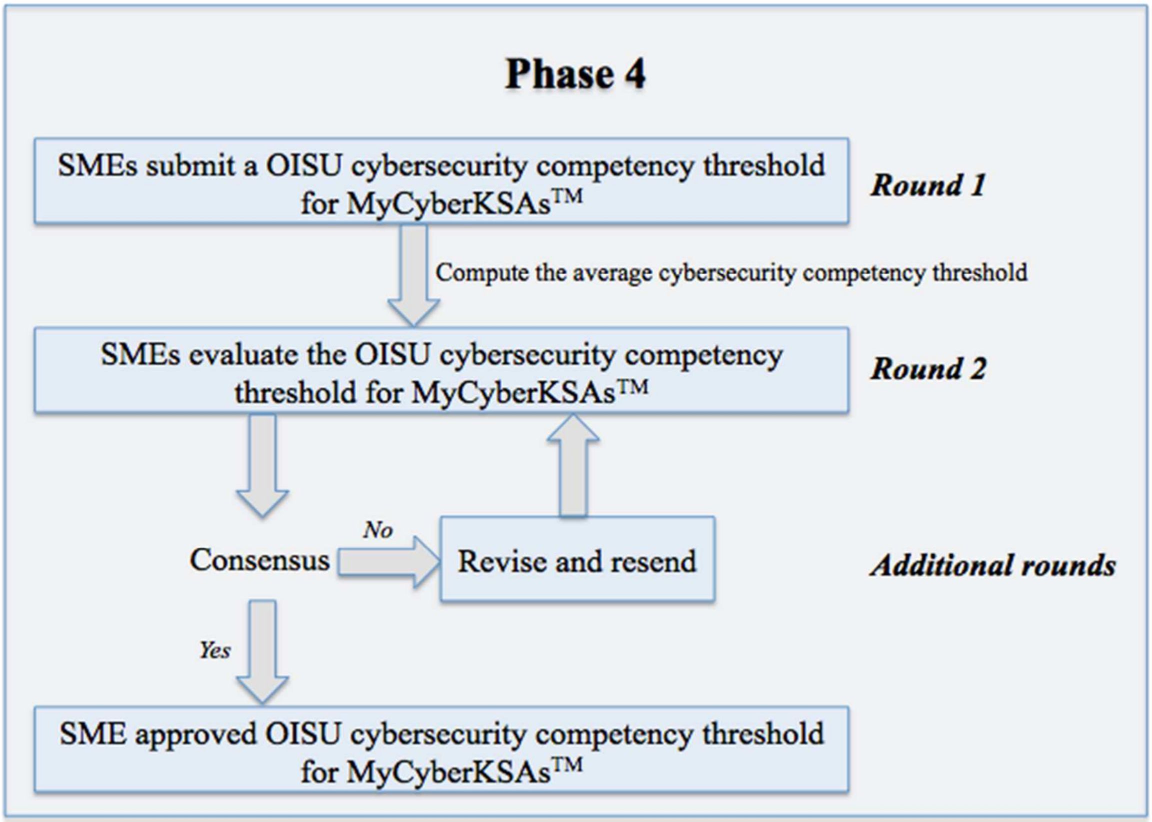

Phase 4
SMEs submit a OISU cybersecurity competency threshold for MyCyberKSAs™
Round 1
Compute the average cybersecurity competency threshold
SMEs evaluate the OISU cybersecurity competency threshold for MyCyberKSAs™
Round 2
Consensus
No
Revise and resend
Additional rounds
Yes
SME approved OISU cybersecurity competency threshold for MyCyberKSAs™

Figure 7. Phase 4 Research design to propose and validate the cybersecurity competency threshold for OISUs

The Phase 4 Survey used a Google® Forms survey (Appendix J) consisting of the weighted KSAs that were validated in Phase 3. The survey also provided a link to the MyCyberKSAs^{TM} assessment prototype tool and the ability to submit a competency threshold. The research design for Phase 4 is shown in Figure 7. The survey required responses from at least 15 SMEs from government and industry. The SMEs possessed the option to submit a percentage required from the MyCyberKSAs^{TM} index score to be used as the cybersecurity threshold. MyCyberKSAs^{TM} included the functionality to provide a total score. The SME responses were averaged and used as the cybersecurity competency threshold. The SMEs did possess the ability to provide qualitative data, which could have resulted in an addition round of assessment by the SMEs. When the required amount of SMEs responses were collected, the fourth specific goal was met and RQ4 had been addressed. The competency threshold was set in the MyCyberKSAs^{TM} prototype tool and the developmental data collection was complete. The study then proceeded to Phase 5.

Phase 5 used a Google® Forms survey (Appendix L) consisting of a link to the MyCyberKSAs^{TM} assessment prototype. The MyCyberKSAs^{TM} prototype was available at http://www.nova.edu/~rn380/. Phase 5 used the MyCyberKSAs^{TM} prototype to collect data on a sample of 54 OISUs to address the fifth specific goal and RQ5. When the required number of OISU responses were collected, and the cybersecurity competency threshold was computed, the fifth specific goal was met and RQ5 had been addressed. After competition of Phase 5, this study then proceeded to data analysis.

Instrument Development Phase 1

The Phase 1 Survey instrument provided the SMEs with the OISU cybersecurity KSAs found in literature and USG documents. The SMEs had the ability to be able to accept KSAs, remove KSAs, or add new KSAs. Additionally, the SMEs had the ability to provide feedback. The instruments for Phase 1 are shown in Appendices A and C. The link to the Google® Forms Phase 1 instrument was emailed to 172 SMEs from academia, government, and industry. The contact form to SMEs for Phase 1 is shown in Appendix B.

Ability Measure

Phase 1 of this study validated OISU abilities that were identified in literature and USG documentation. This validation process allowed the SMEs participating in the study to add, modify, or remove OISU abilities. The Delphi method supported this activity due to the SMEs expertise. The abilities identified in literature and USG documents were the abilities listed on the Phase 1 instrument. However, the direct measure of abilities was not part of this study, given the time limitation on participants to complete the MyCyberKSAs^{TM} prototype tool. Measuring the identified OISU cybersecurity abilities was accomplished via the surrogate measure of the individuals' education indicated, which was collected via the demographics part of the prototype tool. The minimum education that was accepted as a surrogate for OISU cybersecurity abilities is a high school graduate, or equivalent. This study did not argue that an individual that is not a high school graduate (or equivalent) is not capable of possessing OISU cybersecurity abilities. However, a minimum level of education was required for surrogation purposes. The abilities from literature that were listed on the Phase 1 instrument are shown in Table 1.

Knowledge Measure

Phase 1 of this study proposed and validated OISU knowledge topics that were identified in literature and USG documentation. This validation process allowed the SMEs participating in the study to submit additional knowledge topics to all SMEs for review. Additionally, the SMEs had the ability to remove or modify existing knowledge topics. The knowledge topics identified in literature and USG documents were the knowledge topics listed on the Phase 1 instrument. The knowledge topics from literature and USG documents that were listed on the instrument are shown in Table 2.

Skill Measure

Phase 1 of this study proposed and validated OISU skills that were identified in literature and USG documents. This validation process allowed the SMEs participating in the study to submit additional OISU skills. Additionally, the SMEs had the ability to request consensus review on removing or modify existing skills. The skills identified in literature and USG documents were the skills listed on the Phase 1 instrument, and are shown in Table 4. The number of knowledge topics and skill tasks did not align one-to-one, because the literature did not align one-to-one. The literature did not align because not all knowledge topics need to be measured as skill tasks, such as the knowledge of cybersecurity POCs. For example, literature had shown that users require the knowledge that cybersecurity POCs exist, and what circumstances require assistance. However, the literature did not state that OISUs have issues regarding the skill of executing the contact to cybersecurity POCs.

Phase 1 Constructs and Measures

Table 6 lists the constructs and the measures of the Phase 1 Survey instrument for OISU cybersecurity KSA proposal and validation. Table 6 does not include the changes made due to the Phase 1 semi-structured SME interviews. If Phase 1 would have required additional rounds, the instruments additional rounds could not have been constructed until Round 1 of the phase was completed.

Table 6

Constructs and Measures Used in Phase 1 Survey

KSA Type	**KSA number**	**KSA name**	**Author(s)**
Abilities	A1	Near vision ability	Campbell et al., 2015; Trippe et al., 2014
	A2	Problem sensitivity ability	Campbell et al., 2015; Trippe et al., 2014
	A3	Written communication ability	Campbell et al., 2015; Trippe et al., 2014
	A4	Written expression ability	Campbell et al., 2015; Trippe et al., 2014
Knowledge	K1	Knowledge of access control	Gross & Rosson, 2007; Ifinedo, 2012
	K2	Knowledge of antivirus software	Arnold et al., 2010; Gross & Rosson, 2007;
	K3	Knowledge of cyber threats	Gross & Rosson, 2007; Bulgurcu et al., 2010
	K4	Knowledge of cyber vulnerabilities	Gross & Rosson, 2007; Bulgurcu et al., 2010
	K5	Knowledge of cybersecurity POCs	Gross & Rosson, 2007; Parsons et al., 2014
	K6	Knowledge of cybersecurity responsibilities	Gross & Rosson, 2007
	K7	Knowledge of email encryption	Gross & Rosson, 2007; Puhakainen & Siponen, 2010
	K8	Knowledge of email use	Parsons et al., 2014; Barlow et al., 2013
	K9	Knowledge of cyber incident reporting	Imgraben et al., 2014; Parsons et al., 2014
	K10	Knowledge of information handling	Parsons et al., 2014; Arpaci, Kilicer, &, 2015
	K11	Knowledge of information privacy	Bulgurcu et al., 2010; Gross & Rosson, 2007
	K12	Knowledge of Internet use	DISA, 2015; Parsons et al., 2014
	K13	Knowledge of mobile computing risks	DISA, 2015; Levy & Ramim, 2016; Parsons et al., 2014
	K14	Knowledge of password reuse	Ives et al., 2004; Gross & Rosson, 2007
	K15	Knowledge of phishing	Bowen et al., 2012; Verma et al., 2015
	K16	Knowledge of physical security	DISA, 2015; Newsome & Jarmon, 2016
	K17	Knowledge of cybersecurity policy compliance	Mohammed et al., 2015; Safa et al. 2016

Table 6

Constructs and Measures Used in Phase 1 Survey (continued)

KSA Type	**KSA Number**	**KSA name**	**Author(s)**
Knowledge	K18	Knowledge of sensitive information and PII	Gross & Rosson, 2007; Parsons et al. 2014
	K19	Knowledge of social engineering	Cox, 2012; Gross & Rosson, 2007
	K20	Knowledge of social networking security	DISA, 2015; Parsons et al., 2014
	K21	Knowledge of smart card risks	Ardiley, 2012; DISA, 2015; Ives et al., 2004
	K22	Knowledge of strong passwords	Cox, 2012; Parsons et al., 2014
	K23	Knowledge of Webmail risks	Ahmad & Bamnote, 2013; Broucek & Turner, 2005; Symantec, 2016
Skills	S1	Skill in preventing unauthorized access to an IS by controlling access to systems	Gross & Rosson, 2007; Ifinedo, 2012
	S2	Skill in using an antivirus application to properly update the software when notified that antivirus requires an update	Dhepe & Akarte, 2013; Gross & Rosson, 2007; Ifinedo, 2012
	S3	Skill in configuring and using Email in a manner that prevents sensitive information and PII loss	DISA, 2015; Gross & Rosson, 2007
	S4	Skill in cybersecurity incident reporting	Imgraben et al., 2014; Parsons et al., 2014
	S5	Skill in avoiding suspicious and malicious Websites when using the Internet at work	Carlton et al., 2015; DISA, 2015; Parsons et al., 2014
	S6	Skill in securely operating mobile computing devices	Botha et al., 2009; DISA, 2015; Parsons et al., 2014
	S7	Skill in avoiding actions that increase exposure to malicious code downloading or execution	Barlow et al., 2013; DISA, 2015
	S8	Skill in creating using unique passwords for all user accounts and logins	DISA, 2015; Ives et al., 2004
	S9	Skill in peer-to-peer software usage without exploitation by transferring copyrighted materials, sensitive information, or PII	Bishop, 2003; DISA, 2015
	S10	Skill in avoiding a phishing attempts of sensitive information and PII	Carlton et al., 2015; DISA, 2015; Furnell et al., 2008
	S11	Skill in physically protecting an IS from an unauthorized user	DISA, 2015; Dlaminia et al., 2009; Hinduja & Kooi, 2013
	S12	Skill in using authorized systems for sensitive information and PII data processing as well as transmissions	Carlton et al., 2015; DISA, 2015; Knapp & Ferrante, 2012

Table 6

Constructs and Measures Used in Phase 1 Survey (continued)

KSA Type	KSA Number	KSA name	Author(s)
Skill	S13	Skill in labeling removable media that contains sensitive information or PII	Da Veiga & Eloff, 2010; DISA, 2015
	S14	Skill in using encryption to store data on approved removable media	Da Veiga & Eloff, 2010; DISA, 2015
	S15	Skill in identifying sensitive information and PII	DISA, 2015; Puhakainen & Siponen, 2010
	S16	Skill in avoiding social engineering attempts of sensitive information and PII	DISA, 2015; Parsons et al., 2014
	S17	Skill in using social networking without divulging sensitive information and PII	Carlton et al., 2015; DISA, 2015; Gross & Rosson, 2007
	S18	Skill in avoiding a spear-phishing attempts of sensitive information and PII	Botha et al., 2009; DISA, 2015; Luo et al., 2013
	S19	Skill in identifying the spillage of sensitive information and PII	Deshpande et al., 2015; DISA, 2015; Sugii & Nojiri, 2015
	S20	Skill in creating strong passwords	Da Veiga & Eloff, 2010; DISA, 2015; Mujeye & Levy, 2013
	S21	Skill in using encryption to transmit sensitive information and PII when using Webmail	Ahmad & Bamnote, 2013; Broucek & Turner, 2005; Symantec, 2016
	S22	Skill in avoiding a whaling attempts of sensitive information and PII	DISA, 2015; Furnell et al., 2008; Hong, 2012

Instrument Development Phase 2

The instrument for Phase 2 presented the validated knowledge units and skill tasks from Phase 1 to the SMEs as assessment questions as well as vignettes, which were to be validated as KSA measures. Abilities were not directly measured since they were assumed based on the surrogate measure of the individuals' education indicated, which was collected via the demographics part of the prototype tool. It was anticipated that the SMEs would add and/or remove KSAs during Phase 1. When the SMEs removed KSAs in Phase 1, then the tentative Phase 2 Round 1 instrument needed to be amended upon completion of Phase 1. A link to the Google® Forms Phase 2 Round 1 instrument was emailed to 398 SMEs from government and industry. The contact form to SMEs for Phase 2 Rounds 1 and 2 is shown in Appendix D. The Phase 2 Round 1 instrument, which includes all of the KSA measures, is shown in Appendix E. Table 7 provides the constructs and measures of the Phase 2 survey instrument.

Table 7.

Constructs and Measures Used in Phase 2 Survey

Knowledge Category	**Knowledge Unit**	**Knowledge Topic Number**	**Knowledge Topic**
Application Security Knowledge Category	Knowledge of antivirus software	KAV1	Possess knowledge regarding the definition of antivirus software
		KAV2	Possess knowledge regarding keeping antivirus definitions current through updates
	Knowledge of email use	KEU1	Possess knowledge regarding the acceptable uses of work email
	Knowledge of password reuse	KPR1	Possess knowledge regarding creating unique passwords for accounts/logins
	Knowledge of social networking security	KSN1	Possess knowledge regarding the repercussions of posting sensitive information and PII on social networking sites
	Knowledge of applications strong passwords	KSP1	Possess knowledge regarding the properties of a strong password for applications
	Knowledge of Webmail risks	KWM1	Possess knowledge regarding the risk of sending/storing sensitive information and PII on Webmail
		KWM2	Possess knowledge regarding the risk of using work email on public computers
Information Security Knowledge Category	Knowledge of cybersecurity POCs	KCP1	Possess knowledge regarding the reporting of cyber incidents to IT or cybersecurity POCs
	Knowledge of cyber incident reporting	KIR1	Possess knowledge regarding the reporting of cyber incidents regardless of consequence to company reputation

Table 7.

Constructs and Measures Used in Phase 2 Survey (continued)

Knowledge Category	**Knowledge Unit**	**Knowledge Topic Number**	**Knowledge Topic**
Information Security Knowledge Category	Knowledge of cyber incident reporting	KIR2	Possess knowledge regarding the personal consequences for not reporting cyber incidents
		KIR3	Possess knowledge regarding notifying IT or cybersecurity POCs of a quarantined virus
	Knowledge of information handling	KIH1	Possess knowledge regarding the proper destruction of a CD or DVD
		KIH2	Possess knowledge regarding the risks of using thumb drives and USB device
		KIH3	Possess knowledge regarding not posting sensitive information or PII to public domains
	Knowledge of information privacy	KIP1	Possess knowledge regarding the consequences for violating information privacy laws
	Knowledge of cybersecurity policy compliance	KPC1	Possess knowledge regarding the consequences for non-compliance to company cybersecurity policies
	Knowledge of sensitive information and PII	KSI1	Possess knowledge regarding the identification of sensitive information identification
		KSI2	Possess knowledge regarding the identification of PII
Internet and Network Security Knowledge Category	Knowledge of cyber threats	KCT1	Possess knowledge regarding the identification of cyber threats
		KCT2	Possess knowledge regarding a capability of computer viruses
		KCT3	Possess knowledge regarding the purpose of phishing attempts
		KCT4	Possess knowledge regarding the purpose of SPAM
		KCT5	Possess knowledge regarding a capability of computer spyware
		KCT6	Possess knowledge regarding a ransomware attack

Table 7.

Constructs and Measures Used in Phase 2 Survey (continued)

Knowledge Category	Knowledge Unit	Knowledge Topic Number	Knowledge Topic
Internet and Network Security Knowledge Category	Knowledge of cyber vulnerabilities	KCV1	Possess knowledge regarding the identification of cyber vulnerabilities
		KCV2	Possess knowledge regarding methods to help protect against insider attacks
	Knowledge of email encryption	KEE1	Possess knowledge regarding the criteria for when to encrypt an email
	Knowledge of phishing	KP1	Possess knowledge regarding protection against phishing
		KP2	Possess knowledge regarding the goal of phishing emails with embedded links
		KP3	Possess knowledge regarding methods to avoid phishing Websites
	Knowledge of phishing	KP4	Possess knowledge regarding identifying phishing email narratives (such as free gifts)
	Knowledge of using file permissions	KFP1	Possess knowledge regarding the purpose of file permissions
	Knowledge of Internet use	KIU1	Possess knowledge regarding when it is acceptable to use work Internet for personal use
		KIU2	Possess knowledge regarding using peer-to-peer file sharing software
		KIU3	Possess knowledge regarding when it is acceptable to visit suspicious non-secured Websites
		KIU4	Possess knowledge regarding the when it is acceptable to download software
Physical Security Knowledge Category	Knowledge of access control	KAC1	Possess knowledge regarding identifying the risk of writing down passwords
		KAC2	Possess knowledge regarding how often passwords should be changed
		KAC3	Possess knowledge regarding identifying the need to keep passwords confidential

Table 7.

Constructs and Measures Used in Phase 2 Survey (continued)

Knowledge Category	**Knowledge Unit**	**Knowledge Topic Number**	**Knowledge Topic**
Physical Security Knowledge Category	Knowledge of access control	KAC4	Possess knowledge regarding when to disable/lock computer
		KAC5	Possess knowledge regarding restricting computer access from visitors
		KAC6	Possess knowledge regarding understanding who is responsible if computer access is compromised
		KAC7	Possess knowledge regarding what to do when access/credential phishing attempts are received
		KAC8	Possess knowledge regarding the what to do when an access compromise occurs
	Knowledge of cybersecurity responsibilities	KCR1	Possess knowledge regarding the identification of cybersecurity responsibilities
	Knowledge of mobile computing risks	KMC1	Possess knowledge regarding the risks to drive security when using public Wi-Fi
		KMC2	Possess knowledge regarding the risks to email security when using public Wi-Fi
	Knowledge of physical security	KPS1	Possess knowledge regarding what to do when an unauthorized person is at a computer
	Knowledge of social engineering	KSE1	Possess knowledge regarding methods to protect against social engineering
	Knowledge of smart card risks	KSC1	Possess knowledge regarding the risk of hacking a lost smart (PKI) card
		KAC8	Possess knowledge regarding the what to do when an access compromise occurs

Table 7.

Constructs and Measures Used in Phase 2 Survey (continued)

Skill Category	Skill Area	Skill Task Number	Skill Task
Application Security Skill Category	Skill in using an antivirus application to properly update the software when notified that antivirus requires an update	SAV1	Demonstrate the task of updating antivirus software when notified that an antivirus software update is available
	Skill in peer-to-peer software usage without exploitation by transferring copyrighted materials, sensitive information, or PII	SP2P1	Demonstrate the task of not using peer-to-peer software to illegally transfer copyrighted materials, sensitive information, or PII
	Skill in creating using unique passwords for user accounts and logins	SPR1	Demonstrate the task of creating unique passwords on multiple user accounts or logins
	Skill in creating strong passwords	SSTP1	Demonstrate the task of creating strong passwords for user accounts or logins
	Skill in using encryption to transmit sensitive information and PII when using Webmail	SWM1	Demonstrate the task to use encryption when sending sensitive information or PII with Webmail
	Skill in managing cookie settings and usage	SCU1	Demonstrate the task of adjusting Web browser settings to prompt for cookies
		SCU2	Demonstrate the task of declining cookies from suspicious Websites
		SCU3	Demonstrate the task of declining cookies from non-secured Websites
	Skill in using email in a manner that prevents sensitive information and PII loss	SES1	Demonstrate the task of not downloading malicious code
		SES2	Demonstrate the task of encrypting an email
		SES3	Demonstrate the task of not using work email for personal use
		SES4	Demonstrate the task of enables plain text and disabling the preview pane in email client
		SES5	Demonstrate the task of using digital signatures when sending emails

Table 7.

Constructs and Measures Used in Phase 2 Survey (continued)

Skill Category	**Skill Area**	**Skill Task Number**	**Skill Task**
Application Security Skill Category	Skill in using email in a manner that prevents sensitive information and PII loss	SES6	Demonstrate the task of virus-scanning email attachments
Information Security Skill Category	Skill in cybersecurity incident reporting	SIR1	Demonstrate the task of reporting coworker misconduct that violates a company cybersecurity policy
	Skill in using authorized systems for sensitive information and PII data processing as well as transmissions	SSI1	Demonstrate the task of not using an unauthorized system when dealing with sensitive information and PII
		SSI2	Demonstrate the task of not using non-secured text message to transmit sensitive information or PII
	Skill in identifying sensitive information and PII	SSII1	Demonstrate the task of identifying an address and phone number as PII
		SSII2	Demonstrate the task of identifying proprietary information as sensitive information
	Skill in identifying the spillage of sensitive information and PII	SS1	Demonstrate the task of reporting a spillage incident
	Skill in labeling removable media that contains sensitive information or PII	SMP1	Demonstrate the task of labeling any removable media that contains sensitive information or PII
	Skill in using encryption to store data on approved removable media	SMU1	Demonstrate the task of using approved/appropriate removable media
		SMU2	Demonstrate the task of encrypting sensitive information and PII when using removable media
Internet and Network Security Skill Category	Skill in avoiding suspicious and malicious Websites when using the Internet at work	SIU1	Demonstrate the task of identifying and avoiding a malicious popup windows

Table 7.

Constructs and Measures Used in Phase 2 Survey (continued)

Skill Category	**Skill Area**	**Skill Task Number**	**Skill Task**
Internet and Network Security Skill Category	Skill in avoiding suspicious and malicious Websites when using the Internet at work	SIU2	Demonstrate the task of identifying and avoiding dubious or pornographic Websites
		SIU3	Demonstrate the task of not using credit cards on non-secured Websites
	Skill in avoiding actions that increase exposure to malicious code downloading or execution	SMC1	Demonstrate the task of not using links within emails
		SMC2	Demonstrate the task of disabling automatic downloads in a Web browser
		SMC3	Demonstrate the task of virus scanning a CD/DVD/thumb-drive
		SMC4	Demonstrate the task of not forwarding infected files
	Skill in avoiding phishing attempts of sensitive information and PII	SP1	Demonstrate the task of not divulging sensitive information or PII to a phishing attempt
	Skill in avoiding a phishing attempts of sensitive information and PII	SP2	Demonstrate the task of verifying the identity of an email sender to prevent the divulging of sensitive information or PII to a phishing attempt
	Skill in avoiding a spear-phishing attempts of sensitive information and PII	SSP1	Demonstrate the task of not divulging sensitive information or PII to a spear phishing attack that mimics coworker
		SSP2	Demonstrate the task of not divulging sensitive information or PII to a spear-phishing attack that states your name
	Skill in avoiding whaling attempts of sensitive information and PII	SW1	Demonstrate the task of not divulging sensitive information or PII to a whaling attack
Physical Security Skill Category	Skill in preventing unauthorized access to an IS by controlling access to systems	SAC1	Demonstrate the task of keeping a password confidential
		SAC2	Demonstrate the task of locking a computer while not in use

Table 7.

Constructs and Measures Used in Phase 2 Survey (continued)

Skill Category	Skill Area	Skill Task Number	Skill Task
Physical Security Skill Category	Skill in preventing unauthorized access to an IS by controlling access to systems	SAC3	Demonstrate the task of reporting to IT or cybersecurity POCs that an access compromise has occurred
	Skill in physically protecting an IS from an unauthorized user	SPS1	Demonstrate the task of reporting an unauthorized person on an IS to IT or cybersecurity POCs
	Skill in securely operating mobile computing devices	SMS1	Demonstrate the task of locking a mobile device when not in use
		SMS2	Demonstrate the task of disabling wireless capabilities when the IS is using a LAN
		SMS3	Demonstrate the task of encrypting sensitive information or PII when using a mobile device such as a laptop
		SMS4	Demonstrate the task of disabling wireless capabilities when the mobile device is not in use
	Skill in using social networking without divulging sensitive information and PII	SSN1	Demonstrate the task of using a social network without divulging PII
		SSN2	Demonstrate the task of using a social network without divulging sensitive information
	Skill in avoiding social engineering attempts of sensitive information and PII	SSE1	Demonstrate the task of identifying and avoiding social engineering attempts by text messages
		SSE2	Demonstrate the task of identifying and avoiding social engineering by vishing surveys
		SSE3	Demonstrate the task of identifying and avoiding social engineering by public conversations

Instrument Development Phase 3

The instrument for Phase 3 presented the validated KSAs from Phase 1 and the KSA measures from Phase 2 to acquire KSA weights from the SMEs. Abilities were not directly measured since they were assumed based on the surrogate measure of the individuals' education indicated, which was collected via the demographics part of the prototype tool. Therefore, abilities were not weighted, nor do abilities need to be weighted. The knowledge KSAs were divided into four knowledge categories, as shown in Table 8. SMEs were asked to allocate 100 points among the knowledge categories. The skill KSAs were also divided into four skill categories as shown in Table 8. SMEs were asked to allocate 100 points among the skill categories.

Table 8.

Knowledge and Skill Constructs Used in Phase 3 Survey

Knowledge Category	**Knowledge Unit Number**	**Knowledge Unit**
Application Security Knowledge Category	KU1	Knowledge of antivirus software
	KU2	Knowledge of email use
	KU3	Knowledge of password reuse
	KU4	Knowledge of social networking security
	KU5	Knowledge of strong passwords
	KU6	Knowledge of Webmail risks
Information Security Knowledge Category	KU7	Knowledge of cybersecurity POCs
	KU8	Knowledge of cyber incident reporting
	KU9	Knowledge of information handling
	KU10	Knowledge of information privacy
	KU11	Knowledge of cybersecurity policy compliance
	KU12	Knowledge of sensitive information and PII
Internet and Network Security Knowledge Category	KU13	Knowledge of cyber threats
	KU14	Knowledge of cyber vulnerabilities
	KU15	Knowledge of email encryption
	KU16	Knowledge of phishing
	KU17	Knowledge of Internet use

Table 8.

Knowledge and Skill Constructs Used in Phase 3 Survey (continued)

Knowledge Category	**Knowledge Unit Number**	**Knowledge Unit**
Physical Security Knowledge Category	KU18	Knowledge of access control
	KU19	Knowledge of cybersecurity responsibilities
	KU20	Knowledge of physical security
	KU21	Knowledge of social engineering

Skill Category	**Skill Area Number**	**Skill Area**
Application Security Skill Category	SA1	Skill in using an antivirus application to properly update the software when notified that antivirus requires an update
	SA1	Skill in using an antivirus application to properly update the software when notified that antivirus requires an update
	SA2	Skill in creating using unique passwords for all user accounts and logins
	SA3	Skill in creating strong passwords
	SA4	Skill in using encryption to transmit sensitive information and PII when using Webmail
	SA5	Skill in configuring and using Email in a manner that prevents sensitive information and PII loss
	SA5	Skill in configuring and using Email in a manner that prevents sensitive information and PII loss
Information Security Skill Category	SA6	Skill in cybersecurity incident reporting
	SA7	Skill in using authorized systems for sensitive information and PII data processing as well as transmissions
	SA8	Skill in identifying sensitive information and PII
	SA9	Skill in identifying the spillage of sensitive information and PII
	SA10	Skill in using encryption to store data on approved removable media
Internet and Network Security Skill Category	SA11	Skill in avoiding suspicious and malicious Websites when using the Internet at work
	SA12	Skill in avoiding actions that increase exposure to malicious code downloading or execution
	SA13	Skill in avoiding a phishing attempts of sensitive information and PII
	SA14	Skill in avoiding a spear-phishing attempts of sensitive information and PII
	SA15	Skill in avoiding a whaling attempts of sensitive information and PII

Table 8.

Knowledge and Skill Constructs Used in Phase 3 Survey (continued)

Skill Category	**Skill Area Number**	**Skill Area**
Physical Security Skill Category	SA16	Skill in preventing unauthorized access to an IS by controlling access to systems
	SA17	Skill in physically protecting an IS from an unauthorized user
	SA18	Skill in securely operating mobile computing devices
	SA19	Skill in using social networking without divulging sensitive information and PII
	SA20	Skill in avoiding social engineering attempts of sensitive information and PII

A link to the Google® Forms Phase 3 instrument was emailed to 54 SMEs from government and industry. The contact form to SMEs for Phase 3 is shown in Appendix G. The Phase 3 instrument is shown in Appendix H.

Instrument Development Phase 4

The instrument for Phase 4 presented the SMEs with the weighted KSAs from Phase 3 to acquire a cybersecurity competency threshold. Additionally, the SMEs were given a link to the MyCyberKSAs™ prototype assessment tool. A link to the Google® Forms Phase 4 instrument was emailed to 39 SMEs from government and industry. The contact form to SMEs for Phase 4 is shown in Appendix I. The Phase 4 instrument is shown in Appendix J.

Instrument Development Phase 5

The instrument for Phase 5 used participants to test the MyCyberKSAs™ prototype tool. A link to the Google® Forms Phase 5 instrument was sent to 569 OISUs. The contact form to test participants for Phase 5 is shown in Appendix K. The prototype tool also collected demographic data that was needed for data analysis. Demographic questions included: age, gender, job function, time with current organization, education, annual cybersecurity training, and cybersecurity certifications. The Phase 5 instrument is shown in Appendix L.

Proposed Sample

For Phases 1 thru 4, this study was conducted using the Delphi method to collect data from the expert panel. The expert panel was comprised of SMEs that are experts regarding the cybersecurity KSAs of OISUs. Skulmoski et al. (2007) noted that Delphi method expert panel sizes can range from 11 to 345. However, Delphi method panel sizes typically are in the range of 7 to 30 experts (Ramim & Lichvar, 2014; Skinner et al., 2015). Therefore, considering the proposed delimitation for bias, this study selected 15-30 panelists from industry and government for round one of each phase. When a second phase was required in Phase 2 Round 2, seven panelists from industry and government were used. Due to the critical nature of the Phase 1 responses as the foundation for this study, Phase 1 required a minimum of 30 SME responses. This study attempted to contact the same group of SMEs to participate in Phases 1 thru 4. All Phases collected anonymous responses, thus there was no method for verifying recurring SME participation. This study accepted cybersecurity certifications, professional experience, and academic degrees as credentials for the SMEs. This study solicited government and industry SME participation using emails to personal and professional contacts that possess cybersecurity credentials via the LinkedIn© social media Website. Phase 5 used solicitations via FaceBook© to gather responses from a sample of 50 OISUs, from government and industry, to test the prototype MyCyberKSAs^{TM} cybersecurity competency assessment tool.

Pre-Analysis Data Screening

Pre-analysis data screening is a process used to detect issues with collected data (Levy, 2006). Levy (2006) stated that "pre-analysis data preparation deals with the process of detecting irregularities or problems with the collected data" (p. 150). In the event that any SME appeared to be providing dishonest or malicious responses, the SME responses would have been discarded. In the event a SME entered only one value for all responses (known as a response-set), the SME responses would have been discarded.

Levy (2006) noted that missing data presents a significant validity issue. The resources that were used in this study had the ability to make all instrument items required. Therefore, this study did not allow any questions to be skipped within any of the five phases of data collection.

Levy (2006) additionally noted that pre-analysis data screening includes ensuring that data processing errors do not exist. For Phases 1 – 4 this study generated data directly from Google® Forms. It was not possible to manipulate the data storage transactions in Google® Forms, yet they were tested 10 times for accuracy before the phase was initiated. In Phase 5, Java scripts were used within Adobe® Captive to send data to Google® Forms for storage and analysis. Since the data processing error potential is much higher in Phase 5 than the previous phases, 10 different testers were observed and their responses were manually recorded. The manually recorded responses were then cross-referenced with the data transmitted to Google® Forms to ensure accuracy.

Data Analysis

Each round of each phase must be fully documented, as instructed by Seuring and Müller (2008) to conduct Delphi method data analysis. As recommended for Delphi method expert panel studies, this study has shown the levels of dispersion computed for each round of each phase (Hasson, Keeney, & McKenna, 2000). Levels of dispersion include standard deviation and the mean (Hasson et al., 2000; Skinner et al., 2015). The computed means for each instrument item revealed the average SME response for that item. The standard deviation revealed the level of agreement among the SMEs.

The interviews that were performed at the beginning of Phase 1 with 5 SMEs generated quantitative and qualitative data. The SMEs were asked to review the initial KSA list and provide a binary response as to whether KSAs should be accepted or rejected. The SMEs were then asked to provide explanations regarding their decisions to remove KSAs. The SMEs did have the ability to add KSAs to the initial list. Data analysis contained a subjective element where reasoned arguments, asserted with literature, influenced whether or not the SME suggestions were incorporated into the Phase 1 survey instrument. Specifically, if less than 60% of the SMEs suggest the removal of a KSA, or compelling arguments are not made (and asserted with literature) to remove the KSA, the KSA remained on the Phase 1 survey for evaluation by the 30 SMEs expert panel.

The data analysis for Phases 1 – 4 of this study were conducted by exporting the results, which are stored in Google® Forms, into the Microsoft® Excel. Therefore, for Phases 1 – 4, levels of dispersion were computed for each item of every Delphi round. The data analysis for the Phase 5 pilot test of the MyCyberKSAs^{TM} prototype tool consisted of computing the following scores: cumulative, by demographic data, KC, SC, OK, OS, maximums, minimums, and percentage of correct responses for each KSA measure. Phase 5 also included performing one-way ANOVA with IBM® Statistical Package for the Social Sciences (SPSS) for each demographic group. The Phase 5 data was presented in the form of graphs and tables for analysis.

Data analysis for Phase 3 also required the computation of the weights that were proposed and validated by the SMEs. To develop the weights of the KCs, the SMEs were asked to allocate 100 points between each KC, as shown in Table 8. The four KCs were: Application Security Knowledge Category (ASKC), Information Security Knowledge Category (ISKC), Internet and Network Security Knowledge Category (INSKC), and Physical Security Knowledge Category (PSKC). SMEs were also asked to allocate 100 points between each SC, as shown in Table 8. The four SCs were: Application Security Skill Category (ASSC), Information Security Skill Category (ISSC), Internet and Network Security Skill Category (INSSC), and Physical Security Skill Category (PSSC). To compute the weight for each KC, the total number of SME points were added for each KC individually, and then divided by the number of SME responses for the respective KC. To compute the weight for each SC, the total number of SME points were added for each SC individually, and then divided by the number of SME responses for the respective SC.

The need to propose and validate the categories allowed the SMEs to rank the importance of: ASKC, ISKC, INSKC, PSKC, ASSC, ISSC, INSSC, and PSSC. These weights also allowed the SMEs to rank the importance of OK and OS. OK is computed as the sum of all knowledge measures, as shown in Equation 1. OS is computed as the sum of all skill measures, as shown in Equation 2. The overall score for MyCyberKSAs^{TM} is the sum of weighted OK and OS values, as shown in Equation 3. Figure 8 depicts how the MyCyberKSAs^{TM} index score is computed from the two levels of weighted measures. The MyCyberKSAs^{TM} will produce a total maximum score of 100 points.

The equations to compute the weighted totals are as follows:

$$\text{Eq. 1: OK} = ((w(ASKC) * \ ASKC) + (w(ISKC) * \ ISKC) + (w(INSKC) * INSKC) + (w(PSKC) * PSKC))$$

$$\text{Eq. 2: OS} = ((w(ASSC) * \ ASSC) + (w(ISSC) * \ ISSC) + (w(INSSC) * INSSC) + (w(PSSC) * PSSC))$$

$$\text{Eq. 3: MyCyberKSAs Index} = ((w(OK) * OK) + (w(OS) * \ OS))$$

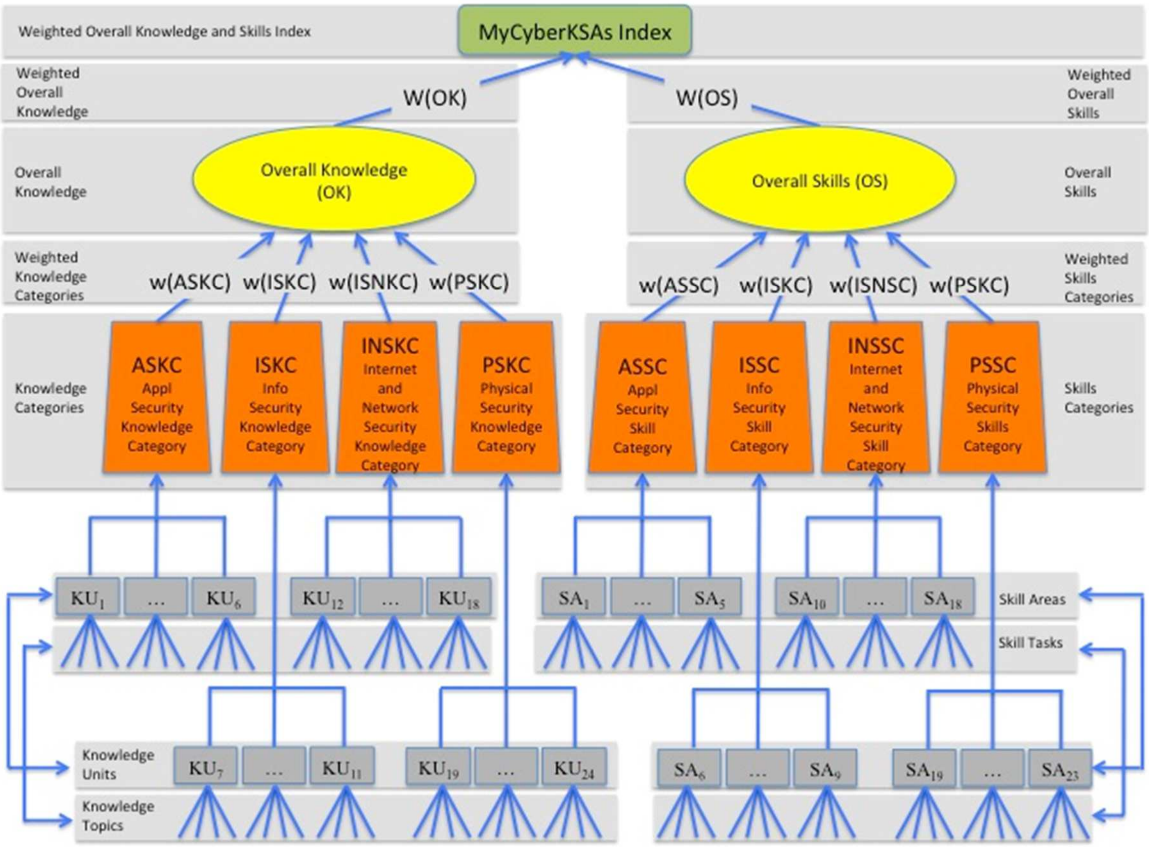

Weighted Overall Knowledge and Skills Index
MyCyberKSAs Index
Weighted Overall Knowledge
W(OK)
W(OS)
Weighted Overall Skills
Overall Knowledge
Overall Knowledge (OK)
Overall Skills (OS)
Overall Skills
Weighted Knowledge Categories
w(ASKC) w(ISKC) w(ISNKC) w(PSKC)
w(ASSC) w(ISKC) w(ISNSC) w(PSKC)
Weighted Skills Categories
Knowledge Categories
ASKC Appl Security Knowledge Category
ISKC Info Security Knowledge Category
INSKC Internet and Network Security Knowledge Category
PSKC Physical Security Knowledge Category
ASSC Appl Security Skill Category
ISSC Info Security Skill Category
INSSC Internet and Network Security Skill Category
PSSC Physical Security Skills Category
Skills Categories
KU_1 … KU_6 KU_{12} … KU_{18}
SA_1 … SA_5 SA_{10} … SA_{18}
Skill Areas
Skill Tasks
Knowledge Units
KU_7 … KU_{11} KU_{19} … KU_{24}
SA_6 … SA_9 SA_{19} … SA_{23}
Knowledge Topics

Figure 8. Depiction of the MyCyberKSAs^{TM} index score computation

Data analysis for Phase 4 required the computation of the cybersecurity competency threshold. SMEs were asked to determine what percentage of points from the maximum composite score defines the OISU cybersecurity competency threshold. Each SME will submit a percentage value for which they assess is the OISU cybersecurity competency threshold. All SMEs submissions will then be averaged to determine the OISU cybersecurity competency threshold.

For Phase 1, once data analysis determined a consensus was achieved, the first specific goal had been met and RQ1 had been addressed. When data analysis determined a consensus was achieved in Phase 2, the second specific goal had been met and RQ2 had been addressed. In Phase 3, once the SMEs submitted the required weights, which were then averaged, the third specific goal has been met and RQ3 had been addressed. For Phase 4, when the SMEs submitted the required cybersecurity competency threshold score, which was then averaged, the fourth specific goal had been met and RQ4 had been addressed.

Data analysis for Phase 5 first tested the reliability of the Web-based MyCyberKSAs^{TM} prototype tool by comparing the submitted selections of 10 participants versus what was recorded in the submission database. When it was confirmed that the prototype tool was accurately recording answers, Phase 5 performed the pilot test of the MyCyberKSAs^{TM} prototype using 54 test participants. The data analysis assessed levels of dispersion and one-way analysis of variance (ANOVA). Phase 5 data analysis included illustrating the levels of dispersion for demographic group.

Reliability and Validity

Reliability

Straub, Rai, and Klein (2004) defined reliability as “the extent to which a variable or set of variables is consistent in what it is intended to measure” (p. 70). Essentially, reliability can be thought of as an evaluation of measurement accuracy where a method yields similar results when under constant conditions for all occasions (Hasson et al., 2000; Straub, 1989). However, the Delphi method is inherently reliable due to the volume of experts on the panel. Essentially, as the number of SMEs on the expert panel increases, the reliability of the Delphi implementation increases (Powell, 2002). While 7 SMEs is acceptable for a Delphi study, this study used 15-30 SMEs in Round 1 of each phase to increase reliability (Skinner et al., 2015). Additionally, reliability is enhanced when reasoned argument is involved (Hasson et al., 2000). Therefore, this study allowed SMEs to provide feedback for each instrument item. Also, the reliability of the Delphi method can be confirmed when the study is documented and the progression of rounds is described (Seuring & Müller, 2008). Therefore, each aspect of this study was documented and the progression of rounds was described.

Validity

The Delphi method itself provides content validity due to the traits of the methodology (Hasson & Keeney, 2011; Straub, 1989). Content validity is acquired by the number of experts serving on the panel, which is viewed as a confirmatory judgment (Hasson & Keeney, 2011). Construct validity is acquired when the researcher performing the study can confirm the statements made by the expert panel members, and also by performing successive rounds (Hasson & Keeney, 2011; Okoli & Pawlowski, 2004).

Criterion-related validity is assumed because concurrent validity and predictive validity are achieved when performing the Delphi method (Hasson & Keeney, 2011). Concurrent validity is met by performing successive rounds of expert input that leads to a consensus agreement (Hasson & Keeney, 2011; Straub, 1989). Predictive validity is often measured by the accuracy of the Delphi, which is argued to be the proof of methodology validity since the Delphi method has proven to be quite accurate in short and long range forecasting (Hasson & Keeney, 2011).

Straub (1989) defined internal validity as the likelihood that "observed effects could have been caused by or correlated with a set of unhypothesized and/or unmeasured variables" (p. 151). Furthermore, Seuring and Müller (2008) stated that when using the Delphi method "internal validity is ensured by applying content analysis and survey techniques for the data analysis" (p. 458). Moreover, Creswell (2002) noted that internal validity is increased when randomly selecting participants for the study. Therefore, this study selected a portion of participants at random using FaceBook© solicitations. Additionally, a threat to internal validity exists where SMEs do not identify all of the required KSAs. To limit this threat to internal validity, this study established a minimum requirement for SME participation with multiple rounds of Delphi method validation (per phase), as well as conducted a thorough review of literature to ensure the threat of missing KSAs is minimized.

Calder, Phillips, and Tybout (1982) stated that external validity "examines whether or not an observed causal relationship should be generalized to and across different measures, persons, settings, and times" (p. 240). In Delphi method research, not mentioning the response rate from expert panelists may pose a threat to external validity

(Lindner, Murphy, & Briers, 2001). Therefore, this study reported response rates for each iteration of each phase of data collection. Additionally, not controlling for nonresponse is a threat to external validity (Lindner et al., 2001). To control for nonresponses, this study solicited SMEs until the required number of responses was received. Another threat to external validity is not having generalizability across measures (Calder, Phillips, & Tybout, 1982). This threat can be controlled in Delphi by selecting expert panelists from different fields of practice (Calder et al., 1982; Okoli & Pawlowski, 2004). Therefore, this study selected SMEs from government and industry. OISUs were accepted from any field of practice, as long as they were 18 years of age or older.

Resources

Google® Forms was utilized to develop as well as deploy surveys to the expert panel participants. FaceBook© was utilized to deploy solicitations to the OISUs. Communication with the expert panel participants was conducted through email, FaceBook© Messenger, and LinkedIn© Messages. Data analysis was conducted by exporting results from Google® Forms into Microsoft® Excel and IBM® SPSS. The MyCyberKSAs™ cybersecurity competency assessment tool was developed using Adobe® Captivate. Additionally, the MyCyberKSAs™ prototype tool wrote all responses to Google® Forms. MyCyberKSAs™ was hosted at http://www.nova.edu/~rn380/ and contained on the Nova Southeastern University server. Free images/graphics for the MyCyberKSAs™ prototype tool were downloaded from www.pexels.com as well as open source images from Google®.

Summary

This chapter provided an overview of the methodology that was implemented for this research study. Specifically, this chapter presented the information regarding the implementation of SME data collection using the Delphi method. This developmental research study used a Delphi method approach to propose, validate, and test the prototype MyCyberKSAs^{TM} cybersecurity competency assessment tool. The MyCyberKSAs^{TM} prototype tool was developed to be an instrument used to determine if an OISU has cybersecurity competency for organizational network access privileges.

This chapter also discussed the methods to address the research questions. Additionally, this chapter extracted the OISU cybersecurity KSAs from the literature review to establish an initial list of KSAs relevant to organizational network access privileges. This chapter also examined reliability, validity, data collection procedures, pre-analysis data screening, data analysis processes, resources, and the proposed sample groups.

This chapter outlined a five-phase approach towards developing the MyCyberKSAs^{TM} cybersecurity competency assessment prototype tool by outlining instrument development for each phase of research. After establishing the initial OISU cybersecurity KSA list from literature and USG documents, the Phase 1 of Delphi method data collection from SMEs proposed and validated OISU cybersecurity KSAs. Phase 2 of Delphi method data collection from SMEs proposed and validated OISU cybersecurity KSA measures. Phase 3 of Delphi method data collection from SMEs proposed and validated OISU cybersecurity KSA weights. Phase 4 of Delphi method data collection proposed and validated the OISU cybersecurity competency threshold. Phase 5 of this study tested the prototype MyCyberKSAs^{TM} cybersecurity competency assessment tool on a sample of 54 OISUs. This chapter also discussed the proposed sample groups for all five phases of research, and the resources used to complete this research.

Chapter 4

Results

Overview

This chapter contains the results and data analysis performed by this research study. This study used five phases data collection, with each phase requiring data analysis, and each phase addressed a research question. Data collection and analysis for Phase 1 proposed and validated the OISU cybersecurity KSAs. Data collection and analysis for Phase 2 proposed and validated the OISU cybersecurity KSA measures. Data collection and analysis for Phase 3 proposed and validated the OISU cybersecurity KSA weights. Data collection and analysis for Phase 4 proposed and validated the OISU cybersecurity competency threshold. Data collection and analysis for Phase 5 measured the cybersecurity competency of 54 OISUs. Data analysis for each phase computed levels of dispersion for each instrument parameter. Data analysis for Phase 5 showed that annual cybersecurity training and job function are significant, showing differences in cybersecurity competency. Data analysis for Phase 5 showed that age, cybersecurity certification, gender, and time with company are not significant, showing no differences in cybersecurity competency.

Semi-Structured Subject Matter Expert (SME) Interviews

This study compiled a list of all KSAs applicable to OISUs from scholarly literature and USG documents. Before initiating Phase 1 of this study, five semi-structured SME interviews were accomplished to ensure the quality of the initial KSA list. The results of the semi-structured SME interviews identified three KSAs that were deemed unnecessary in regards to the cybersecurity competency assessment of an OISU. To eliminate a KSA from the Phase 1 instrument, 60% of the SMEs needed to recommend removal of the KSA. The KSAs identified for removal were: advanced written comprehension ability, skill in managing cookie settings & usage, and knowledge of using file permissions. The summary of all KSAs nominated for removal based on the results of the semi-structured SME interviews are shown in Table 9. In addition to providing feedback of KSA removals from the initial list, the SMEs provided qualitative feedback on KSA additions and modifications. Specifically, 60% of the SMEs noted that 'skill in configuring and using Email in a manner that prevents sensitive information and PII loss' needed to be modified. Three of the five SMEs recognized the need to measure OISU skill with using email, but do not agree with OISUs needing to configure email as this is a system configuration/function managed by company policies and IT. Additionally, 80% of all SMEs noted that ransomware should be assessed within this study. Moreover, the SMEs advised that knowledge of ransomware is required in some form, as well as the assessment of skill on how to respond to a ransomware situation within the workplace. More specifically, a highly qualified SME advised that in the event of a ransomware notification, ideally an OISU will immediately unplug their system (without logging off or shutting down the system) and notify IT of cybersecurity POCs of the incident. The SME explained that some sophisticated ransomware software seen 'in the wild' will scan and encrypt all systems on the network (including backup/recovery systems), which is not an immediate process, thus unplugging from the network can be extremely beneficial.

Table 9.

Summary of Semi-Structured SME Interview KSA Removal Feedback

KSA to Remove	Percentage of SMEs removing KSA	Reasoned Arguments for Removing KSA
Advanced written comprehension ability	60%	OISUs should not be receiving documents that are technical in nature. This ability is desired, but not required. OISUs do not need to comprehend tech documentation.
Knowledge of using file permissions	60%	File permissions may need to be managed/handled by other personnel, rather than end users. I don't want my users changing file and folder permissions, they should ask IT to handle it. File permissions may need to be managed/handled by other personnel, rather than end users.
Skill in managing cookie settings and usage	80%	How OISUs manage cookie settings and usage is not important enough to assess, if they even have the privilege to manage. Cookie settings and usage are of little to no concern. I'm not interested in how users may or may not manage cookies. Why are cookies a factor? They should be managed by policy.
Skill in using encryption to store data on approved removable media	20%	End-users should not be doing these types of data transfers.
Skill in peer-to-peer software usage without exploitation by transferring copyrighted materials, sensitive information, or PII	40%	Only essential and trained personnel should be allowed to use P2P software. Disagree with using P2P, orgs should not allow any P2P for end users.
Skill in using encryption to transmit sensitive information and PII when using Webmail	20%	Need to assess the avoidance of PII or sensitive information in Webmail, but encryption in Webmail is not necessary.

In summary, based on the semi-structured SME interviews, the following three KSAs were removed from the Phase 1 instrument: advanced written comprehension ability, knowledge of using file permissions, and skill in managing cookie settings & usage. Additionally, KCT6 was added to ‘knowledge of cyber threats’, which was defined as ‘possess knowledge regarding a ransomware attack’. Furthermore, SIR2 was added to ‘skill in cybersecurity incident reporting’, which was defined as ‘demonstrate the task of reporting a ransomware attack’.

Phase 1

Over a two-week period, the Phase 1 survey instrument was sent to 172 SMEs and collected 30 responses for a 17.4% response rate. The SMEs validated three cybersecurity abilities, 21 knowledge units, and 20 skill areas that are critical for the cybersecurity competency assessment of an OISU. To be validated, 70% of the SMEs were required to rate a KSA as ‘moderately important’, or five on a seven point Likert scale. The cybersecurity KSAs that were found in literature as well as USG documents, but not validated by the SMEs were: near vision ability, knowledge of smart card risks, knowledge of Webmail, skill in peer-to-peer software usage without exploitation by transferring copyrighted materials/sensitive information/PII, and skill in labeling removable media that contains sensitive information or PII.

Pre-Analysis Data Screening

Pre-analysis data screening did not identify any SME responses that needed to be removed. No responses sets were identified, and no malicious responses were submitted.

No incomplete data sets were submitted, as designed, due to all survey items being set as 'required' when developing the instrument.

Demographic Analysis

Upon completing pre-analysis data screening, demographic analysis was performed on the collected data to assess the sample. Phase 1 achieved the goal of ensuring that respondents were evenly split between federal government and private sector employees. A summary of the demographic data is shown in Table 10.

Table 10.

Summary of Phase 1 Demographic Data

Group	Frequency	Percentage
Age		
20-29	3	10%
30-39	9	30%
40-49	15	50%
50-59	2	7%
Over 60	1	3%
Gender		
Female	3	10%
Male	27	90%
Job function		
Cybersecurity/IT Staff	18	60%
Engineer	3	10%
Manager	6	20%
Operations	2	7%
Teacher/Professor	1	3%
Time with employer		
Under 1 year	6	20%
1-5 years	16	53%
6-10 years	4	13%
11-15 years	2	7%
16-20 years	2	7%
Employment sector		
Academia	2	7%
Federal government	12	40%
Private sector	12	40%
Other	4	13%

Data Analysis

The primary goal of Phase 1 data analysis was to determine if SMEs accepted or rejected the cybersecurity KSAs for OISUs that were found in literature and USG documents. Additionally, data analysis for Phase 1 consisted of computing levels of dispersion. Determining the levels of dispersion required the computation of standard deviations and the means.

To accept a proposed KSA, 70% of the SMEs are required to rate the KSA as 'moderately acceptable', or five on a seven point Likert scale. As shown in Figure 9, five KSAs did not meet the acceptance criteria. Table 11 shows the levels of dispersion.

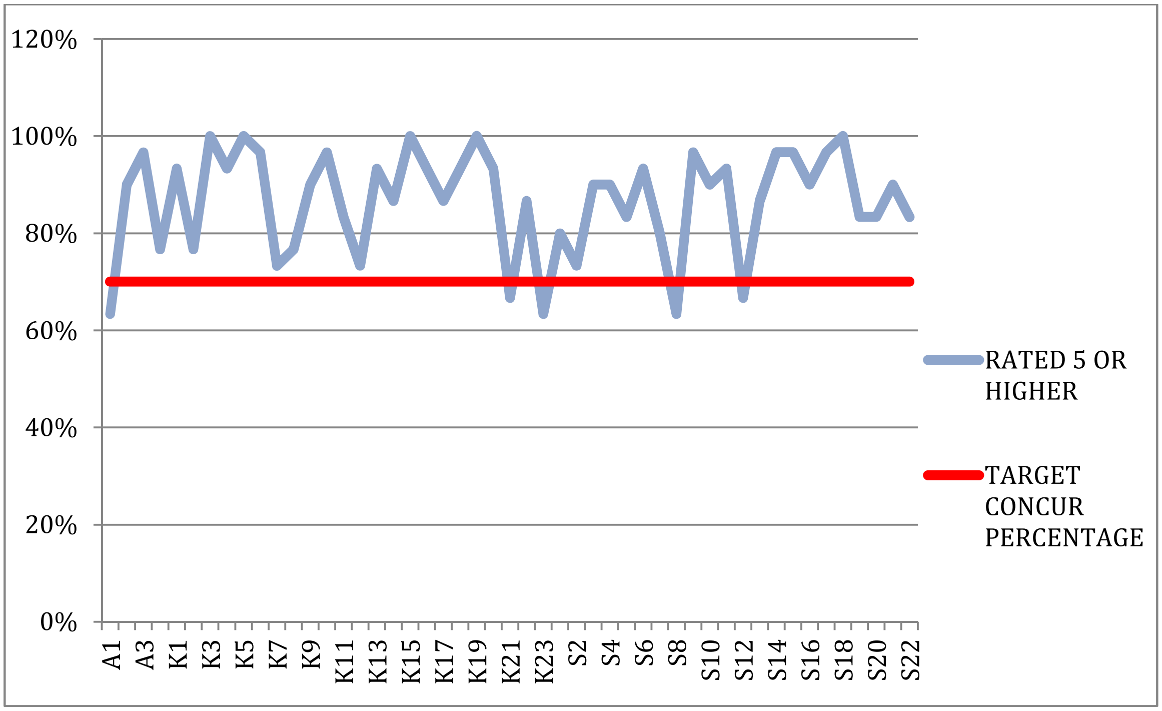


Figure 9. Summary of KSAs validated by SMEs in Phase 1

Table 11.

Summary of Phase 1 Levels of Dispersion

KSA	STD DEV	MEAN	RATED 5 OR HIGHER
A1	1.5	4.6	**63%**
A2	1.1	6.0	90%
A3	0.8	5.9	97%
A4	1.4	5.1	77%
K1	1.3	6.0	93%
K2	1.3	5.0	77%
K3	0.8	6.4	100%
K4	1.4	6.1	93%
K5	0.7	6.2	100%
K6	1.1	6.2	97%
K7	1.4	5.1	73%
K8	1.6	5.3	77%
K9	1.1	6.0	90%
K10	0.8	6.2	97%
K11	1.2	5.9	83%
K12	1.8	5.3	73%
K13	1.4	5.9	93%
K14	1.5	5.4	87%
K15	0.7	6.5	100%
K16	1.3	5.7	93%
K17	1.3	5.7	87%
K18	1.0	6.2	93%
K19	0.7	6.6	100%
K20	1.0	5.9	93%
K21	1.7	4.7	**67%**
K22	1.5	5.7	87%
K23	1.6	4.5	**63%**
S1	1.5	5.7	80%
S2	1.6	5.1	73%
S3	1.2	5.9	90%
S4	1.3	5.9	90%
S5	1.4	5.4	83%
S6	1.0	6.2	93%
S7	1.5	5.6	80%
S8	1.4	5.0	**63%**
S9	0.8	6.6	97%
S10	1.2	5.9	90%
S11	1.0	5.9	93%
S12	1.4	5.2	**67%**
S13	1.2	6.0	87%
S14	0.9	6.1	97%
S15	0.8	6.5	97%
S16	1.2	6.1	90%
S17	0.8	6.5	97%
S18	0.8	6.1	100%
S19	1.6	5.5	83%
S20	1.2	5.7	83%
S21	1.2	6.2	90%
S22	1.5	6.1	83%

The KSAs that were not accepted were: A1, K21, K23, S8, and S12 as shown in Figure 9 and Table 11. The levels of dispersion, shown in Table 11, did not reveal any problematic KSA measures due to a wide range of responses. The rejection of five KSAs is a due to the requirement of 70% of the SMEs rating a KSA at five (moderately important) or higher for acceptance, not due to problematic levels of dispersion. It is assumed that the strength of the KSAs is due to the KSAs being grounded in literature and USG documents.

Phase 2

Round 1

Over a four-week period, the Phase 2 Round 1 survey instrument was sent to 398 SMEs and collected 16 responses for a 4% response rate. The SMEs validated 60 of 90 KSA measurement methods. To be validated, 70% of the SMEs were required to rate a KSA as 'slightly acceptable', or five on a seven point Likert scale. However, if SMEs provided reasoned arguments as to why a KSA measurement method should be reworked, the KSA measurement method may not be accepted regardless of the rating achieved. Additionally, if 70% of the SMEs rated items at five or above, but identified typographical errors, the errors will be corrected and the KSA measurement method is considered as accepted due to consensus.

Pre-Analysis Data Screening

Pre-analysis data screening did not identify any SME responses that needed to be removed. No responses sets were identified, and no malicious responses were submitted.

No incomplete data sets were submitted, as designed, due to all survey items being set as ‘required’ when developing the instrument.

Demographic Analysis

Upon completing pre-analysis data screening, demographic analysis was performed on the collected data to assess the sample. Phase 2 Round 1 demographic data shows that respondents were evenly split between federal/state government and private sector employees. A summary of the demographic data is shown in Table 12.

Table 12

Summary of Phase 2 Round 1 Demographic Data

Group	Frequency	Percentage
Age		
30-39	1	6.25%
40-49	9	56.2%
50-59	6	37.75%
Gender		
Female	3	19%
Male	13	81%
Job function		
Cybersecurity/IT Staff	8	50%
Engineer	1	6.25%
Manager	4	25%
Scientist	1	6.25%
Teacher/Professor	1	6.25%
Technical staff	1	6.25%
Time with employer		
Under 1 year	4	25%
1-5 years	8	50%
6-10 years	3	18.75%
Over 30 years	1	6.25%
Employment sector		
Academia	2	12.5%
Federal government	5	31.25%
Private sector	6	37.5%
Other	2	12.5%
State government	1	6.25%

Data Analysis

For the Phase 2 Round 1 survey, KCT1 was the only KSA measurement method that did not achieve a rating of five or higher by 70% of the SMEs, as shown in Figure 10. However, due to qualitative feedback, 28 additional KSA measurement methods were selected for rework based on the SME recommendations. A summary of the KSA measurement methods identified for rework via qualitative data is shown in Table 13. Table 14 shows the Phase 2 Round 1 levels of dispersion.

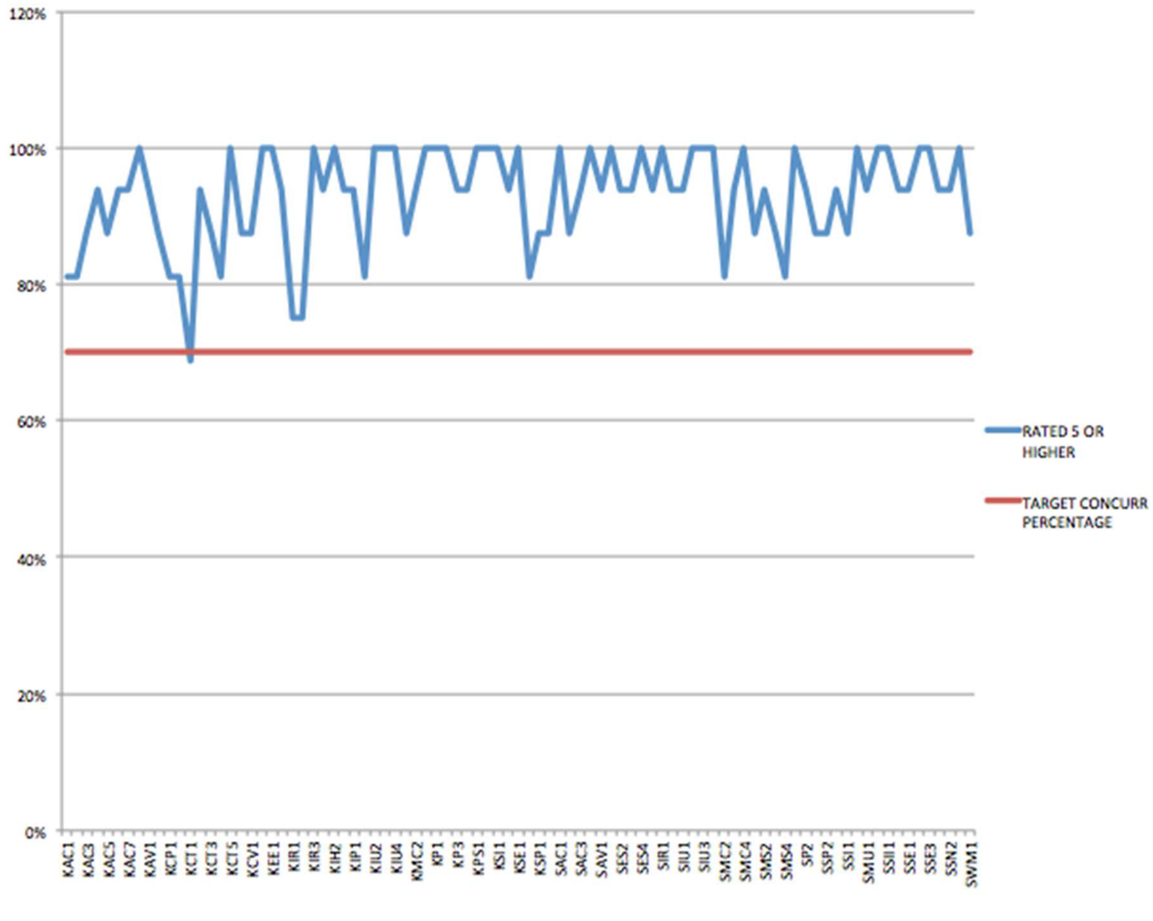


Figure 10. Summary of KSAs validated by SMEs in Phase 2 Round 1

Table 13.

Summary of Phase 2 Round 1 Qualitative Results

KSA	Qualitative Feedback	Corrective Action
KAC1	Secure safe for admin passwords.	Discourage writing down passwords, unless secured in a safe.
KAC2	Changing it daily is just as bad as never.	Set points for 'daily' to the same points as 'never', which is zero points.
KAC3	Rephrase C to read "To perform a critical work related function".	Rephrased option C to read, "To perform a critical work related function".
KAC5	A) Seems OK as stated, but I wonder if you need to add "...for guidance" to clarify you're not suggesting contacting them to file some sort of incident.	Added "for guidance" to option A.
KAC5	Answer C could be better.	Changed option C to "Do not allow the visitor to use your computer".
	Answer C, "Call the police" seems not relevant.	Changed option C to "Do not allow the visitor to use your computer".
KAC6	This is perhaps too subtle, but the phrasing of A. B, and C seems very black and white. I'm not sure if you should modify with "...is primarily..." to get at your likely intent here.	Added "is primarily" to all options.
	This is acceptable, but I think the answers need tweaking as it may confuse the people. Maybe something along the lines of "Allowing access to my computer" instead of say access control.	Reworded from "Access control to you computer" to "Who sits at your computer".
KCP1	I found C and D to both be answers to this question, so you're actually asking a prioritization question... if your intent is to provide only one right answer to the question then I would modify C at a minimum - or adjust the question to reflect prioritization.	Reworded "phishing email" to "an email from an unknown source.
KCR1	Updating software is not a user function and introduces a lot of risk by giving them admin rights to update the software.	Changed "Updating software when needed" to "Protecting personally identifiable information (PII)".
	Last one is dependent on group IT security policies.	Changed "Updating software when needed" to "Protecting personally identifiable information (PII)".

Table 13.

Summary of Phase 2 Round 1 Qualitative Results (continued)

KSA	Qualitative Feedback	Corrective Action
KCR1	Updating software when needed is not usually a user responsibility; usually an IT function.	Changed “Updating software when needed” to “Protecting personally identifiable information (PII)”.
KCT1	Response E should not be valued at 2 points.	Changed points for option E to zero.
KCT2	C & D are misleading for T/F question.	Reworded the questions from “true” to “most true”. Also changed points for option C to two, changed points for option D to one.
KCT3	Why only partial points for D? They can be effective sometimes. They are not always effective. So D is an accurate answer.	Changed option D from “Phishing attacks can be effective sometimes (4 points)” to Phishing attacks may attempt to gain your access credentials (10 points).
KCT4	Don't agree main purpose of spam is identity theft.	Changed question from “What is the purpose of SPAM?” to “What is a purpose of SPAM?”
KCT5	Review points for D. B and D should be weighted equal.	Set the points for options B and D to two.
KCT6	D should get some points.	Set the points for options A and D to two.
	A and D may deserve to get some points.	Set the points for options A and D to two.
KIR1	Double negatives should be avoided.	Changed “ not acceptable to not report” to “acceptable to report”.
KIH1	Here, as you've done in other questions, is probably one that should be phrased as which "is the best method"... and the question is phrased in plural form, but you're asking for one answer.	Reworded to “What is the desired method”.
KIH3	In the last item, perhaps instead of "...is a major...” maybe better to say "...may be a major...” because "is" is so global and definitive but it will really depend on the data.	Changed to “may be a major”.
KIP1	Liability determination is usually based on court ruling.	Changed uses of “liable” to “liable in court”.
KIU1	I think personal devices would also be discouraged because you are on company time	Reworded as “personal device” to “personal device, during a break if allowed”.

Table 13.

Summary of Phase 2 Round 1 Qualitative Results (continued)

KSA	Qualitative Feedback	Corrective Action
KIU1	The last question could lead to meaning it's acceptable to user your personal device on company network.	Reworded as “personal device” to “personal device, during a break if allowed”.
	Depends from company policies.	Reworded as “personal device” to “personal device, during a break if allowed”.
KSI1	A marriage license is public information in most states	Replaced “marriage license” with “social security number”.
	As one can look up marriage licenses on county clerks' websites, I thought it wasn't sensitive.	Replaced “marriage license” with “social security number”.
	Marriage license information may not be sensitive in FLA.	Replaced “marriage license” with “social security number”.
KSI2	Mothers maiden name by itself is not PII.	Replaced “Mothers maiden name” with “Driver’s license number”.
KSN1	Here I would probably put more repercussions such as harm to the employer etc.	Changed options A, B, and C to three points. Changed option D to ten points. Replaced option C with “You can be convicted, depending on the nature of the offense”.
	Can be convicted, depending on the nature.	Changed options A, B, and C to three points. Changed option D to ten points. Replaced option C with “You can be convicted, depending on the nature of the offense”.
KSP1	I would reword to say "combination of" vs. "consisting of". It could be misread as requiring an equal number of each item.	Replaced uses of “consisting of” with “combination of”.
SAC2	Removing a PKI card does not automatically lock your workstation unless configured through the computer/domain security policy.	Removed the option of “Removing PKI card”.
SES3	Replying to the sender should not be a valid option since email may be spoofed or an in-house software engineer might be at work. Besides IT Policy shall forbid chain emails to reduce risk and increase productivity.	Corrected the points to zero when forwarding the chain mail.
SES5	Depending on the email client (Outlook) their may be no option to scan. Also, from a technical standpoint, it would be impossible to scan until it is downloaded.	Reworded option to “Immediately run a virus scan on the PDF file after downloading.” Added the option to ask a supervisor for assistance for four points.

Table 13.

Summary of Phase 2 Round 1 Qualitative Results (continued)

KSA	Qualitative Feedback	Corrective Action
SMS1	Closing the laptop is acceptable.	Changed the points for closing the laptop to 10.
	Closing the laptop should lock it.	Changed the points for closing the laptop to 10.
	Closing laptop usually is same as locking.	Changed the points for closing the laptop to 10.
SMS4	Probably 10 points for shutdown.	Changed the points for shutting down the laptop to 10.
	Shut down is acceptable	Changed the points for shutting down the laptop to 10.
	In my opinion, shutting down the laptop is a better choice	Changed the points for shutting down the laptop to 10.
	If you shut down the laptop while out for lunch, 2 points are awarded - more correct answer.	Changed the points for shutting down the laptop to 10.
SSI1	Clarify taking the CD home to work on your personal workstation.	Clarified that taking the disk home will be to work on the assignment at home.
SWM1	If you do not send the email and report to security, some points may be awarded.	Changed the points for not sending the email and reporting the incident to 10.

Table 14.

Summary of Phase 2 Round 1 Levels of Dispersion

KSA	STD DEV	MEAN	RATED 5 OR HIGHER
KAC1	1.53	5.8	81%
KAC2	1.54	5.4	81%
KAC3	0.93	6.1	88%
KAC4	0.86	6.3	94%
KAC5	1.29	5.8	88%
KAC6	1.21	6.0	94%
KAC7	1.06	6.3	94%
KAC8	0.51	6.4	100%
KAV1	1.09	5.9	94%
KAV2	1.06	6.1	88%
KCP1	1.63	5.5	81%
KCR1	1.13	5.8	81%
KCT1	1.75	5.1	69%
KCT2	0.95	5.7	94%
KCT3	0.93	5.8	88%
KCT4	1.78	5.3	81%

Table 14.

Summary of Phase 2 Round 1 Levels of Dispersion (continued)

KSA	STD DEV	MEAN	RATED 5 OR HIGHER
KCT5	0.62	5.9	100%
KCT6	1.06	6.1	88%
KCV1	1.24	5.9	88%
KCV2	0.68	6.3	100%
KEE1	0.63	6.5	100%
KEU1	0.85	6.1	94%
KIR1	1.71	5.5	75%
KIR2	1.78	5.4	75%
KIR3	0.70	6.3	100%
KIH1	1.06	6.1	94%
KIH2	0.68	6.3	100%
KIH3	1.09	5.9	94%
KIP1	0.87	6.3	94%
KIU1	1.28	5.8	81%
KIU2	0.58	6.3	100%
KIU3	0.77	6.3	100%
KIU4	0.72	6.4	100%
KMC1	1.05	6.2	88%
KMC2	0.89	6.4	94%
KPR1	0.60	6.3	100%
KP1	0.72	6.1	100%
KP2	0.63	6.5	100%
KP3	1.03	6.0	94%
KP4	1.10	6.0	94%
KPS1	0.48	6.3	100%
KPC1	0.77	6.3	100%
KSI1	0.72	6.4	100%
KSI2	0.87	6.3	94%
KSE1	0.75	6.2	100%
KSN1	1.31	5.9	81%
KSP1	1.03	6.0	88%
SSTP1	1.02	5.9	88%
SPR1	1.02	5.9	88%
SAC1	0.68	6.1	100%
SAC2	1.17	5.8	88%
SAC3	0.77	6.1	94%
SPS1	0.68	6.3	100%
SAV1	0.89	5.9	94%
SES1	0.68	6.3	100%
SES2	0.93	5.9	94%
SES3	1.26	5.9	94%
SES4	0.81	6.1	100%
SES5	1.06	6.1	94%
SIR1	0.70	6.3	100%
SIR2	1.31	6.1	94%
SIU1	0.77	5.9	94%
SIU2	0.73	6.0	100%
SIU3	0.62	6.1	100%

Table 14.

Summary of Phase 2 Round 1 Levels of Dispersion (continued)

KSA	STD DEV	MEAN	RATED 5 OR HIGHER
SMC1	0.68	6.1	100%
SMC2	1.28	5.8	81%
SMC3	1.06	6.1	94%
SMC4	0.58	6.3	100%
SMS1	1.03	6.0	88%
SMS2	1.09	5.9	94%
SMS3	1.02	5.9	88%
SMS4	1.15	5.6	81%
SP1	0.81	6.1	100%
SP2	0.77	6.1	94%
SSP1	1.18	5.9	88%
SSP2	1.15	5.9	88%
SW1	0.83	6.2	94%
SSI1	1.02	5.9	88%
SSI2	0.68	6.3	100%
SMU1	0.93	6.1	94%
SMU2	0.77	6.1	100%
SSII1	0.60	6.3	100%
SSII2	0.83	6.2	94%
SSE1	1.26	6.0	94%
SSE2	0.70	6.3	100%
SSE3	0.73	6.0	100%
SSN1	0.85	5.9	94%
SSN2	1.29	5.9	94%
SS1	0.68	6.3	100%
SWM1	1.44	5.8	88%

The KSAs that were not accepted were: KAC1, KAC2, KAC3, KAC5, KAC6, KCP1, KCR1, KCT1, KCT2, KCT3, KCT4, KCT5, KCT6, KIR1, KIH1, KIH3, KIP1, KIU1, KSI1, KSI2, KSN1, KSP1, SAC2, SES3, SES5, SMS1, SMS4, SSI1, and SWM1 as shown in Figure 10 and Table 13. The levels of dispersion did not reveal any problematic KSAs due to a wide range of responses. Accordingly, nearly all of the KSA measurement methods evaluated by the SMEs met the acceptance criteria of having achieved a rating of five or higher by 70% of the SMEs. The only KSA that did not meet the quantitative acceptance criteria was KCT1, and it missed the requirement by one percentage point. However, while virtually all of the KSA measurement methods were by the SMEs, the qualitative data that was received provided the opportunity to improve the KSA measurement methods even further. Using the results and data analysis from Phase 2 Round 1, the Phase 2 Round 2 instrument was developed to rework and validate the previously highlighted KSA measures. The contact form to SMEs for Phase 2 Round 2 is shown in Appendix D.

Round 2

Over a two-week period, the Phase 2 Round 2 survey instrument was sent to 12 SMEs and received the targeted number of seven responses, for a 58% response rate. The SMEs validated all 29 of the presented KSA measurement methods. To be validated, 70% of the SMEs were required to rate a KSA as 'slightly acceptable', or five on a seven point Likert scale. The SMEs did not provide any reasoned arguments as to why a KSA measurement method should be reworked.

Pre-Analysis Data Screening

Pre-analysis data screening did not identify any SME responses that needed to be removed. No responses sets were identified, and no malicious responses were submitted. No incomplete data sets were submitted, as designed, due to all survey items being set as 'required' when developing the instrument.

Demographic Analysis

Upon completing pre-analysis data screening, demographic analysis was performed on the collected data to assess the sample. Phase 2 Round 2 respondents were evenly split between federal government and private sector employees. A summary of the demographic data is shown in Table 15.

Table 15

Summary of Phase 2 Round 2 Demographic Data

Group	Frequency	Percentage
Age		
40-49	5	71.4%
50-59	2	28.6%
Gender		
Female	2	28.6%
Male	5	71.4%
Job function		
Cybersecurity/IT Staff	4	57.1%
Manager	2	28.6%
Scientist	1	14.3%
Time with employer		
Under 1 year	1	14.3%
1-5 years	4	57.1%
6-10 years	2	28.6%
Employment sector		
Academia	1	14.3%
Federal government	3	42.85%
Private sector	3	42.85%

Data Analysis

For the Phase 2 Round 2 survey, all 29 of the presented KSA measurement methods were accepted by achieving a rating of five or higher by 70% of the SMEs, as shown in Figure 11. No reasoned arguments were provided that necessitated any further amendments to the remaining 29 KSA measurement methods. Therefore, the amended KSA measures shown in Appendix F were all accepted.

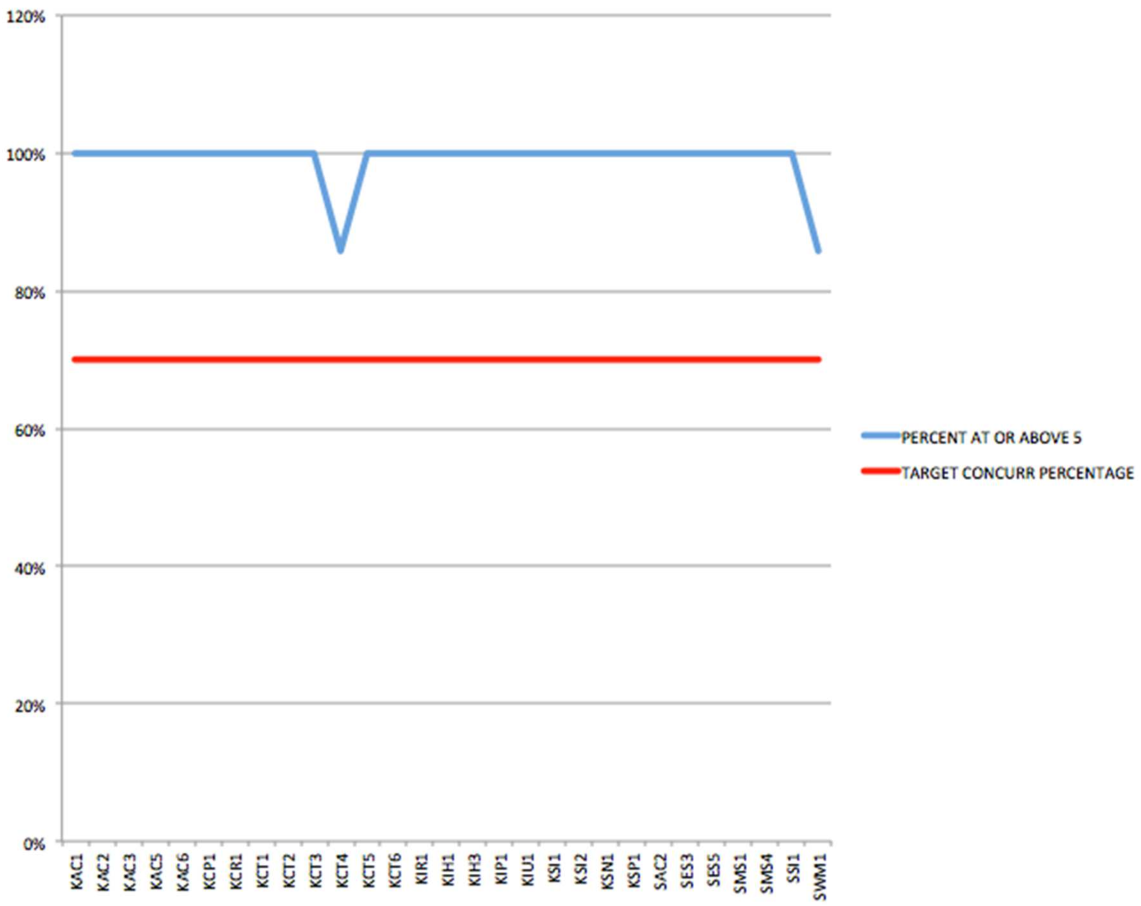


Figure 11. Summary of KSAs validated by SMEs in Phase 2 Round 2

Table 16.

Summary of Phase 2 Round 2 Levels of Dispersion

KSA	STDEV	MEAN	RATED 5 OR HIGHER
KAC1	0.0	7.0	100%
KAC2	0.5	6.4	100%
KAC3	0.4	6.9	100%
KAC5	0.0	7.0	100%
KAC6	0.5	6.3	100%
KCP1	0.6	6.0	100%
KCR1	0.4	6.9	100%
KCT1	0.5	6.4	100%
KCT2	0.4	6.1	100%
KCT3	0.4	6.9	100%
KCT4	2.2	5.9	86%
KCT5	0.4	6.1	100%
KCT6	0.4	6.9	100%

Table 16.

Summary of Phase 2 Round 2 Levels of Dispersion (continued)

KSA	STDEV	MEAN	RATED 5 OR HIGHER
KIR1	0.5	6.6	100%
KIH1	0.0	7.0	100%
KIH3	0.5	6.7	100%
KIP1	0.0	7.0	100%
KIU1	0.5	6.3	100%
KSI1	0.5	6.4	100%
KSI2	0.5	6.6	100%
KSN1	0.4	6.9	100%
KSP1	0.7	6.1	100%
SAC2	0.8	6.3	100%
SES3	0.4	6.1	100%
SES5	0.6	6.0	100%
SMS1	0.6	6.0	100%
SMS4	0.7	6.1	100%
SSI1	0.5	6.3	100%
SWM1	1.7	5.7	86%
KAC1	0.0	7.0	100%
KAC2	0.5	6.4	100%
KAC3	0.4	6.9	100%
KAC5	0.0	7.0	100%

The levels of dispersion, as shown in Table 16, did not reveal any problematic KSAs due to a wide range of responses. Additionally, all 29 of the KSA measurement methods evaluated by the SMEs met the acceptance criteria of having achieved a rating of five or higher by 70% of the SMEs. Figure 12 illustrates the improvement of SMEs ratings from Phase 2 Round 1 to Phase 2 Round 2. By using Phase 2 Round 2 to improve the KSA measurement methods, all of the KSA measurement methods were accepted by the SMEs and Phase 3 of this study was initiated.

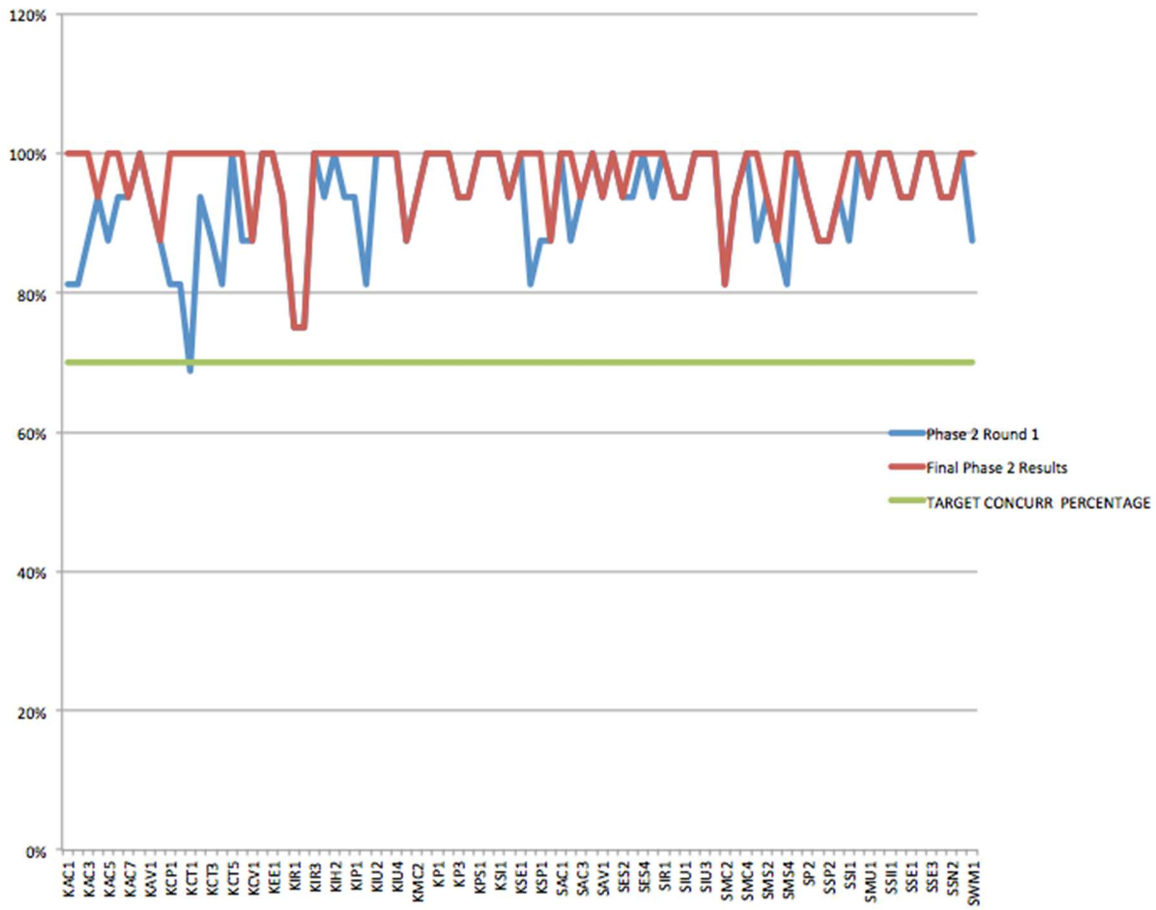


Figure 12. Summary of Phase 2 Round 1 compared to the Phase 2 Final Results

Phase 3

Over an eight-day period, the Phase 3 survey instrument was sent to 54 SMEs and collected 15 responses for a 28% response rate. The SMEs proposed and validated weights for the four KCs (ASKC, ISKC, INSKC, PSKC), four SCs (ASSC, ISSC, INSSC, PSSC), OK, and OS. The SMEs were asked to divide 100 points among the four KCs, which were averaged and used as the KC weights. The SMEs were also asked to divide 100 points among the four SCs, which were averaged and used as the SC weights. Additionally, the SMEs were asked to divide 100 points between OK and OS, which were averaged and used as the OK and OS weights.

Pre-Analysis Data Screening

Pre-analysis data screening did not identify any SME responses that needed to be removed. No responses sets were identified, and no malicious responses were submitted. No incomplete data sets were submitted, as designed, due to all survey items being set as 'required' when developing the instrument.

Demographic Analysis

Upon completing pre-analysis data screening, demographic analysis was performed on the collected data to assess the sample. Respondents were almost evenly split between federal government and private sector employees. A summary of the demographic data is shown in Table 17.

Table 17.

Summary of Phase 3 Demographic Data

Group	Frequency	Percentage
Age		
20-29	1	7%
30-39	1	7%
40-49	9	60%
50-59	4	26%
Gender		
Female	3	20%
Male	12	80%
Job function		
Cybersecurity/IT Staff	11	73%
Engineer	1	7%
Manager	2	13%
Scientist	1	7%
Time with employer		
Under 1 year	2	13%
1-5 years	9	60%
6-10 years	3	20%
Over 30 years	1	7%
Employment sector		
Academia	1	7%
Federal government	6	40%
Private sector	7	46%
Other	1	7%

Data Analysis

For the Phase 3 survey, the SMEs submitted weights for KCs, SCs, OK, and OS. The SMEs submissions were then averaged to form the applicable weights. The SMEs did not submit any qualitative feedback regarding any of the Phase 3 parameters. The results of Phase 3 are shown in Table 18. The Phase 3 levels of dispersion are shown in Table 19.

Table 18.

Summary of Phase 3 Results

Item	**Weight**
ASKC	21.8%
ISKC	27.6%
INSKC	27.3%
PSKC	23.3%
ASSC	22.7%
ISSC	26.3%
INSSC	27.6%
PSSC	23.4%
OK	46.1%
OS	53.9%

Table 19.

Summary of Phase 3 Levels of Dispersion

Item	**STDEV**	**MEAN**
ASKC	3.6	21.8
ISKC	2.9	27.6
INSKC	4.5	27.3
PSKC	3.9	23.3
ASSC	2.7	22.7
ISSC	3.0	26.3
INSSC	4.9	27.6
PSSC	2.8	23.4
OK	5.5	46.1
OS	5.5	53.9

The levels of dispersion, as shown in Table 19, did not reveal any problematic dispersion levels from the SME responses. The responses proposed by the SMEs did not show any statistical reason to reject the computed weights. Additionally, the SMEs did not submit qualitative feedback. Therefore the weights were accepted and Phase 4 of this study was initiated.

Phase 4

Over a five-day period, the Phase 4 survey instrument was sent to 39 SMEs and collected 15 responses for a 38% response rate. The SMEs proposed and validated the OISU cybersecurity competency threshold. The SMEs were asked to propose an overall percentage score between 1-100% for an OISU cybersecurity competency threshold. SME responses were then assessed and averaged to produce an OISU cybersecurity competency threshold.

Pre-Analysis Data Screening

Pre-analysis data screening did not identify any SME responses that needed to be removed. No responses sets were identified, and no malicious responses were submitted. No incomplete data sets were submitted, as designed, due to all survey items being set as 'required' when developing the instrument.

Demographic Analysis

Upon completing pre-analysis data screening, demographic analysis was performed on the collected data to assess the sample. Phase 4 respondents were almost evenly split between federal government and private sector employees. A summary of the demographic data is shown in Table 20.

Table 20

Summary of Phase 4 Demographic Data

Group	Frequency	Percentage
Age		
20-29	1	6.7%
30-39	1	6.7%
40-49	9	60%
50-59	3	20%
Over 60	1	6.7%
Gender		
Female	3	20%
Male	12	80%
Job function		
Cybersecurity/IT Staff	11	73.3%
Engineer	1	6.7%
Manager	2	13.3%
Scientist	1	6.7%
Time with employer		
Under 1 year	1	6.7%
1-5 years	11	73.3%
6-10 years	1	6.7%
16-20 years	1	6.7%
Over 30 years	1	6.7%
Employment sector		
Academia	1	6.7%
Federal government	5	33.3%
Private sector	7	46.7%
Other	2	13.3%
Education		
4-year degree (Bachelors	1	6.7%
Degree)	11	73.3%
Graduate degree	3	20%
Doctorate		

Data Analysis

For the Phase 4 survey, the SMEs provided their expert view on what percentage score needed to be achieved to reach the OISU cybersecurity competency threshold. The results of Phase 4 determined the OISU cybersecurity competency threshold is 80%. The Phase 4 levels of dispersion are shown in Table 21.

Table 21.

Summary of Phase 4 Levels of Dispersion

Item	STDEV	MEAN
OISU Cybersecurity Competency Threshold	4.2	80.0

The levels of dispersion, as shown in Table 21, did not reveal any problematic response levels from the SME. The responses proposed by the SMEs did not show any statistical reason to reject the computed OISU cybersecurity competency threshold of 80%. Additionally, the SMEs did not submit any qualitative feedback that required data analysis. Therefore the threshold value was accepted and Phase 5 of this study was initiated.

Phase 5

Over an eight-day period, the MyCyberKSAs^{TM} prototype tool was distributed to approximately 569 OISUs and collected 54 responses for a 9% response rate. The required sample of 50 OISUs for this Phase is not large enough to perform analysis investigating statistical significance of multivariate factors. However, using the 50 OISU sample allowed for data analysis of cybersecurity competency by each demographic group. Data analysis for Phase 5 gave the ability to judge the effectiveness or ineffectiveness of the MyCyberKSAs^{TM} prototype tool, to determine if RQ5 of this study had been met.

Pre-Analysis Data Screening

Pre-analysis data screening did not identify any OISU responses that needed to be removed. No responses sets were identified, and no malicious responses were submitted. Additionally, no incomplete data sets were submitted.

Demographic Analysis

Upon completing pre-analysis data screening, demographic analysis was performed on the collected data to assess the sample. Respondents were unintentionally evenly split between female and male OISUs. A summary of the demographic data is shown in Table 22.

Table 22

Summary of Phase 5 Demographic Data

Group	**Frequency**	**Percentage**
Age		
20-29	3	5.5%
30-39	15	27.8%
40-49	23	42.6%
50-59	9	16.7%
Over 60	4	7.4%
Gender		
Female	27	50%
Male	27	50%
Job function		
Administrative staff	5	9.3%
Cybersecurity/IT staff	3	5.6%
Engineer	5	9.3%
Manager	6	11.1%
Medical/Veterinary	5	9.3%
Operations	3	5.6%
Professional staff	4	7.4%
Retail	1	1.8%
Scientist	2	3.7%
Technical staff	1	1.8%
Security operator	1	1.8%
Teacher/Professor	5	9.3%
Other	13	24.0%

Table 22

Summary of Phase 5 Demographic Data (continued)

Group	Frequency	Percentage
Time with employer		
Under 1 year	6	11.1%
1-5 years	18	33.3%
6-10 years	10	18.5%
11-15 years	11	20.4%
16-20 years	5	9.3%
21-25 years	2	3.7%
Over 30 years	2	3.7%
Education		
High school diploma	15	27.8%
2-year degree (Associates degree)	10	18.5%
4-year degree (Bachelors degree)	16	29.6%
Graduate degree	11	20.4%
Other	2	3.7%
Cybersecurity certified		
No	47	87%
Yes	7	13%
Annual cybersecurity training		
No	34	63%
Yes	20	37%

Data Analysis

In Phase 5, this study recruited 54 OISUs test participants that fully completed the MyCyberKSAs^{TM} prototype assessment tool. The OISU cybersecurity competency threshold for the MyCyberKSAs^{TM} prototype assessment tool was defined as an overall score that is greater than or equal to 80%. In this data analysis section, the KCs and SCs are not weighted. The values for OK and OS will be based on the weighted KCs and SCs, but will not have the OK and OS weights applied. The cybersecurity competency scores will be based on the weighted OK and OS scores, and those OK and OS scores are based on the weighted KCs and SCs. Table 23 shows cybersecurity competency scores for each OISU. As shown in Table 23, 37 of 54 (69%) OISUs were measured as possessing cybersecurity competency for organizational information systems. Additionally, Figure 13 illustrates the cybersecurity competency score for each OISU while displaying the OK and OS components. Figure 13 is a graphical representation of the data collected using a methodology based on the model shown in Figure 1. Due to mathematical complexities with normalization, Figure 13 stacks cybersecurity knowledge and skill to reach the cybersecurity competency threshold, instead of having cybersecurity knowledge and skill side-by-side.

Table 23

Summary of Phase 5 OISU Cybersecurity Competency Scores

Response	**Competency**	**Response**	**Competency**	**Response**	**Competency**
ID	**Score**	**ID**	**Score**	**ID**	**Score**
1	**83.81%**	21	**89.26%**	41	**80.58%**
2	**84.95%**	22	**81.92%**	42	**83.39%**
3	**89.70%**	23	**87.20%**	43	**94.98%**
4	**91.98%**	24	**83.95%**	44	**85.94%**
5	73.21%	25	79.36%	45	**85.32%**
6	69.98%	26	**89.14%**	46	**92.86%**
7	**83.04%**	27	**89.39%**	47	**86.94%**
8	67.08%	28	73.28%	48	**90.91%**
9	**84.65%**	29	60.59%	49	**85.25%**
10	75.57%	30	62.89%	50	**81.50%**
11	**83.88%**	31	79.78%	51	78.13%
12	**85.36%**	32	**89.52%**	52	48.37%
13	56.91%	33	**85.92%**	53	**85.72%**
14	**86.91%**	34	**92.28%**	54	**88.30%**
15	**90.80%**	35	78.07%		
16	**91.70%**	36	71.56%		
17	**80.98%**	37	70.30%		
18	**81.23%**	38	**85.94%**		
19	75.88%	39	**86.05%**		
20	**88.20%**	40	73.71%		

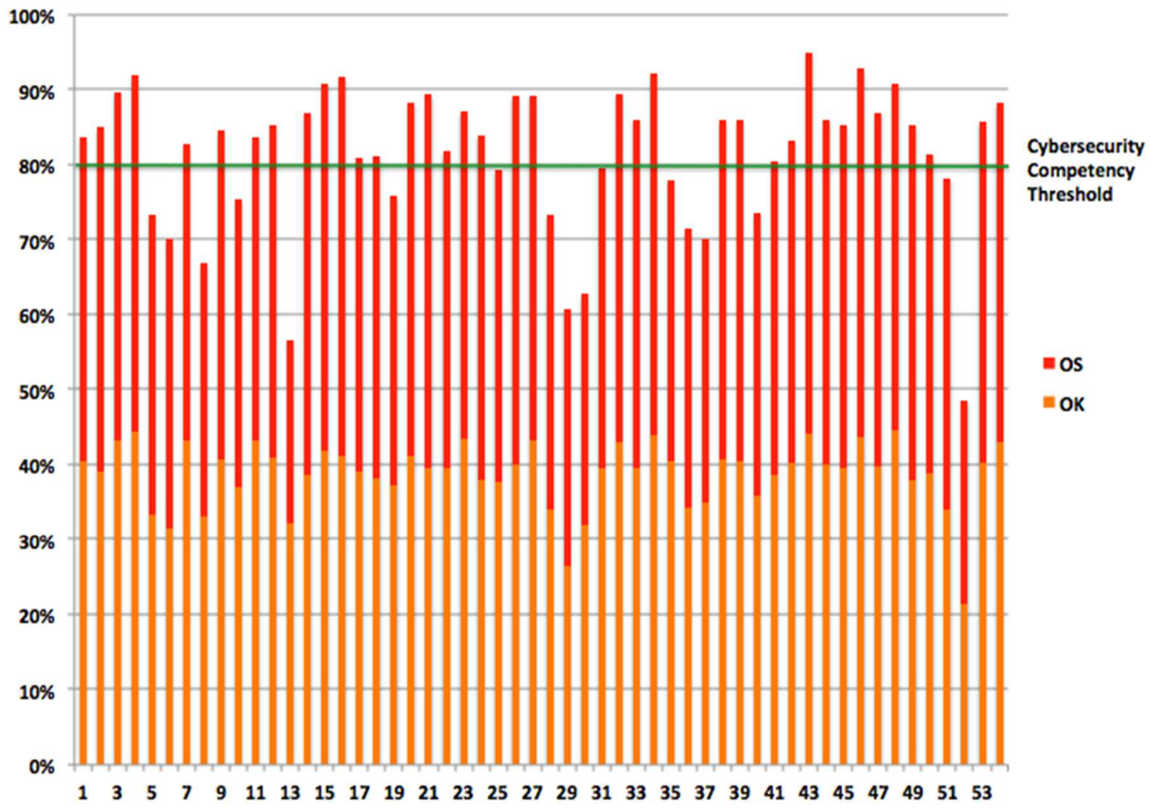


Figure 13. Summary of Phase 5 OISU Cybersecurity Competency Scores with OK and OS components (N = 54)

Table 24 shows the scores of the KCs, SCs, and cybersecurity competency for each OISU. To assess the OISU performance on the KCs and SCs, the percentages shown in Table 24 are not weighted. Additionally, the OK and OS values are not included in Table 24. The OK, OS, and cybersecurity competency scores for each OISU are shown in Table 25. Levels of dispersion were assessed for each demographic group and are presented in Figures 14 – 20.

Table 24

Summary of Phase 5 KCs, SCs, and Cybersecurity Competency Scores

Response									**Competency**
ID	**ASKC**	**ISKC**	**INSKC**	**PSKC**	**ASSC**	**ISSC**	**INSSC**	**PSSC**	**Score**
1	77%	95%	91%	85%	60%	78%	87%	95%	**83.81%**
2	87%	84%	85%	85%	58%	91%	100%	86%	**84.95%**
3	100%	96%	88%	91%	64%	89%	93%	95%	**89.70%**
4	100%	100%	86%	100%	80%	100%	88%	82%	**91.98%**
5	70%	85%	71%	60%	78%	63%	92%	62%	73.21%
6	50%	79%	59%	83%	58%	78%	65%	86%	69.98%
7	100%	95%	94%	85%	53%	91%	65%	83%	**83.04%**
8	67%	69%	72%	78%	42%	60%	70%	78%	67.08%
9	100%	82%	82%	92%	67%	100%	72%	86%	**84.65%**
10	70%	82%	82%	86%	57%	67%	68%	95%	75.57%
11	97%	100%	91%	86%	63%	89%	63%	85%	**83.88%**
12	100%	78%	94%	85%	70%	69%	100%	89%	**85.36%**
13	60%	75%	82%	57%	42%	38%	53%	48%	56.91%
14	60%	100%	88%	82%	73%	100%	93%	89%	**86.91%**
15	87%	87%	94%	95%	78%	100%	88%	95%	**90.80%**
16	90%	88%	88%	91%	84%	100%	100%	89%	**91.70%**
17	100%	65%	85%	95%	68%	69%	85%	88%	**80.98%**
18	70%	86%	86%	86%	56%	100%	75%	86%	**81.23%**
19	78%	76%	82%	88%	49%	58%	95%	80%	75.88%
20	100%	78%	90%	92%	76%	89%	97%	85%	**88.20%**
21	87%	81%	85%	91%	87%	91%	100%	91%	**89.26%**
22	90%	74%	88%	95%	60%	71%	93%	86%	**81.92%**
23	100%	90%	91%	98%	64%	82%	83%	92%	**87.20%**
24	97%	73%	87%	75%	88%	89%	77%	89%	**83.95%**
25	87%	90%	69%	83%	62%	80%	80%	85%	79.36%
26	97%	91%	68%	94%	100%	91%	87%	89%	**89.14%**
27	100%	100%	88%	88%	76%	91%	87%	86%	**89.39%**
28	57%	85%	65%	86%	38%	100%	72%	77%	73.28%
29	47%	46%	59%	78%	67%	50%	58%	83%	60.59%
30	70%	75%	68%	65%	58%	47%	57%	69%	62.89%
31	67%	86%	97%	89%	62%	89%	68%	77%	79.78%
32	100%	91%	89%	95%	73%	91%	88%	89%	**89.52%**
33	97%	84%	73%	94%	93%	80%	83%	89%	**85.92%**
34	100%	95%	91%	95%	89%	100%	93%	74%	**92.28%**

Table 24

Summary of Phase 5 KCs, SCs, and Cybersecurity Competency Scores (continued)

Response ID	ASKC	ISKC	INSKC	PSKC	ASSC	ISSC	INSSC	PSSC	Competency Score
35	100%	98%	81%	72%	82%	60%	70%	66%	78.07%
36	67%	70%	79%	82%	63%	67%	62%	86%	71.56%
37	73%	76%	72%	83%	52%	58%	68%	83%	70.30%
38	77%	100%	83%	92%	78%	89%	75%	94%	**85.94%**
39	100%	83%	79%	92%	64%	100%	87%	83%	**86.05%**
40	58%	81%	72%	100%	71%	44%	78%	89%	73.71%
41	67%	90%	82%	95%	69%	89%	67%	86%	**80.58%**
42	100%	86%	78%	86%	73%	78%	82%	88%	**83.39%**
43	100%	100%	91%	92%	93%	100%	93%	89%	**94.98%**
44	83%	79%	91%	95%	56%	100%	88%	92%	**85.94%**
45	83%	90%	83%	86%	78%	89%	83%	89%	**85.32%**
46	100%	91%	94%	95%	84%	100%	85%	95%	**92.86%**
47	90%	75%	86%	95%	70%	100%	88%	89%	**86.94%**
48	100%	100%	91%	97%	67%	100%	82%	92%	**90.91%**
49	67%	75%	88%	100%	76%	100%	88%	85%	**85.25%**
50	70%	90%	83%	92%	67%	80%	88%	78%	**81.50%**
51	75%	69%	72%	80%	76%	80%	93%	77%	78.13%
52	52%	52%	37%	46%	38%	36%	78%	45%	48.37%
53	87%	79%	92%	92%	84%	89%	82%	82%	**85.72%**
54	100%	95%	85%	94%	67%	89%	85%	94%	**88.30%**

Table 25

Summary of Phase 5 OK, OS, and Cybersecurity Competency Scores

Response ID	OK	OS	Competency Score	Response ID	OK	OS	Competency Score
1	88%	80%	**83.81%**	28	74%	73%	73.28%
2	85%	85%	**84.95%**	29	57%	64%	60.59%
3	94%	86%	**89.70%**	30	69%	57%	62.89%
4	96%	88%	**91.98%**	31	86%	74%	79.78%
5	72%	74%	73.21%	32	93%	86%	**89.52%**
6	68%	72%	69.98%	33	86%	86%	**85.92%**
7	94%	74%	**83.04%**	34	95%	90%	**92.28%**
8	72%	63%	67.08%	35	88%	69%	78.07%

Table 25

Summary of Phase 5 OK, OS, and Cybersecurity Competency Scores (continued)

Response			**Competency**	**Response**			**Competency**
ID	**OK**	**OS**	**Score**	**ID**	**OK**	**OS**	**Score**
9	88%	82%	**84.65%**	36	74%	69%	71.56%
10	80%	71%	75.57%	37	76%	65%	70.30%
11	94%	75%	**83.88%**	38	89%	84%	**85.94%**
12	89%	82%	**85.36%**	39	88%	85%	**86.05%**
13	70%	45%	56.91%	40	78%	70%	73.71%
14	84%	90%	**86.91%**	41	84%	78%	**80.58%**
15	91%	91%	**90.80%**	42	87%	80%	**83.39%**
16	89%	94%	**91.70%**	43	96%	94%	**94.98%**
17	85%	77%	**80.98%**	44	87%	85%	**85.94%**
18	83%	80%	**81.23%**	45	86%	85%	**85.32%**
19	81%	71%	75.88%	46	95%	91%	**92.86%**
20	89%	87%	**88.20%**	47	86%	88%	**86.94%**
21	86%	93%	**89.26%**	48	97%	86%	**90.91%**
22	86%	78%	**81.92%**	49	82%	88%	**85.25%**
23	94%	81%	**87.20%**	50	84%	79%	**81.50%**
24	82%	85%	**83.95%**	51	74%	82%	78.13%
25	82%	77%	79.36%	52	46%	50%	48.37%
26	87%	91%	**89.14%**	53	87%	84%	**85.72%**
27	94%	85%	**89.39%**	54	93%	84%	**88.30%**

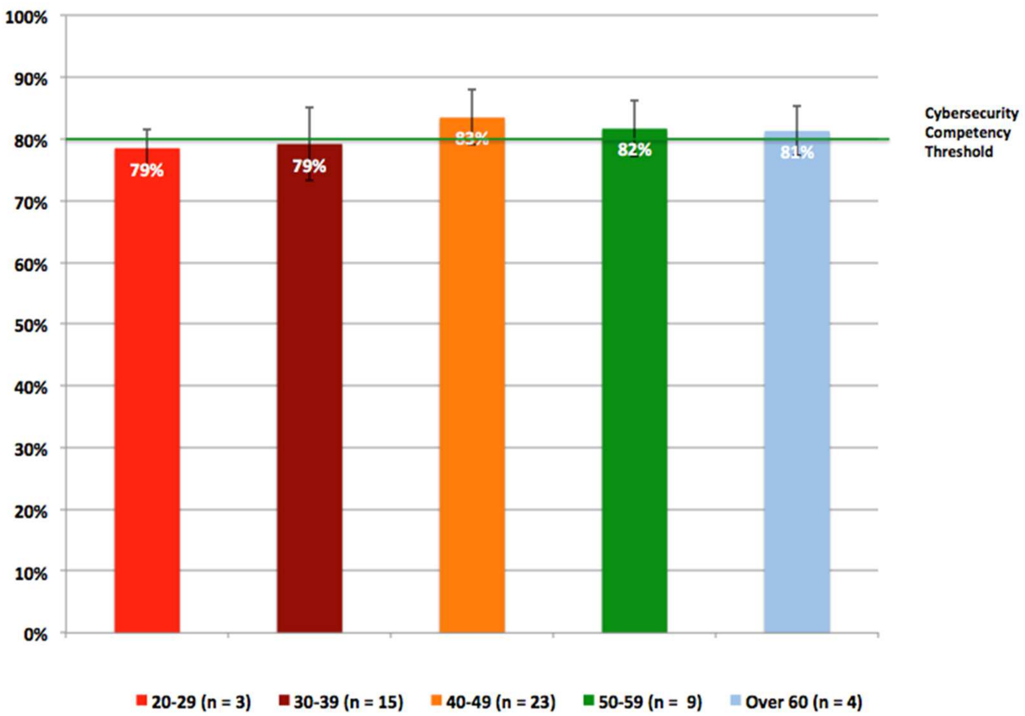


Figure 14. Summary of cybersecurity competency means and standard deviations by age (N = 54)

As shown in Figure 14, the difference between the means for the age groups is 4%. Standard deviations ranged from 6% (ages 20-29) to 12% (ages 30-39). The highest mean scores belonged to the 40-49 age group, while the lowest mean was the 20-29 age group. Figure 14 also shows that the mean score for OISUs over the age of 40 exceeds the cybersecurity competency threshold, while mean scores for OISUs under the age of 40 did not meet the OISU cybersecurity competency threshold. Thus, mean cybersecurity competency scores for OISUs below the age of 40 did not meet or exceed the cybersecurity competency threshold. It is thus inferred that as age increases, cybersecurity competency increases.

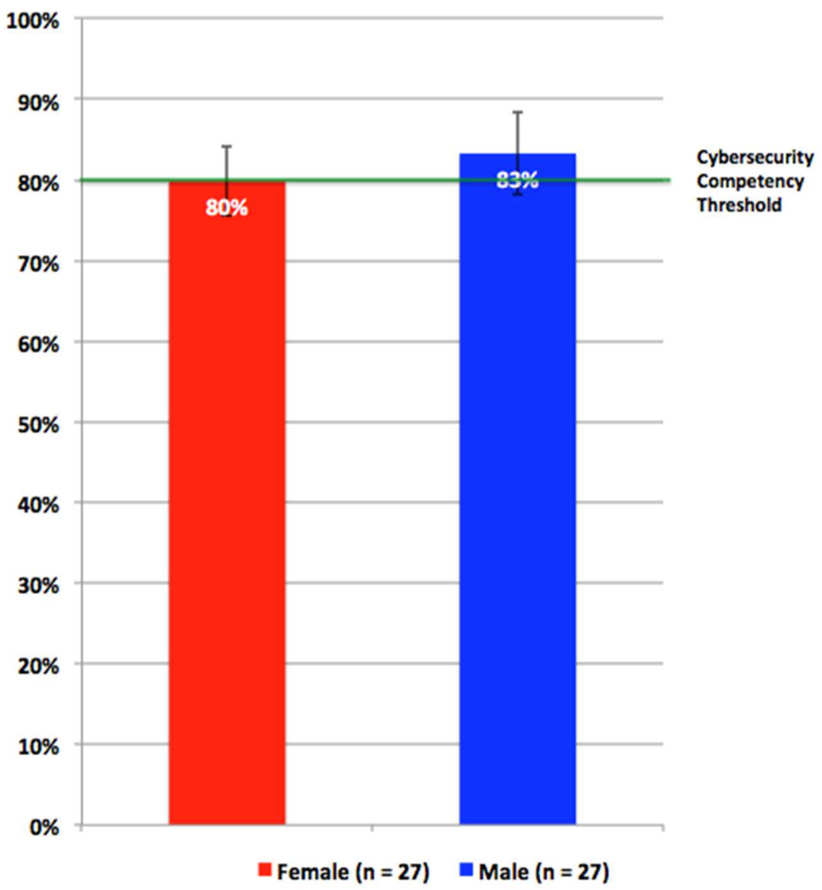


Figure 15. Summary of cybersecurity competency means and standard deviations by gender (N = 54)

Figure 15 illustrates that the sample of 54 OISUs was evenly split between females and males. The difference in means scores between genders was 3%. Females mean scores were 80% with a 9% standard deviation, while males mean scores were 83% with a 10% standard deviation. Using means, both genders as wholes scored at or above the OISU cybersecurity competency threshold.

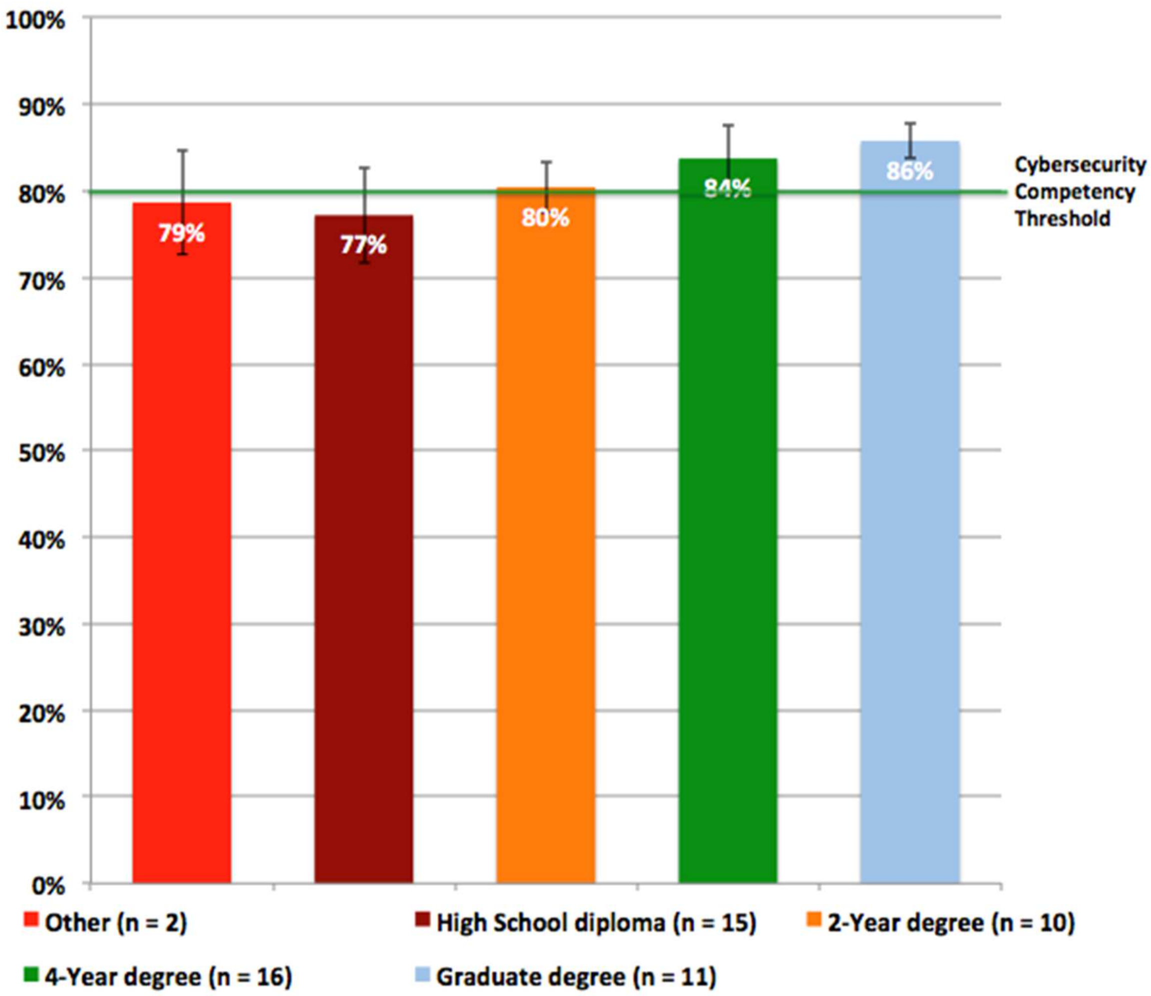


Figure 16. Summary of cybersecurity competency means and standard deviations by education (N = 54)

As shown in Figure 16, the difference between the lowest and highest means for the education groups is 9%. Standard deviations ranged from 4% (other education) to 12% (high school diploma). Figure 16 illustrates that as education is increased, the mean OISU cybersecurity competency score increases. Additionally, it is shown that mean scores for respondents with at least a 2-year college degree meet or exceed the OISU cybersecurity competency threshold. It is thus inferred that as education increases, cybersecurity competency increases.

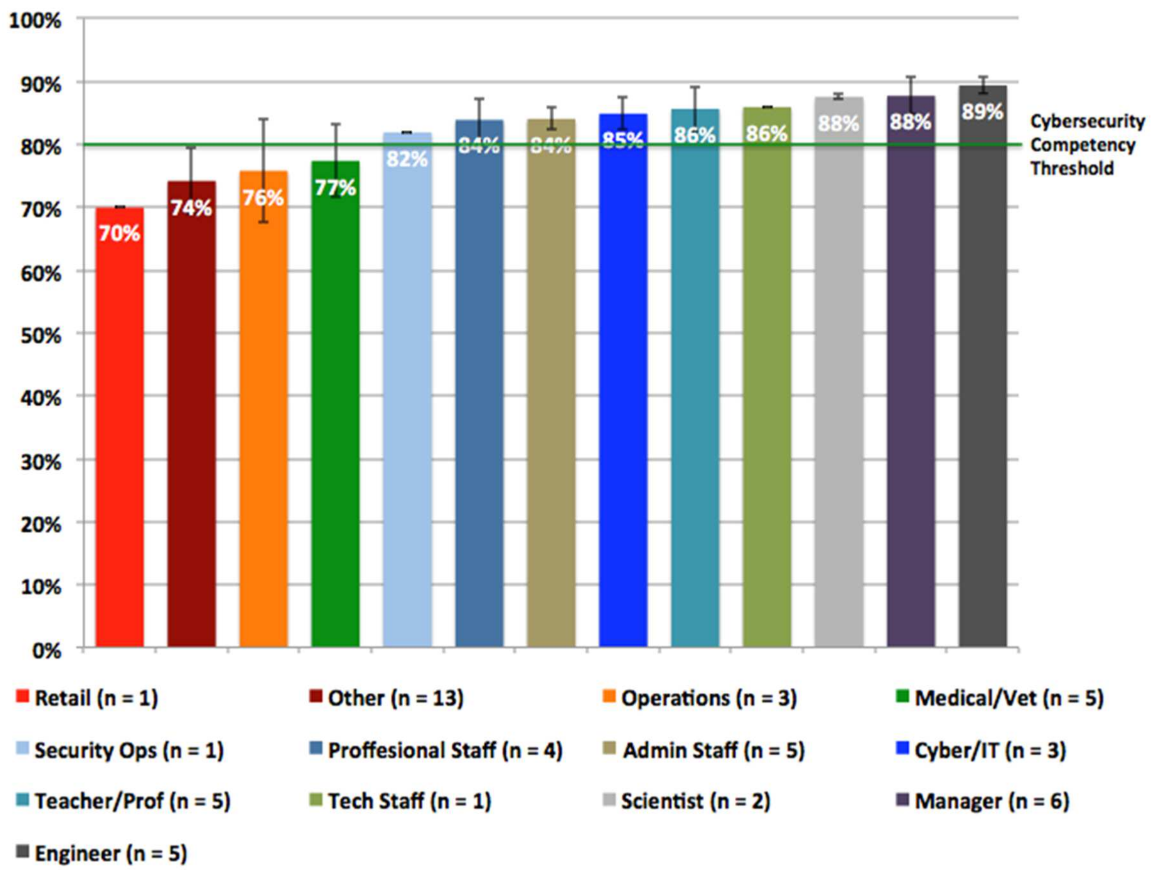


Figure 17. Summary of cybersecurity competency means and standard deviations by job function (N = 54)

Figure 17 illustrates mean OISU cybersecurity competency scores and standard deviations by 13 different jobs. The difference between the lowest and highest means scores was 19%. However, the lowest mean OISU cybersecurity competency score was from a sample size of one. The lowest standard deviations of 0% were from the sample sizes of one (security operator, retail, and technical staff). The highest mean score was 89% by engineers, with a 3% standard deviation. Figure 17 suggests that there exists a correlation between job function and IS usage, where gains in IS experience and/or cybersecurity training positively influences the cybersecurity competency of an OISU.

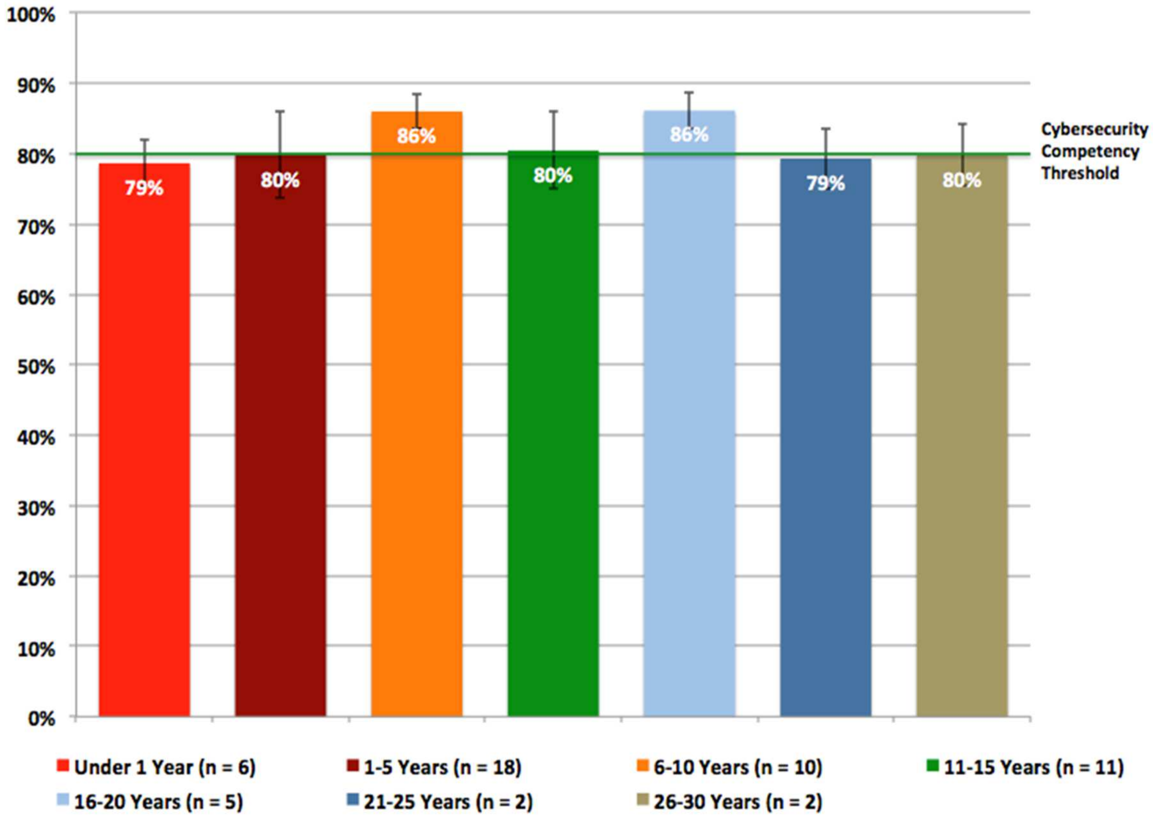


Figure 18. Summary of cybersecurity competency means and standard deviations by time with current employer (N = 54)

Figure 18 illustrates the difference between the lowest and highest means for the ‘time with employer’ groups is 9%. Standard deviations ranged from 5% (16-20 years) to 12% (1-5 years). Figure 17 illustrates that for the first 10 years of employment, as time with the company is increased, the mean OISU cybersecurity competency score increases. Additionally, it is shown that mean scores for respondents with 1-20 years with their company meet or exceed the OISU cybersecurity competency threshold.

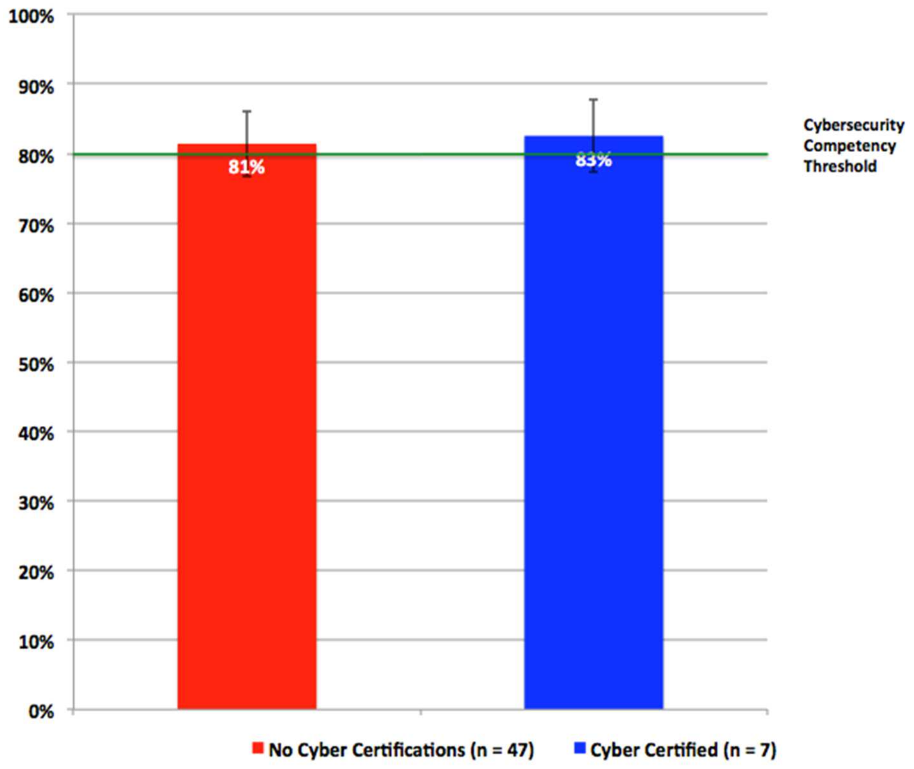


Figure 19. Summary of cybersecurity competency means and standard deviations for OISUs with and without cybersecurity certification (N = 54)

Figure 19 shows that there was a large difference in the sample of 54 OISUs with and without cybersecurity certifications. The difference in means scores between groups was 2%. OISUs without cybersecurity certifications mean scores were 81% with a 10% standard deviation, while cybersecurity certified OISUs mean scores were 83% with an 11% standard deviation. Using means, both groups scored at or above the OISU cybersecurity competency threshold.

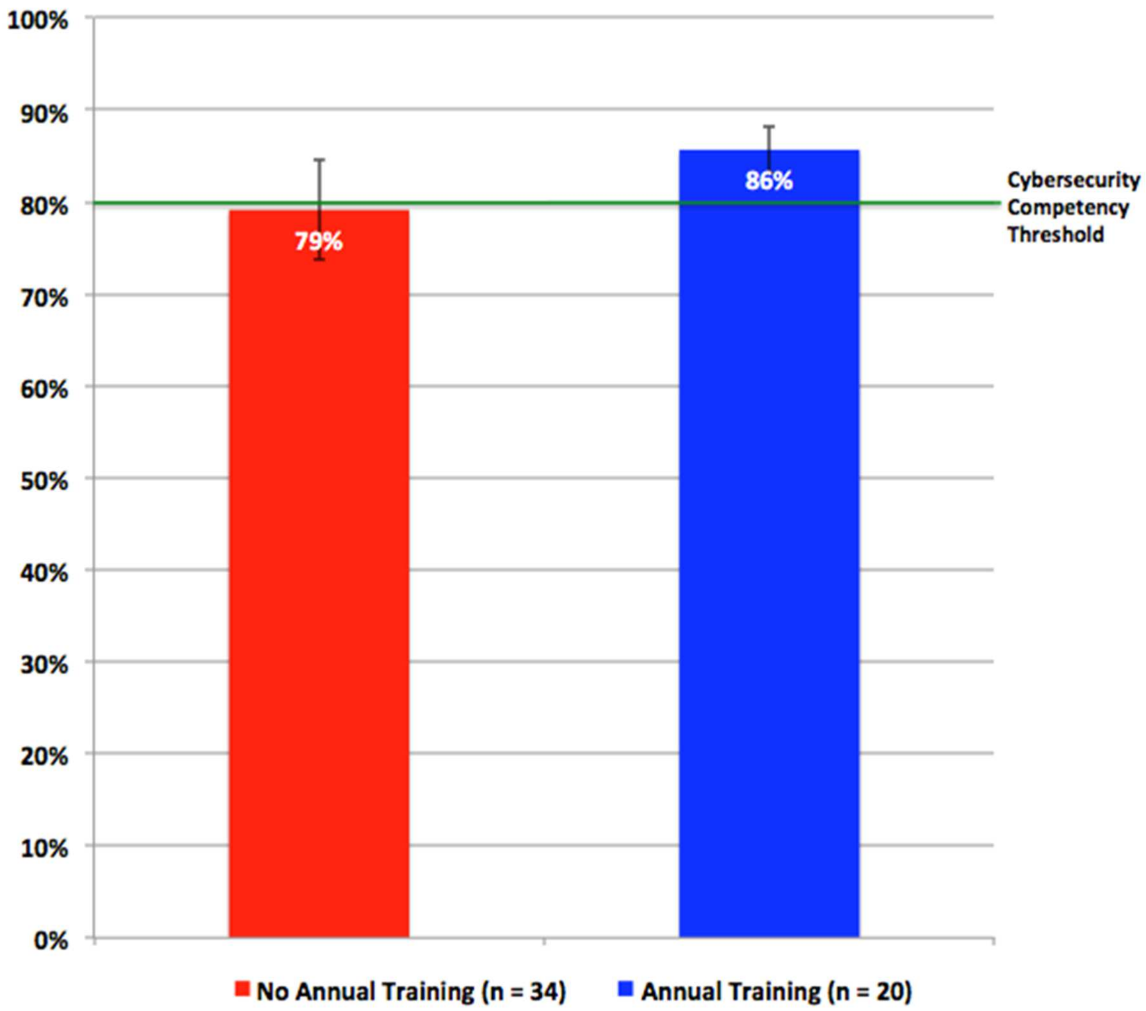


Figure 20. Summary of cybersecurity competency means and standard deviations for OISUs with and without annual cybersecurity training (N = 54)

As shown in Figure 20, the difference between the means for OISUs with and without annual cybersecurity training is 7%. Standard deviations were 10% for OISUs without annual cybersecurity training and 11% for those with annual cybersecurity training. The highest mean scores belonged to OISUs with annual cybersecurity training, while the lowest mean was for OISUs without annual cybersecurity training. Figure 20 also shows that the mean score for OISUs with annual cybersecurity training exceeds the cybersecurity competency threshold, while mean scores for OISUs without annual cybersecurity training did not meet the OISU cybersecurity competency threshold.

Further data analysis assessed the means, standard deviations, ceilings (highest), and floors (lowest) of the scores computed by the MyCyberKSAs^{TM} prototype assessment tool. These assessments were performed on KCs, SCs, OK, OS, and OISU cybersecurity competency scores, as shown in Table 26. A graphical representation of the means as well as standard deviations for KCs, SCs, OK, OS, and OISU cybersecurity competency scores is shown in Figure 21.

Table 26

Summary of Phase 5 Means, Standards Deviations, Ceilings, Floors for KCs, SCs, OK, OS, and Cybersecurity Competency Scores (N = 54)

	ASKC	**ISKC**	**INSKC**	**PSKC**	**ASSC**	**ISSC**	**INSSC**	**PSSC**	**OK**	**OS**	**Score**
Mean	83%	84%	82%	87%	69%	82%	81%	84%	84%	79%	82%
Std Dev	16%	12%	11%	11%	14%	18%	12%	10%	10%	11%	10%
Ceiling (max)	100%	100%	97%	100%	100%	100%	100%	95%	97%	94%	95%
Floor (min)	47%	46%	37%	46%	38%	36%	53%	45%	46%	45%	48%

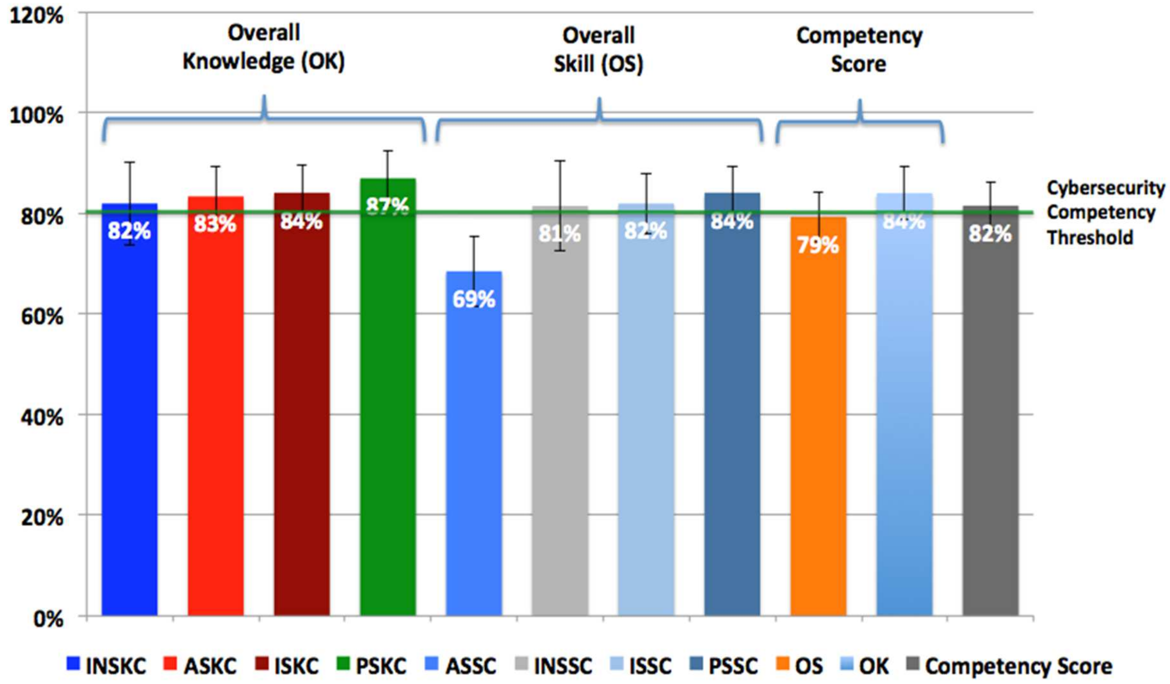


Figure 21. Summary of means and standard deviations for KCs, SCs, OK, OS, and cybersecurity competency scores

Table 26 and Figure 21 both show that the mean OK scores for OISUs was 5% higher than the OS scores. Thus, it appears the OISU participants in this study possess slightly more cybersecurity knowledge than cybersecurity skill. Additionally, the mean OISU cybersecurity competency score was 82%, which exceeds the OISU cybersecurity competency threshold. The ceiling scores for KCs, SCs, OK, OS, and OISU cybersecurity competency are mid-to-high 90's. These ceiling scores, specifically the OISU cybersecurity competency score, revealed that the MyCyberKSAs^{TM} prototype assessment tool appears to be a reliable method for measuring the cybersecurity competency of OISUs. If the MyCyberKSAs^{TM} prototype assessment tool were moderately-to-severely flawed, such high scores would be highly improbable. Therefore, as Phase 5 measured the cybersecurity competency levels of 54 OISUs, RQ5 had been met, and data collection for this research study was complete.

Table 27

ANOVA Results by Demographics (N = 54)

			ANOVA	
Item	**df**	**Mean Square Between Groups**	**F**	**Sig.**
Age	4	49.434	0.521	0.720
Annual cybersecurity training	*1*	*537.414*	*6.491*	*0.014**
Cyber certified	1	7.918	0.085	0.772
Education	4	146.274	1.683	0.169
Gender	1	160.373	1.781	0.188
Job function	*12*	*151.441*	*2.052*	*0.044**
Time with company	6	72.252	0.77	0.597

* - *p* <.05, ** - *p* <.01, *** - *p* <.001

Table 27 lists the results of the one-way ANOVA for each demographic group. The ANOVA for annual cybersecurity training was significant, *F*(1, 54) = 6.491, *p* = 0.014, and suggested that cybersecurity competency assessment scores differed by annual cybersecurity training due to a *p*-value that is less than 0.05 (Terrell, 2012). The ANOVA for job function was significant, *F*(12, 54) = 2.052, *p* = 0.044, and suggested that cybersecurity competency assessment scores differed by job function. The one-way ANOVA for age, cybersecurity certification, education, gender, and time with company were not significant, which suggested that there is no difference in cybersecurity competency assessment scores.

Summary

This chapter contained the results and data analysis performed by this research study. This study used a five-phased approach, with each phase collecting data and performing data analysis. Moreover, each phase of this study addressed a research question. Data collection and analysis for Phase 1 validated the OISU cybersecurity

KSAs, and addressed RQ1. Data collection and analysis for Phase 2 validated the OISU cybersecurity KSA measures, and addressed RQ2. Data collection and analysis for Phase 3 validated the OISU cybersecurity KSA weights, and addressed RQ3. Data collection and analysis for Phase 4 validated the OISU cybersecurity competency threshold, and addressed RQ4. Data collection and analysis for Phase 5 measured the cybersecurity competency of 54 OISUs, and addressed RQ5. Data analysis for Phase 5 showed that annual cybersecurity training and job function are significant, showing differences in cybersecurity competency. Data analysis for Phase 5 additionally showed that age, cybersecurity certification, gender, and time with company are not significant, showing no differences in cybersecurity competency.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Because cyber threats continue to cause financial and information losses to organizations by exploiting the human factor of cybersecurity, the need exists to continually and accurately assess OISU cybersecurity competency (Al Neaimi et al., 2015; Behrens et al., 2012; Johnson, 2012; Pittenger, 2016; Toth & Klein, 2013). Therefore, the main goal of this research study was to propose and validate, using SMEs, a reliable hands-on assessment prototype for measuring the combined necessary KSAs for cybersecurity competency of an OISU. To develop a reliable and valid method of measuring the cybersecurity competency of an OISU, this study achieved five goals using a five-phased approach. First, using the Delphi method, an expert panel of SMEs was used to propose and validate the necessary cybersecurity KSAs required to be measured when assessing the cybersecurity competency of an OISU. Second, using the Delphi method, an expert panel of SMEs was used to propose and validate KSA measures that were to be integrated into the MyCyberKSAs^{TM} prototype assessment tool. Third, using the Delphi method, an expert panel of SMEs was used to establish weights for the KSA measures. At this stage of research, the MyCyberKSAs^{TM} prototype assessment tool was operationalized using the data collected from the SMEs in Phases 1 - 3. Fourth, using the Delphi method, an expert panel of SMEs was used to establish the OISU cybersecurity competency threshold that was integrated into the MyCyberKSAs^{TM} prototype assessment tool. Last, the MyCyberKSAs^{TM} prototype assessment tool was used to measure the cybersecurity competency of 54 OISUs.

Discussion

First, this study resulted in defining a comprehensive list of validated cybersecurity KSAs for OISUs. Second, this study resulted in establishing validated measures for the OISU cybersecurity KSAs. Third, this study resulted in defining validated weights for the OISU cybersecurity KSAs. Fourth, this study resulted in establishing a validated cybersecurity competency threshold for determining the cybersecurity competency of OISUs. Fifth, this study resulted in establishing the MyCyberKSAs^{TM} prototype assessment tool for measuring the cybersecurity competency of OISUs. Last, this research study measured the cybersecurity competency of 54 OISUs.

The data analysis using one-way ANOVA in Phase 5 revealed that age, gender, cybersecurity certification, and time with company are not significant. Moreover, the data analysis of Phase 5 revealed that annual cybersecurity training as well as job function are significant, and suggest differences in cybersecurity competency assessment scores. Therefore, a result of this study shows that annual cybersecurity training is effective in increasing the OISU cybersecurity competency. Job function effecting OISU cybersecurity competency is assumed to be gains in IS experience causing positive increases to cybersecurity competency.

Phase 2 and Phase 5 of this study had limitations due to large data collection instruments that required a high level of commitment from participants. While the required numbers of participants were met for all phases of this study, it is assumed that some participants towards the end of the instruments may have lacked the high level of commitment necessary to provide accurate/detailed responses instead of convenient/quick responses. A possibly inconsequential limitation of this study is that cybersecurity ability was surrogated with education, instead of being measured. Another possible limitation of this study is that skill was measured with a Web-based tool, instead of observing a live demonstration of the skill being performed.

Implications

The implications of this research study are contributing to the cybersecurity body of knowledge and providing organizations with validated materials for constructing cybersecurity assessments. Specifically, literature has shown that in regards to the cybersecurity KSAs of OISUs, research tends to focus on a single KSA or small group of KSAs. A comprehensive list of cybersecurity KSAs for OISUs did not appear to exist in the body of knowledge. Accordingly, the body of knowledge on OISU cybersecurity competency did not appear to provide any comprehensive research studies. Therefore, this study provides valuable information that will assist organizations with constructing tools to accurately and continually assess the cybersecurity competency of their OISUs. Such assessments will help organizations identify strengths as well as weaknesses of OISUs, identify areas in which OISUs require additional training or supervision, and continually assess OISUs which is extremely helpful regarding emerging threats. Moreover, if the results of this study are implemented by organizations, this should reduce the probability of an OISU being exploited by a cybersecurity threat.

Recommendations and Future Research

This research study outlined an approach for employing the Delphi method to construct a prototype assessment tool for measuring the cybersecurity competency of an

OISU. The approach demonstrated by this research study can be implemented by other fields of study to propose and validate KSAs for other specialties. Moreover, this approach is transferrable between different fields of study where a prototype assessment tool needs to be developed. After collecting data with the MyCyberKSAs^{TM} prototype assessment tool, data analysis was conducted in which the findings and results were reported.

This research study provides many opportunities for future research studies to be conducted. First, the MyCyberKSAs^{TM} prototype assessment tool can be used on a larger sample and conduct more robust data analysis to determine the effects of multivariate factors on OISU cybersecurity competency. Second, the MyCyberKSAs^{TM} prototype assessment tool is large. Future studies can research alternative methods of performing as accurate of an assessment as MyCyberKSAs^{TM}, but in a shorter amount of time, perhaps by checking the validity of utilizing a smaller and randomized question pool. Third, future studies can develop third level weights for the KUs and SAs. Fourth, future studies can develop fourth level weights for the KTs and STs. By developing weights for the KUs, KTs, SAs, and STs, there will be no need to use the KC and SC group weights for the KSAs. Fifth, future studies may use virtual reality (VR) software to measure cybersecurity skills. While measuring skills with a Web-based tool is a legitimate substitute for observing a live demonstration of the skills, witnessing the cybersecurity skills being performed in VR is worthy of future research. Moreover, future studies involving VR could assess if there is a significant or insignificant difference in results when using VR versus Web-based tools, possibly reinforcing the confidence in Web-based tool skill assessment. Sixth, another opportunity for future research would be to study the OISU self-perceived cybersecurity competency versus what is measured by MyCyberKSAs^{TM}. Seventh, future studies could build on the results of this research study to produce a version of MyCyberKSAs^{TM} with higher validity. As with any exam or test, the first draft usually has room for improvement, MyCyberKSAs^{TM} is no different. Such future studies can improve the content used to measure the OISU cybersecurity KSAs with possibly further refined assessment questions, which also could include new KTs, STs, KUs, SAs, and/or KSAs based on emerging threats and vulnerabilities. Eighth, the results of this study suggested that the annual cybersecurity training and job function of an OISU positively influenced cybersecurity competency. Future studies could research whether and how education level influences OISU cybersecurity competency. Additionally, future studies could research if annual cybersecurity training actually helps OISUs, or conditions them on how to pass a cybersecurity assessment. Last, future research could build on MyCyberKSAs^{TM} to create a ‘Cybersecurity Drivers License’. Acquiring a motor vehicle drivers license does not mean that the driver is now an expert at operating a motor vehicle; a driver’s license signifies a minimal acceptable level of competency. Moreover, a driver’s license deems a person legally safe to drive a car. This same principle is applicable to the cybersecurity of OISUs. A ‘Cybersecurity Drivers License’ using a cybersecurity competency assessment of OISUs would assert that the end-user is safe to operate an Internet enabled IS within an organizational network. Even further, the ‘Cybersecurity Drivers License’ can be acquired in different classes, such as personal use or professional use.

Summary

The research problem addressed by this study is significant financial, information, and intellectual property loses for organizations as well as governments as a result of inadequate cybersecurity competency of IS users (Barlow et al., 2013; Choi et al., 2013; Shaw et al., 2009). Organizations invest large sums of money on cybersecurity controls to protect assets. However, a single OISU that does not possess cybersecurity competency may negate cybersecurity controls, which may cause catastrophic losses to the organization. Companies around the world are fully aware of the human factor shortfalls in cybersecurity and many institute SETA programs to increase OISU cybersecurity awareness. However, an empirical assessment of OISU cybersecurity competency can provide organizations with valuable insight into the cybersecurity competency of their workforce. Such insight can be used to determine if OISUs require additional training or even supervision for performing specific IS tasks. Additionally, empirical assessments of OISU cybersecurity can identify those with a high level of competency that may be leveraged in other capacities within the organization. This research study increased the body of knowledge and provided an approach for organizations to build their own OISU cybersecurity competency assessment tools. Moreover, this research study provided all of the content necessary to reconstruct the MyCyberKSAs^{TM} prototype assessment tool for public use.

The main goal of this research study was to propose and validate, using subject matter experts (SME), a reliable hands-on assessment prototype for measuring the combined necessary KSAs for cybersecurity competency of an OISU. The main goal of this study was building on the work of Behrens et al. (2012), as well as Toth and Klein

(2013), to develop a prototype OISU cybersecurity assessment tool. To achieve the main goal, this research study set five specific goals required to address five specific RQs using a five-phased approach.

In Phase 1, this study used a group of cybersecurity SMEs from the USG and private sector to answer the first research question:

> RQ1. What are the specific SME approved *set of cybersecurity KSAs*, which need to be measured to assess the attainment of cybersecurity competency by OISUs for organizational network access?

First this study performed a thorough review of literature to establish a list of applicable cybersecurity KSAs for OISUs. Next, a small group of cybersecurity experts participated in semi-structured SME interviews to pre-screen the list of OISU cybersecurity KSAs. Last, using anonymous online surveys, the Delphi method was used with 30 SMEs to propose and validate the set of cybersecurity KSAs to be measured in the cybersecurity competency assessment of OISUs. Upon gaining a consensus from the SMEs regarding the set of cybersecurity KSAs to be measured in the cybersecurity competency assessment of OISUs, the first research question had been answered.

Phase 2 of this research study used a group of cybersecurity SMEs from the USG and private sector to answer the second research question:

> RQ2. What are the SME approved cybersecurity *KSA measures*, which are needed to assess the attainment of cybersecurity competency by OISUs for organizational network access?

In Phase 2, using anonymous online surveys, two rounds of the Delphi method were conducted with SMEs to propose and validate the cybersecurity KSA measures to be used in the cybersecurity competency assessment of OISUs. In Phase 2 Round 1, the SMEs were presented with 90 KTs and STs to be assessed for acceptability. Phase 2 Round 1 collected qualitative and quantitative from 15 cybersecurity SMEs. While the quantitative data collected in Phase 2 was used to identify one deficient KSA measure, the qualitative data was used to improve 28 other KSA measures. The feedback from the SMEs in Phase 2 Round 1 was used to rework the 29 KSA measures that were incorporated into the Phase 2 Round 2 survey instrument for the SMEs to evaluate. In Phase 2 Round 2, qualitative and quantitative data was collected from seven SMEs, which resulted in a consensus to accept the 90 KTs and STs, thus answering the second research question.

Phase 3 of this research study used a group of cybersecurity SMEs from the USG and private sector to answer the third research question:

> RQ3. What are the SME identified *weights of the cybersecurity KSA measures*, which are needed to assess the attainment of cybersecurity competency by OISUs for organizational network access to form the MyCyberKSAs^{TM} hands-on assessment prototype?

In Phase 3, the KSAs were grouped into four KCs and four SCs, and using the Delphi method with anonymous online surveys, a group of 15 cybersecurity SMEs was asked to define weights for the KCs and SCs. The weights provided by the SMEs were averaged and accepted as weights for the cybersecurity KSA measures, thus answering the third research question.

Phase 4 of this research study used a group of cybersecurity SMEs from the USG and private sector to answer the fourth research question:

RQ4. What is the SME identified cybersecurity *competency threshold* for the combined *KSA measures*, which is the maximum needed for organizational network access as measured by the MyCyberKSAs^{TM} hands-on assessment prototype?

In Phase 4, using the Delphi method with anonymous online surveys, a group of 15 cybersecurity SMEs was asked to define the cybersecurity competency threshold for OISUs. The anonymous online survey provided the SMEs with the results from Phases 1 – 3, as well as a link to the MyCyberKSAs^{TM} prototype assessment tool. The responses from the SMEs were averaged and accepted as the OISU cybersecurity competency threshold for this research study, thus answering the fourth research question.

Phase 5 of this research study used a random group of OISUs to answer the fifth research question:

RQ5. What is the cybersecurity *competency level* as measured by the MyCyberKSAs^{TM} hands-on assessment prototype of a sample of 50 OISUs?

In Phase 5, using the FaceBook$^{©}$ social media Website to recruit participants, 54 OISUs completed the MyCyberKSAs^{TM} cybersecurity assessment for OISUs. The results and data analysis from Phase 5 answered the fifth and final research question of this study. The data analysis in Phase 5 using one-way ANOVA showed that annual cybersecurity training and job function are significant, thus suggesting these two demographics produce differences in OISU cybersecurity competency.

This study identified three limitations of the research being conducted. The first limitation was the level of commitment by participants. Due to the size of two instruments, and the necessary time required to complete the instruments, the level of commitment by participants was a limitation. Second, the surrogation of cybersecurity ability with education was a limitation of this study. Last, measuring skills with a Web-based tool was a limitation.

This research study contributed to the body of knowledge as well as the field of cybersecurity. This study resulted in the definition of a comprehensive list of validated cybersecurity KSAs for OISUs. This study also resulted in establishing validated OISU cybersecurity KSA measures. Additionally, this study resulted in the establishing validated weights for the OISU cybersecurity KSAs. The result of this study defined a validated cybersecurity competency threshold for determining the cybersecurity competency of OISUs. Moreover, this study resulted in establishing the MyCyberKSAs^{TM} prototype assessment tool for measuring the cybersecurity competency of OISUs. Therefore, the work presented in this research study may be leveraged by organizations to improve cybersecurity which could lower the probability of financial and information losses.

In conclusion, other researchers can use the MyCyberKSAs^{TM} index score to measure larger and more diverse populations. The MyCyberKSAs^{TM} prototype assessment tool can be used by researchers to assess: OISU cybersecurity competency, specific KSAs, or sets of KSAs. The MyCyberKSAs^{TM} prototype assessment tool can also be used by organizations to assess the cybersecurity competency of their workforce. Additionally, government organizations such as the Department of Homeland Security can provide MyCyberKSAs^{TM} to the general public to identify individual cybersecurity weaknesses for training, thus protecting the population from foreign and domestic cyber threats.

Appendix A

Phase 1 Semi-Structured SME Interview

Dear Cybersecurity Expert,

This semi-structured SME interview intends to evaluate the knowledge, skills, and abilities (KSA) for organizational information system users that were identified in scholarly literature. We ask that you assess the KSAs to determine if they are required for the measurement of the cybersecurity competency of an organizational information system user. Furthermore, we ask you to identify any KSAs that may be missing from the list.

Please respond to all questions as honestly and accurately as possible. By completing this interview you agree and understand that your responses are voluntary. Measures will be taken to ensure than responses are anonymous and cannot be traced to any individual. You may stop this interview at any time. In the event that you chose to stop this interview, your responses will not be recorded. By participating in this survey you certify that you are over the age of 18 years old.

Demographics

What is your age?

What is your gender?

What is your job title?

How long have you been with your current organization?

What is your highest level of education?

Which cybersecurity certifications do you possess?

KSA Evaluation

1. Please evaluate the following KSAs and accept or remove the KSA

KSA Type	KSA Name	Accept or remove KSA?
Abilities	Advanced written comprehension ability	Accept / Remove
	Near vision ability	Accept / Remove
	Problem sensitivity ability	Accept / Remove
	Written communication ability	Accept / Remove
	Written expression ability	Accept / Remove
Knowledge	Knowledge of access control	Accept / Remove
	Knowledge of antivirus software	Accept / Remove
	Knowledge of cyber threats	Accept / Remove

	Knowledge of cyber vulnerabilities	Accept / Remove
	Knowledge of cybersecurity POCs	Accept / Remove
	Knowledge of cybersecurity responsibilities	Accept / Remove
	Knowledge of email encryption	Accept / Remove
	Knowledge of email use	Accept / Remove
	Knowledge of using file permissions	Accept / Remove
	Knowledge of cyber incident reporting	Accept / Remove
	Knowledge of information handling	Accept / Remove
	Knowledge of information privacy	Accept / Remove
	Knowledge of Internet use	Accept / Remove
	Knowledge of mobile computing risks	Accept / Remove
	Knowledge of password reuse	Accept / Remove
	Knowledge of phishing	Accept / Remove
	Knowledge of physical security	Accept / Remove
	Knowledge of cybersecurity policy compliance	Accept / Remove
	Knowledge of sensitive information and PII	Accept / Remove
	Knowledge of social engineering	Accept / Remove
	Knowledge of social networking security	Accept / Remove
	Knowledge of smart card risks	Accept / Remove
	Knowledge of strong passwords	Accept / Remove
	Knowledge of Webmail risks	Accept / Remove
Skills	Skill in preventing unauthorized access to an IS by controlling access to systems	Accept / Remove
	Skill in using an antivirus application to properly update the software when notified that antivirus requires an update	Accept / Remove
	Skill in managing cookie settings and usage	Accept / Remove
	Skill in configuring and using Email in a manner that prevents sensitive information and PII loss	Accept / Remove
	Skill in cybersecurity incident reporting	Accept / Remove
	Skill in avoiding suspicious and malicious Websites when using the Internet at work	Accept / Remove
	Skill in securely operating mobile computing devices	Accept / Remove
	Skill in avoiding actions that increase exposure to malicious code downloading or execution	Accept / Remove
	Skill in creating using unique passwords for all user accounts and logins	Accept / Remove
	Skill in peer-to-peer software usage without exploitation by transferring copyrighted materials, sensitive information, or PII	Accept / Remove
	Skill in avoiding a phishing attempts of sensitive information and PII	Accept / Remove
	Skill in physically protecting an IS from an unauthorized user	Accept / Remove
	Skill in using authorized systems for sensitive information and PII data processing as well as transmissions	Accept / Remove
	Skill in labeling removable media that contains sensitive information or PII	Accept / Remove
	Skill in using encryption to store data on approved removable media	Accept / Remove
	Skill in identifying sensitive information and PII	Accept / Remove
	Skill in avoiding social engineering attempts of sensitive information and PII	Accept / Remove
	Skill in using social networking without divulging sensitive information and PII	Accept / Remove
	Skill in avoiding a spear-phishing attempts of sensitive information and PII	Accept / Remove
	Skill in identifying the spillage of sensitive information and PII	Accept / Remove
	Skill in creating strong passwords	Accept / Remove
	Skill in using encryption to transmit sensitive information and PII when using Webmail	Accept / Remove
	Skill in avoiding a whaling attempts of sensitive information and PII	Accept / Remove

2. Were there any KSAs that you think should be removed from the list? Can you explain why each KSA should be removed? ______________________________

____

____

____

3. Are any abilities missing from the list? Can you explain why the abilities should be added? ____

____

____

____

4. Are any knowledge units missing from the list? Can you explain why the knowledge units should be added? ____
____
____
____

5. Are any skill areas missing from the list? Can you explain why the skill areas should be added? ____
____
____
____

Appendix B

Phase 1 Email to Expert Panel

Dear Cybersecurity Expert,

We need your help in providing expert validation for an upcoming doctoral research study. I am a Ph.D. Candidate in Information Systems at the College of Engineering and Computing, Nova Southeastern University. My research is seeking to develop a prototype tool that will determine the cybersecurity competency of an organizational information system user. Such users include: IT personnel, secretaries, accountants, technical writers, physicians, etc. To develop the prototype tool, I need assistance from those that have knowledge in cybersecurity for four phases of data collection. This phase of research, Phase 1, requires assistance from experts to validate the knowledge, skills, and abilities (KSA) that may be used by an organizational information system user.

The surveys you will receive will follow the Delphi method. This may require one or two additional rounds of the survey to be completed to form a consensus. Once a consensus is achieved, the study will proceed to the next phase. All participants are subject matter experts in this area.

By participating in this study you agree and understand that your responses are voluntary. Measures will be taken to ensure that responses are anonymous and cannot be traced to any individual. You may stop participating in this study at any time. In the event that you no longer participate in this study, your responses will not be recorded. By participating in this study you certify that you are over the age of 18 years old. If you are willing to participate, please click on the following link for access: www.nova.edu/~rn380

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study.

If you wish to receive the findings of the study, please send contact me via email and I will provide you with information about the academic research publication(s) resulting from this study.

Regards,
Richard Nilsen, PhD Candidate
E-mail: rn380@nova.edu

Appendix C

Phase 1 Round 1 Survey

Dear Cybersecurity Expert,

This survey will be completed using the Delphi method. All participants are subject matter experts in this area. This survey intends to compile a list of all cybersecurity knowledge, skills, and abilities (KSAs) that an organizational information system user must possess. Such users include: IT personnel, secretaries, accountants, technical writers, physicians, etc.

Please respond to all questions as honestly and accurately as possible. By completing this survey you agree and understand that your responses are voluntary. Measures will be taken to ensure that responses are anonymous and cannot be traced to any individual. You may exit this survey at any time. In the event that you chose to exit this survey, your responses will not be recorded. By participating in this survey you certify that you are over the age of 18 years old.

Cybersecurity Abilities

Cybersecurity as defined by the Association of Computing Machinery Joint Task Force (ACMJTF) on Cybersecurity Education (2016) is "computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (p. 1).

Prager, Moran, and Sanchez (1997) defined ability as "the capacity to carry out physical and mental acts required by tasks" (p. 39)

Demographics

What is your age?

(A) Under 20
(B) 20-29
(C) 30-39
(D) 40-49
(E) 50-59
(F) Over 60

What is your gender?

(A) Female
(B) Male

What is your job function?

(A) Administrative staff
(B) Cybersecurity/IT staff
(C) Engineer
(D) Manager
(E) Operations
(F) Professional staff
(G) Scientist
(H) Security operator
(I) Teacher/Professor
(J) Technical staff
(K) Other

How long have you been with your current organization?

(A) Under 1 year
(B) 1 – 5 years
(C) 6 – 10 years
(D) 11 – 15 years
(E) 16 – 20 years
(F) 21 – 25 years
(G) 26 – 30 years
(H) Over 30 years

Which describes your current employer?

(A) Academia
(B) Federal government employee
(C) Private sector company
(D) State government employee
(E) Other

What is your highest level of education?

(A) High school diploma
(B) 2-year college (Associates degree)
(C) 4-year college (Bachelors degree)
(D) Graduate degree
(E) Doctorate
(F) Other

Which cybersecurity certifications do you possess?

____

____

Please evaluate the following cybersecurity ability requirements for an organizational information system user (OISU) and rate their importance.

	Not at all important (1)	Low importance (2)	Slight importance (3)	Neutral (4)	Moderately important (5)	Very important (6)	Extremely important (7)
A1. Near vision ability	○	○	○	○	○	○	○

Near vision is defined as the “ability to see details at close range (within a few feet of the observer)” (Trippe et al., 2014, p.185).

Provide feedback (optional): ____

____

A2. Problem sensitivity ability	○	○	○	○	○	○	○

Problem sensitivity is defined as the “ability to tell when something is wrong or is likely to go wrong. It does not involve solving the problem, only recognizing there is a problem” (Trippe et al., 2014, p.185).

Provide feedback (optional): ____

____

A3. Written communication ability	○	○	○	○	○	○	○

Written communication is defined as the “transmission of [a] message in written symbols” (Terkan, 2013, p. 149).

Provide feedback (optional): ____

____

A4. Written expression ability	○	○	○	○	○	○	○

Written expression is “a visible representation of thoughts, feelings, and ideas using symbols of the writer’s language system for the purpose of communication or recording” (Poteet, 1980, p. 88).

Provide feedback (optional): ____

____

Are there any important cybersecurity abilities for OISU's that are missing? Please provide justifications with your response: ______________________________

____

____

____

Cybersecurity Knowledge

Knowledge is defined by Alavi and Leidner (2001) as "a justified belief that increases an entity's capacity for taking effective action" (p. 109).

Please evaluate the following cybersecurity knowledge requirements for an organizational information system user (OISU) and rate their importance.

	Not at all important (1)	Low importance (2)	Slight importance (3)	Neutral (4)	Moderately important (5)	Very important (6)	Extremely important (7)
K1. Knowledge of access control	○	○	○	○	○	○	○

Access control is defined as "the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner" (Lopez, Oppliger, & Pernul, 2004, p. 580).

Provide feedback (optional): ____

____

K2. Knowledge of antivirus software	○	○	○	○	○	○	○

Antivirus software is "a program that attempts to identify, thwart and eliminate computer viruses and other malicious software" (Karantjias & Polemi, 2010, p. 60).

Provide feedback (optional): ____

____

K3. Knowledge of cyber threats	○	○	○	○	○	○	○

Cyber threats are any sources or circumstances that have the potential to compromise the confidentiality, integrity, and availability of an information system (Jung, Han, & Suh, 1999; Mejias & Balthazard, 2014).

Provide feedback (optional): ____

____

K4. Knowledge of cyber vulnerabilities	○	○	○	○	○	○	○

Cyber vulnerabilities are **"**weaknesses or flaws, in terms of security and privacy" (Kalloniatis, Mouratidis, & Islam, 2013, p. 4).

Provide feedback (optional): ____

____

K5. Knowledge of cybersecurity POCS	○	○	○	○	○	○	○

Cybersecurity POCs are “computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information officers (CIOs), computer security program managers, and others who are responsible for preparing for, or responding to, security incidents” (Cichonski, Millar, Grance, & Scarfone, 2012, p .1)

Provide feedback (optional): ______________________________

____

K6. Knowledge of cybersecurity responsibilities	○	○	○	○	○	○	○

Cybersecurity responsibilities include protecting sensitive information, protecting information systems, protecting PII, providing physical security, and potentially updating software (Gross & Rosson, 2007; Karantjias & Polemi, 2010).

Provide feedback (optional): ______________________________

____

K7. Knowledge of email encryption	○	○	○	○	○	○	○

Email encryption is defined as “the process by which [email] is encoded so that only an authorized recipient can decode and consume the [email]” (Microsoft, 2016a).

Provide feedback (optional): ______________________________

____

K8. Knowledge of email use	○	○	○	○	○	○	○

“An email acceptable use policy sets out your employees' responsibilities when using email in their day-to-day working activities” (NIBusinessInfo, 2016).

Provide feedback (optional): ______________________________

____

K9. Knowledge of cyber incident reporting	○	○	○	○	○	○	○

Incident reporting is the act of reporting suspicious individuals, worker misconduct, and all security incidents (Parsons et al., 2014).

Provide feedback (optional): ______________________________

____

K10. Knowledge of information handling	○	○	○	○	○	○	○

Information handling is the access, creation, destruction, disposition, distribution, maintenance, receipt, storage, transmittal, and use of information (Bernard, 2007).

Provide feedback (optional): ______________________________

____

K11. Knowledge of information privacy	○	○	○	○	○	○	○

Information privacy is defined as "the claim of individuals, groups, or institutions to determine when, and to what extent, information about them is communicated to others" (Lallmahamood, 2007, p. 7).

Provide feedback (optional): ____

____

K12. Knowledge of Internet use	○	○	○	○	○	○	○

An acceptable Internet use policy defines "guidelines for employees indicating both acceptable and unacceptable Internet usages, with the intention of controlling employee [behaviors] and actions which contribute to the incidence and severity of the [organization's] Internet risks" (Lichtenstein & Swatman, 1997, p. 1).

Provide feedback (optional): ____

____

K13. Knowledge of mobile computing risks	○	○	○	○	○	○	○

Mobile computing is defined as "using portable computers capable of wireless networking" (Johansson & Andersson, 2015, p. 1).

Provide feedback (optional): ____

____

K14. Knowledge of password reuse	○	○	○	○	○	○	○

Password reuse is using the same password for multiple accounts (Ives, Walsh, & Schneider, 2004).

Provide feedback (optional): ____

____

K15. Knowledge of phishing	○	○	○	○	○	○	○

Phishing is defined as "a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion" (Jakobsson & Myers, 2007, p. 1).

Provide feedback (optional): ____

____

K16. Knowledge of physical security	○	○	○	○	○	○	○

Physical security is defined as "physical measures taken to safeguard personnel, to protect unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft" (Newsome & Jarmon, 2016, p. 322).

Provide feedback (optional): ____

____

K17. Knowledge of cybersecurity policy compliance	○	○	○	○	○	○	○

Policy compliance is the adherence to a policy, where a policy is defined as “a course or principle of action adopted or proposed by a government, party, business, or individual” (Oxford, 2016, p.1).

Provide feedback (optional): ____

____

K18. Knowledge of sensitive information and PII	○	○	○	○	○	○	○

Sensitive information is defined as “protected information that the owner does not want to reveal to others and not to be divulged outside the [organization] as well as Information about an individual’s racial or ethnic origin, criminal record, sexual preferences or practices and other information that include political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, or a trade union” (Ajigini, Van der Poll, & Kroeze, 2012, p. 7).

PII is defined as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (McCallister el al., 2010, p. 7)

Provide feedback (optional): ____

____

K19. Knowledge of social engineering	○	○	○	○	○	○	○

Social engineering is defined as “the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks” (Abraham & Chengalur-Smith, 2010, p. 183).

Provide feedback (optional): ____

____

K20. Knowledge of social networking security	○	○	○	○	○	○	○

Social networking is defined as “web-based services allowing individuals to: (a) construct a profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and interact with their list of connections and those made by others within that system” (Weeden, Cooke, & McVey, 2013, p. 250).

Provide feedback (optional): ____

____

K21. Knowledge of smart card risks	○	○	○	○	○	○	○

Smart cards are defined as “credit card-shaped devices incorporating an integrated circuit chip (memory, microprocessor, application-specific, etc.), although they can also take the form of tokens, keys, and non-credit card-shaped card-type devices” (Hester & Joseph, 1998, p. 54).

Provide feedback (optional): ____

____

K22. Knowledge of strong passwords	○	○	○	○	○	○	○

Passwords are considered strong when “having more than eight characters, at least one change of case, a number that is not at the end, and a non-alphanumeric character such as # or * that is also not at the end of the password” (Keller, Powell, Horstmann, Predmore, & Crawford, 2005, p. 13).

Provide feedback (optional): ____

____

K23. Knowledge of Webmail risks	○	○	○	○	○	○	○

Webmail is defined as “web application that allows users to read and write e-mail on the Internet through a web interface” (Ioannou & Hannafin, 2008, p. 47).

Provide feedback (optional): ____

____

Are there any important cybersecurity knowledge units for OISU's that are missing? Please provide justifications with your response.

____

____

____

Cybersecurity Skill

Skill is defined as a goal-directed, well-organized set of actions that is acquired through practice and performed with economy of effort, which enables a person to do something well (Boyatzis & Kolb, 1995)

Please evaluate the following cybersecurity skill requirements for an organization information system user (OISU) and rate their importance.

	Not at all important (1)	Low importance (2)	Slight importance (3)	Neutral (4)	Moderately important (5)	Very important (6)	Extremely important (7)
S1. Skill in preventing unauthorized access to	○	○	○	○	○	○	○

an IS by controlling access to systems

Provide feedback (optional): ____

____

S2. Skill in using an antivirus application to properly update the software when notified that antivirus requires an update	○	○	○	○	○	○	○

Provide feedback (optional): ____

____

S3. Skill in configuring and using Email in a manner that limits sensitive information and PII loss	○	○	○	○	○	○	○

Email security is the secure use of email that ensures the protection of sensitive information and PII, as well as preventing the propagation of malicious code (Carlton et al., 2015; DISA, 2015; Wang, Li, & Cheng, 2014).

Provide feedback (optional): ____

____

S4. Skill in cybersecurity incident reporting	○	○	○	○	○	○	○

Provide feedback (optional): ____

____

S5. Skill in securely operating mobile computing devices	○	○	○	○	○	○	○

Provide feedback (optional): ____

____

S6. Skill in avoiding actions that increase exposure to malicious code downloading or execution	○	○	○	○	○	○	○

Malicious code is capable of giving hackers access to a network or system, erase hard drives, and corrupt files (DISA, 2015). Examples of malicious code are viruses, worms, Trojan horses, spyware, and scripts (DISA, 2015).

Provide feedback (optional): ____

____

S7. Skill in creating	○	○	○	○	○	○	○

using unique passwords for all user accounts and logins

Provide feedback (optional): ______________________________

____

S8. Skill in peer-to-peer software usage without exploitation by transferring copyrighted ○ ○ ○ ○ ○ ○ ○

Peer-to-peer is defined as “technology that enables two or more peers to collaborate spontaneously in a network of equals (peers) by using appropriate information and communication systems without the necessity for central coordination” (Schoder & Fischbach, 2003, p. 27).

Provide feedback (optional): ______________________________

____

S9. Skill in identifying and avoiding a phishing attempt ○ ○ ○ ○ ○ ○ ○

Provide feedback (optional): ______________________________

____

S10. Skill in physically protecting an IS from an unauthorized user ○ ○ ○ ○ ○ ○ ○

Provide feedback (optional): ______________________________

____

S11. Skill in using authorized systems for sensitive information and PII data processing as well as transmissions ○ ○ ○ ○ ○ ○ ○

Provide feedback (optional): ______________________________

____

S12. Skill in labeling removable media that contains sensitive information or PII ○ ○ ○ ○ ○ ○ ○

Removable media are external storage mediums such as: CDs, DVDs, thumb drives, and USB hard drives.

Provide feedback (optional): ______________________________

____

S13. Skill in using encryption to store data ○ ○ ○ ○ ○ ○ ○

approved removable media

Provide feedback (optional): ____

____

S14. Skill in identifying sensitive information and PII	○	○	○	○	○	○	○

Provide feedback (optional): ____

____

S15. Skill in avoiding social engineering attempts	○	○	○	○	○	○	○

Provide feedback (optional): ____

____

S16. Skill in using social networking without divulging sensitive information and PII	○	○	○	○	○	○	○

Provide feedback (optional): ____

____

S17. Skill in identifying and avoiding a spear-phishing attempt	○	○	○	○	○	○	○

Spear-phishing is defined as “a type of phishing attack that targets particular individuals, groups of people, or organizations” (DISA, 2015).

Provide feedback (optional): ____

____

S18. Skill in identifying the spillage of sensitive information and PII	○	○	○	○	○	○	○

Spillage occurs “when information is spilled from a higher classification or protection level to a lower classification or protection level” (DISA, 2015).

Provide feedback (optional): ____

____

S19. Skill in creating strong passwords	○	○	○	○	○	○	○

Provide feedback (optional): ____

____

S20. Skill in using encryption to transmit sensitive information and PII when using Webmail	○	○	○	○	○	○	○

Provide feedback (optional): ______________________________

____

S21. Skill in identifying and avoiding a whaling attempt	○	○	○	○	○	○	○

Whaling is a form of spear-phishing that targets high-level personnel (DISA, 2015).

Provide feedback (optional): ______________________________

____

S22. Skill in avoiding suspicious and malicious Websites when using the Internet at work	○	○	○	○	○	○	○

Provide feedback (optional): ______________________________

____

Are there any important cybersecurity skill areas for OISU's that are missing? Please provide justifications with your response.

____

____

____

Appendix D

Phase 2 Email to Expert Panel

Dear Cybersecurity Expert,

We need your help in providing expert validation for an upcoming doctoral research study. I am a Ph.D. Candidate in Information Systems at the College of Engineering and Computing, Nova Southeastern University. My research is seeking to develop a prototype tool that will determine the cybersecurity competency of an organizational information system user. Such users include: IT personnel, secretaries, accountants, technical writers, physicians, etc. To develop the prototype tool, I need assistance from those that have knowledge in cybersecurity for four phases of data collection. This phase of research, Phase 2, requires assistance from experts to validate the intended methods to measure the KSAs that were validated in phase 1.

The surveys you will receive will follow the Delphi method. This may require one or two additional rounds of the survey to be completed to form a consensus. Once a consensus is achieved, the study will proceed to the next phase. All participants are subject matter experts in this area.

By participating in this study you agree and understand that your responses are voluntary. Measures will be taken to ensure that responses are anonymous and cannot be traced to any individual. You may stop participating in this study at any time. In the event that you no longer participate in this study, your responses will not be recorded. By participating in this study you certify that you are over the age of 18 years old. If you are willing to participate, please click on the following link for access: www.nova.edu/~rn380

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study.

If you wish to receive the findings of the study, please send contact me via email and I will provide you with information about the academic research publication(s) resulting from this study.

Regards,
Richard Nilsen, PhD Candidate
E-mail: rn380@nova.edu

Appendix E

Phase 2 Round 1 Survey

Dear Cybersecurity Expert,

This survey will be completed using the Delphi method. All participants are subject matter experts in this area. This survey intends to compile a list of methods to measure the cybersecurity knowledge, skills, and abilities (KSAs) that an organizational information system user must possess. Such users include: IT personnel, secretaries, accountants, technical writers, physicians, etc.

Please respond to all questions as honestly and accurately as possible. By completing this survey you agree and understand that your responses are voluntary. Measures will be taken to ensure than responses are anonymous and cannot be traced to any individual. You may exit this survey at any time. In the event that you chose to exit this survey, your responses will not be recorded. By participating in this survey you certify that you are over the age of 18 years old.

Demographics

What is your age?

(A) Under 20
(B) 20-29
(C) 30-39
(D) 40-49
(E) 50-59
(F) Over 60

What is your gender?

(A) Female
(B) Male

What is your job function?

(A) Administrative staff
(B) Cybersecurity/IT staff
(C) Engineer
(D) Manager
(E) Operations
(F) Professional staff
(G) Scientist
(H) Security operator
(I) Teacher/Professor

(J) Technical staff
(K) Other

How long have you been with your current organization?

(A) Under 1 year
(B) 1 – 5 years
(C) 6 – 10 years
(D) 11 – 15 years
(E) 16 – 20 years
(F) 21 – 25 years
(G) 26 – 30 years
(H) Over 30 years

Which describes your current employer?

(A) Academia
(B) Federal government employee
(C) Private sector company
(D) State government employee
(E) Other

What is your highest level of education?

(A) High school diploma
(B) 2-year college (Associates degree)
(C) 4-year college (Bachelors degree)
(D) Graduate degree
(E) Doctorate
(F) Other

Which cybersecurity certifications do you possess?
____
____

Organizational Information System User Cybersecurity Knowledge Assessment

Cybersecurity as defined by the Association of Computing Machinery Joint Task Force (ACMJTF) on Cybersecurity Education (2016) is "computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (p. 1).

Knowledge is defined by Alavi and Leidner (2001) as "a justified belief that increases an entity's capacity for taking effective action" (p. 109).

Please evaluate the following cybersecurity knowledge measures and scoring of the measure answers for an organizational information system user (OISU) and rate their acceptability.
Note: questions in the form of “check all that apply” deduct points for incorrect selections. The need to deduct points for incorrect selections is needed to ensure maximum points are not achieved by simply “checking” all options, without penalty. Additionally, these “check all that apply” questions will have a minimum score of zero. Hence, multiple negative point selections for a question will not produce a negative score.

Knowledge of access control (KAC)
Access control is defined as “the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner” (Lopez, Oppliger, & Pernul, 2004, p. 580).

KAC1. (Possess knowledge regarding identifying the risk of writing down passwords)
When writing down a login password, it is best to hide the password under your keyboard where it is not visible.
A) Yes, this is easily accessible (2 points)
B) No, inside a desk drawer is more secure (4 points)
C) No, you should not write down your passwords (10 points)
D) No, you should place it on your monitor or somewhere visible, in case your coworkers need it to log in (0 points)

The above answers related to the question and scoring about KAC1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KAC2. (Possess knowledge regarding how often passwords should be changed)
Which is the most reasonable timeframe for changing passwords?
A) Daily (2 points)

B) Weekly (4 points)
C) Quarterly (10 points)
D) Never (0 points)

The above answers related to the question and scoring about KAC2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KAC3. (Possess knowledge regarding identifying the need to keep passwords confidential)
Which of the following is an acceptable situation for giving a coworker your username and password?
A) To check email (0 points)
B) To send an important official business email (4 points)
C) Any critical work related function (2 points)
D) Never (10 points)

The above answers related to the question and scoring about KAC3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KAC4. (Possess knowledge regarding when to disable/lock computer)
When you step away from your work computer, what is the most appropriate action to do with your computer?

A) Ask a coworker to watch your system for unauthorized users (4 points)
B) Lock (or disable) the computer (10 points)
C) Turn the monitor off so it appears the computer is shut down (2 points)
D) None of the above (0 points)

The above answers related to the question and scoring about KAC4 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KAC5. (Possess knowledge regarding restricting computer access from visitors)
A visitor from another company needs to email some files to his home office. The visitor asks to use your computer. Which of the following is the most appropriate action?

A) Contact your IT/cybersecurity point of contact (10 points)
B) Allow the visitor to use your computer (2 points)
C) Call the police (0 points)
D) Allow the visitor to use your computer, under your supervision (4 points)

The above answers related to the question and scoring about KAC5 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KAC6. (Possess knowledge regarding understanding who is responsible if computer access is compromised)
Which of the following is most true regarding access control to your work computer?
A) Access control to your computer is an IT responsibility (4 points)
B) Access control to your computer is your responsibility (10 points)
C) Access control to your computer is your supervisor's responsibility (2 points)
D) None of the above (0 points)

The above answers related to the question and scoring about KAC6 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KAC7. (Possess knowledge regarding what to do when access/credential phishing attempts are received)
If you receive a suspicious email indicating it is from IT, asking you to update your password with a link. What should you do?
A) Delete the email, it might be a phishing attempt (4 points)
B) Contact IT to verify their identity and the intent of the email (10 points)
C) Reply to the email, but don't give out your username (2 points)
D) Click on the link and update the password as requested by IT (0 points)

The above answers related to the question and scoring about KAC7 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable

(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

KAC8. (Possess knowledge regarding the what to do when an access compromise occurs)
You notice an email was sent from your email account to a strange email address. You did not send the email. What should you do?
A) Contact IT [or cybersecurity personnel] about the incident (10 points)
B) Ignore the incident since it appears to be a software bug (0 points)
C) Ask your coworkers if they sent the email (2 points)
D) Contact your supervisor (4 points)

The above answers related to the question and scoring about KAC8 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of antivirus software (KAV)
Antivirus software is “a program that attempts to identify, thwart and eliminate computer viruses and other malicious software” (Karantjias & Polemi, 2010, p. 60).

KAV1. (Possess knowledge regarding the definition of antivirus software)
Select the most appropriate definition of “antivirus software”:
A) A program that ensures a computer never gets a virus by firewalling virus infection states (0 points)

B) A program used for cybersecurity of a computer (4 points)
C) A program that attempts to identify, thwart and eliminate computer viruses and other malicious software (10 points)
D) A program that ensures a computer is 100% immune to a computer virus (2 points)

The above answers related to the question and scoring about KAV1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KAV2 (Possess knowledge regarding keeping antivirus definitions current through updates)
Your computer is displaying a message that your antivirus software is out of date. What should you do?
A) Attempt to update the antivirus software thru the antivirus application (10 points)
B) Ignore the message since IT will fix it (2 points)
C) Disregard the message since antivirus automatically updates (4 points)
D) Uninstall the antivirus software (0 points)

The above answers related to the question and scoring about KAV2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of cybersecurity responsibilities (KCR)
Cybersecurity responsibilities include protecting sensitive information, protecting information systems, protecting PII, providing physical security, and potentially updating software (Gross & Rosson, 2007; Karantjias & Polemi, 2010).

KCR1. (Possess knowledge regarding the identification of cybersecurity responsibilities)
Which if the following are your cybersecurity responsibilities for your work computer? Check all that apply.
__ Protecting sensitive information (2 points)
__ Protecting my work computer (2 points)
__ Physically securing my work computer (2 points)
__ Reporting security incidents (2 points)
__ Updating software when needed (2 points)

The above answers related to the question and scoring about KCR1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of cyber threats (KCT)
Cyber threats are any sources or circumstances that have the potential to compromise the confidentiality, integrity, and availability of an information system (Jung, Han, & Suh, 1999; Mejias & Balthazard, 2014).

KCT1. (Possess knowledge regarding the identification of cyber threats)
Which of the following cyber threat definitions are true? Check all that apply.

A) An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access (10 points)
B) Spyware is when an attacker attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion (0 points)
C) A virus is typically an email message that claims to be from a legitimate source but when the user clicks on the link provided, he or she lands on a fake Web page (0 points)
D) Phishing is software secretly installed on a computer without the user's consent that monitors user activity or interferes with user control over a computer (0 points)
E) SPAM is software that can replicate itself and infect a computer without the permission or knowledge of the user (2 points)

The above answers related to the question and scoring about KCT1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KCT2. (Possess knowledge regarding a capability of computer viruses)
Which of the following is most true regarding computer viruses?
A) A virus is capable of erasing all data from a hard drive (10 points)
B) Antivirus software will always protect a computer from all viruses (0 points)
C) Viruses are only spread via emails or Websites (4 points)
D) Only emails with “exe” attachments contain viruses (2 points)

The above answers related to the question and scoring about KCT2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable

(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

KCT3. (Possess knowledge regarding the purpose of phishing attempts)
Which of the following is most accurate regarding phishing attacks?
A) Phishing attacks are always detected by antivirus software (0 points)
B) Phishing attacks are rarely successful (2 points)
C) Phishing attacks may attempt to gain credit card numbers (10 points)
D) Phishing attacks can be effective sometimes (4 points)

The above answers related to the question and scoring about KCT3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

KCT4. (Possess knowledge regarding the purpose of SPAM)
What is the purpose of SPAM?
A) SPAM emails are just harmless advertisements (4 points)
B) SPAM emails are often an identity theft attempt (10 points)
C) SPAM emails are a DDoS attack (2 points)
D) SPAM emails are often insider attacks (0 points)

The above answers related to the question and scoring about KCT4: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral

(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

KCT5. (Possess knowledge regarding a capability of computer spyware)
Which of the following is most true regarding spyware?
A) Spyware is capable of stealing your usernames and passwords (10 points)
B) Antivirus software eliminates the risk of spyware (4 points)
C) Spyware is used to secure your computer from virus threats (0 points)
D) Spyware is not a major threat (2 points)

The above answers related to the question and scoring about KCT5 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

Knowledge of cyber vulnerabilities (KCV)
Cyber vulnerabilities are "weaknesses or flaws, in terms of security and privacy" (Kalloniatis, Mouratidis, & Islam, 2013, p. 4).

KCV1. (Possess knowledge regarding the identification of cyber vulnerabilities)
Identify all of the potential cyber vulnerabilities (check all that apply):
__ Antivirus that has not been updated (1 point)
__ Email that does not filter spam (1 point)
__ Hackers conducting remote attacks (-1 point)
__ Information posted to social networking sites (-1 point)
__ Malware (-1 point)

__ Misconfigured or disabled firewalls (1 point)
__ Misconfigured or disabled antivirus (1 point)
__ Not installing software patches/updates (1 point)
__ Not using antivirus software (1 point)
__ Reused passwords on multiple accounts (1 point)
__ Recycling passwords on the same account (1 point)
__ Unencrypted email (1 point)
__ Trojan Horses (-1 points)
__ Viruses that steal credit card numbers (-1 points)
__ Weak passwords (1 point)

The above answers related to the question and scoring about KCV1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KCV2. (Possess knowledge regarding methods to help protect against insider attacks)
Which of the following protects against insider attacks? Check all that apply.
__ Antivirus software prevents insider attacks (-5 points)
__ Changing file permissions can help prevent data loss from an insider attack (5 points)
__ Restricting user account and user group privileges (5 points)
__ Labeling removable media prevents insider attacks (-5 points)

The above answers related to the question and scoring about KCV2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of email encryption (KEE)
Email encryption is defined as "the process by which [email] is encoded so that only an authorized recipient can decode and consume the [email]" (Microsoft, 2016a).

KEE1. (Possess knowledge regarding the criteria for when to encrypt an email)
When should you encrypt a work email?
A) When it contains personally identifiable information (PII) (4 points)
B) When it contains sensitive information (4 points)
C) When it contains cybersecurity vulnerabilities of the organization (4 points)
D) All of the above (10 points)

The above answers related to the question and scoring of KEE1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of email use (KEU)
"An email acceptable use policy sets out your employees' responsibilities when using email in their day-to-day working activities" (NIBusinessInfo, 2016).

KEU1. (Possess knowledge regarding the acceptable uses of work email)
When using your work email, you should attempt to (check all that apply):
__ delete SPAM (2 points)
__ disable unused security controls (-2 points)
__ forward emails with viruses to IT (-2 points)
__ not forward unnecessary emails such as jokes and chain mail (2 points)

__ prevent downloading of malicious codes and viruses (2 points)
__ scan attachments for viruses (2 points)
__ send personally identifiable information (PII) without encryption (-2 points)
__ encrypt emails that contain sensitive information (2 points)

The above answers related to the question and scoring about KEU1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of cybersecurity POCs (KCP)
Cybersecurity POCs include but are not limited to "computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information officers (CIOs), computer security program managers, and others who are responsible for preparing for, or responding to, security incidents" (Cichonski, Millar, Grance, & Scarfone, 2012, p .1)

KCP1. (Possess knowledge regarding the reporting of cyber incidents to IT or cybersecurity assistance POCs)
When should you report an incident to a cybersecurity point of contact?
A) When you forget your password (0 points)
B) When you leave your desk without locking access to the computer (2 points)
C) When you receive phishing emails (4 points)
D) When a stranger is on your computer without your permission (10 points)

The above answers related to the question and scoring about KCP1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of cyber incident reporting (KIR)
Incident reporting is the act of reporting suspicious individuals, worker misconduct, and all security incidents (Parsons et al., 2014).

KIR1. (Possess knowledge regarding the reporting of cyber incidents regardless of consequence to company reputation)
When the reputation of the company/organization is at stake, it is _______ cybersecurity incidents?
__ acceptable to not report (-10 points)
__ not acceptable to not report (10 points)
__ acceptable to cover-up (-10 points)
__ acceptable to downgrade severity regarding (-10 points)

The above answers related to the question and scoring about KIR1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KIR2. (Possess knowledge regarding the personal consequences for not reporting cyber incidents)
Which of the following most true regarding the failure to report cybersecurity incidents? Check all that apply.
__ Failure to report a cybersecurity incident may result in termination of employment (5 points)
__ It is illegal to fire someone for failure to report a cybersecurity incident (-5 points)

__ Failure to report a cybersecurity incident may result in a suspension (5 points)
__ Failure to report a cybersecurity incident is a minor infraction (-5 points)

The above answers related to the question and scoring about KIR2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KIR3. (Possess knowledge regarding notifying IT or cybersecurity POCs of a quarantined virus)
If your antivirus software identifies and quarantines a virus, what should you do?
A) Immediately have the antivirus software remove the virus from your computer (2 points)
B) Leave the virus in quarantine (4 points)
C) Quarantine is unnecessary, have the antivirus software release the file back to your computer (0 points)
D) Leave the virus in quarantine, and notify IT or cybersecurity personnel (10 points)

The above answers related to the question and scoring about KIR3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____

____

Knowledge of information handling (KIH)
Information handling is the access, creation, destruction, disposition, distribution, maintenance, receipt, storage, transmittal, and use of information (Bernard, 2007).

KIH1. (Possess knowledge regarding the proper destruction of a CD or DVD)
Which of the following are acceptable methods for destroying a CD or DVD that contains sensitive work related information?
A) Throw into the trash (0 points)
B) Shred (10 points)
C) Write on the data side of the disk with a permanent marker (0 points)
D) Scratch the disk with a piece of metal, such as a key or screwdriver (2 points)
E) Break the disk in half (4 points)

The above answers related to the question and scoring about KIH1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KIH2. (Possess knowledge regarding the risks of using thumb drives and USB devices)
Which of the following is most true about thumb drives and USB devices? Check all that apply.
__ Thumb drives and USB devices may execute a virus just by being inserted into a computer (5 points)
__ Thumb drives and USB devices are immune to viruses (-5 points)
__ Thumb drives and USB devices represent no threat to cybersecurity (-5 points)
__ An organization may prohibit the use of thumb drives and USB devices since they are a security risk (5 points)

The above answers related to the question and scoring about KIH2 is: _______

(1) Totally unacceptable

(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

KIH3. (Possess knowledge regarding not posting sensitive information or PII to public domains)
Which of the following is most true about posting sensitive information to a public domain? Check all that apply.
__ Posting sensitive information or PII to a public domain, such as the cloud, is acceptable if it is deleted within 5 minutes (-5 points)
__ Posting sensitive information or PII to a public domain, such as the cloud, is acceptable since it is a secure web-service (-5 points)
__ Posting sensitive information or PII to a public domain, such as the cloud, is typically discouraged, even when the files are encrypted (5 points)
__ Posting sensitive information or PII to a public domain, such as the cloud, is a major cybersecurity incident (5 points)

The above answers related to the question and scoring about KIH3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

Knowledge of information privacy (KIP)

Information privacy is defined as “the claim of individuals, groups, or institutions to determine when, and to what extent, information about them is communicated to others” (Lallmahamood, 2007, p. 7).

KIP1. (Possess knowledge regarding the consequences for violating information privacy laws)
Which of the following is most true regarding information privacy laws?
A) You may be found personally liable for breaking information privacy laws (5 points)
B) Your company may be liable for your conduct when breaking information privacy laws (5 points)
C) Both A and B (10 points)
D) None of the above (0 points)

The above answers related to the question and scoring about KIP1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of Internet use (KIU)
An acceptable Internet use policy defines “guidelines for employees indicating both acceptable and unacceptable Internet usages, with the intention of controlling employee [behaviors] and actions which contribute to the incidence and severity of the [organization’s] Internet risks” (Lichtenstein & Swatman, 1997, p. 1).

KIU1. (Possess knowledge regarding when it is acceptable to use work Internet for personal use)
Which of the following is most true regarding personal Internet use at work? Check all that apply.
__ Browsing the Internet for personal use during a lunch break is acceptable if company policy allows it (5 points)
__ Browsing the Internet for personal use is always acceptable if you have an Internet connection (-5 points)

__ Browsing the Internet for personal use is acceptable if your company does not monitor Internet usage (-5 points)
__ Personal Internet use should be done on your personal device (5 points)

The above answers related to the question and scoring about KIU1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KIU2. (Possess knowledge regarding using peer-to-peer file sharing software)
Using peer-to-peer file sharing software at work _______.
A) may be a cybersecurity risk (4 points)
B) may be acceptable if the software is approved by company policy (4 points)
C) such as FTP software, is not completely secured (4 points)
D) all of the above (10 points)

The above answers related to the question and scoring about KIU2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KIU3. (Possess knowledge regarding when it is acceptable to visit suspicious non-secured Websites)
When is it appropriate to visit a suspicious non-secured Website using your work computer?
A) Always (0 points)
B) When your supervisor directs you to do so (4 points)
C) Never (10 points)
D) Only when your antivirus is up to date (2 points)

The above answers related to the question and scoring about KIU3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KIU4. (Possess knowledge regarding the when it is acceptable to download software)
Downloading software that is not approved by your organization is acceptable _________.
A) when the software comes from a reputable Website (2 points)
B) whenever your supervisor directs you to do so (4 points)
C) when your antivirus is up to date (0 points)
D) none of the above (10 points)

The above answers related to the question and scoring about KIU4 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of mobile computing risks (KMC)
Mobile computing is defined as "using portable computers capable of wireless networking" (Johansson & Andersson, 2015, p. 1).

KMC1. (Possess knowledge regarding the risks to drive security when using public Wi-Fi)
If you have a mobile device that contains sensitive information, when is it acceptable to connect to public free Wi-Fi?
A) Always (0 points)
B) Never (10 points)
C) Rarely (4 points)
D) When directed by your supervisor to do so (2 points)

The above answers related to the question and scoring about KMC1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KMC2. (Possess knowledge regarding the risks to email security when using public Wi-Fi)
When is it safe to use public free Wi-Fi to connect to your work email that contains sensitive information?
A) When your hard drive is encrypted (2 point)
B) When using encrypted email (4 points)
C) Always (0 points)
D) Never (10 points)

The above answers related to the question and scoring about KMC2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of password reuse (KPR)
Password reuse is using the same password for multiple accounts (Ives, Walsh, & Schneider, 2004).

KPR1. (Possess knowledge regarding creating unique passwords for accounts/logins)
Why is it appropriate to use the same password on all of your home and personal accounts/logins?
A) It reduces the need to write down passwords (4 points)
B) It reduces the probably of lockout due to forgotten passwords (2 points)
C) It makes it easier to share passwords with coworkers (0 points)
D) You should not use the same password on all of your accounts (10 points)
E) None of the above (0 points)

The above answers related to the question and scoring about KPR1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of phishing (KP)
Phishing is defined as “a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion” (Jakobsson & Myers, 2007, p. 1).

KP1. (Possess knowledge regarding protection against phishing)
Which of the following protect against or help avoid phishing? Check all that apply.
__ Avoid Websites with expired certificates (-5 points)
__ Antivirus and Anti-Spyware software (-5 points)
__ Digitally signed emails (5 points)
__ Not participating in email and phone surveys from unknown senders (5 points)
__ Firewalls (-5 points)

The above answers related to the question and scoring about KP1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KP2. (Possess knowledge regarding the goal of phishing emails with embedded links)
Phishing emails with links typically attempt to _________
A) direct you to a Website that looks real/legitimate in an attempt to steal information (4 points)
B) show what appears to be legitimate text for a Website, but is linked to a malicious Website (4 points)
C) direct you to a Website that will try to get you to input your username and password (4 points)
D) all of the above (10 points)

The above answers related to the question and scoring about KP2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

Provide feedback and alternative **scoring** of the answers (optional):

KP3. (Possess knowledge regarding methods to avoid phishing Websites)
Which of the following practices are used to avoid phishing Websites? Check all that apply.
__ Ensure your antivirus is up to date (-5 points)
__ Type Web addresses instead of using clicking links or pop-ups (5 points)
__ Disable cookies in your browser settings (-5 points)
__ Use bookmarks for Websites whenever possible (5 points)

The above answers related to the question and scoring about KP3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

Provide feedback and alternative **scoring** of the answers (optional):

KP4. (Possess knowledge regarding identifying phishing email narratives (such as free gifts))
Phishing emails attempt to (check all that apply):
__ claim that you must update or validate information (2 points)
__ claim to be from your company, or other plausible sender (2 points)
__ offer to give you a free prizes, such as money (2 points)

__ threaten a serious situation that requires your attention (2 points)
__ can lead to identity theft (2 points)

The above answers related to the question and scoring about KP4 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of physical security (KPS)
Physical security is defined as "physical measures take to safeguard personnel, to protect unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft" (Newsome & Jarmon, 2016, p. 322).

KPS1. (Possess knowledge regarding what to do when an unauthorized person is at a computer)
If you witness an unauthorized person using your computer, what should you do?
A) Have IT disconnect the computer (2 points)
B) Immediately contact a cybersecurity POC, security, or management (10 points)
C) This is not my responsibility (0 points)
D) Confront the individual (4 points)

The above answers related to the question and scoring about KPS1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of cybersecurity policy compliance (KPC)
Policy compliance is the adherence to a policy, where a policy is defined as "a course or principle of action adopted or proposed by a government, party, business, or individual" (Oxford, 2016, p.1).

KPC1. (Possess knowledge regarding the consequences for non-compliance to company cybersecurity policies)
Failure to follow the cybersecurity policies of your organization, such as an Email Acceptable Use Policy, may lead to (check all that apply):
__ being fired (5 points)
__ being reprimanded (5 points)
__ additional antivirus software on your computer (-5 points)
__ additional firewall software on your computer (-5 points)

The above answers related to the question and scoring about KPC1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of sensitive information and personally identifiable information (PII) (KSI)
Sensitive information is defined as "protected information that the owner does not want to reveal to others and not to be divulged outside the [organization] as well as Information about an individual's racial or ethnic origin, criminal record, sexual preferences or practices and other information that include political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, or a trade union" (Ajigini, Van der Poll, & Kroeze, 2012, p. 7).

PII is defined as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (McCallister el al., 2010, p. 7)

KSI1. (Possess knowledge regarding the identification of sensitive information identification)
Which of the following are classified as sensitive information? Check all that apply.
__ Credit card numbers (2 points)
__ Job title (-2 points)
__ Health records (2 points)
__ Marriage license (2 points)
__ Bank statements (2 points)
__ Tax records (2 points)

The above answers related to the question and scoring about KSI1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KSI2. (Possess knowledge regarding the identification of PII)
Which of the following is classified as personally identifiable information? Check all that apply.
__ Bank records (2 points)
__ Social security number (2 points)
__ Mothers maiden name (2 points)
__ Medical records (2 points)
__ Fingerprints (2 points)

The above answers related to the question and scoring about KSI2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of social engineering (KSE)
Social engineering is defined as "the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks" (Abraham & Chengalur-Smith, 2010, p. 183).

KSE1. (Possess knowledge regarding methods to protect against social engineering)
How can you protect yourself from social engineering?
__ Do not participate in telephone surveys (2 points)
__ Do not give out personal information (2 points)
__ Do not electronically sign documents (-2 points)
__ Do not give out computer or network information (2 points)
__ Do not follow instructions from unverified personnel (2 points)
__ Do not throw personal information in the trash without shredding (2 points)
__ Do not log out from your computer at the end of the day (-2 points)
__ Do not use signature blocks in your emails (-2 points)

The above answers related to the question and scoring about KSE1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of social networking security (KSN)
Social networking is defined as “web-based services allowing individuals to: (a) construct a profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and interact with their list of connections and those made by others within that system” (Weeden, Cooke, & McVey, 2013, p. 250).

KSN1. (Possess knowledge regarding the repercussions of posting sensitive information and PII on social networking sites)
Which of the following is most true regarding accidentally or intentionally leaking sensitive information from work on one of you social media accounts.
A) You may lose your job (10 points)
B) Your job cannot punish you due to freedom of speech protection by the Constitution (0 points)
C) Your job cannot punish you if you delete the post (0 points)
D) All of the above (0 points)

The above answers related to the question and scoring about KSN1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of applications strong passwords (KSP)
Passwords are considered strong when “having more than eight characters, at least one change of case, a number that is not at the end, and a non-alphanumeric character such as # or * that is also not at the end of the password” (Keller, Powell, Horstmann, Predmore, & Crawford, 2005, p. 13).

KSP1. (Possess knowledge regarding the properties of a strong password for applications)
What constitutes a strong password?

A) Using a password consisting of 8 lower case letters and upper case letters (2 points)
B) Using a password consisting of 10 lower case letters, upper case letters, and numbers (4 points)
C) Using passphrase consisting of 12 lower case letters, upper case letters, numbers, and special characters (10 points)
D) None of the above (0 points)

The above answers related to the question and scoring about KSP1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Is there any other feedback you would like to submit regarding the knowledge units or knowledge topics?

____

____

Organizational Information System User Cybersecurity Skill Assessment

Skill is defined as a goal-directed, well-organized set of actions that is acquired through practice and performed with economy of effort, which enables a person to do something well (Boyatzis & Kolb, 1995).

Please evaluate the following cybersecurity skill measures and scoring of the measures answers for an organizational information system user (OISU) and rate their acceptability.

Skill in creating strong passwords (SSTP)

SSTP1. (Demonstrate the task of creating strong passwords for user accounts or logins)

SPR1. (Demonstrate the task of creating unique passwords on multiple user accounts or logins)
You are asked to create a password for a work related Website. You are also asked to create a password for a personal home use Website. The requirements for a strong password will be stated as follows: at least 12 total characters, at least 1 lower case letter, at least 1 uppercase letter, at least 1 number, and at least 1 special character. A special character is any of the following: !@#$%^&*(). If you do not reuse passwords for the work and personal Websites, 10 points are awarded for SAC1. If you create one strong password as defined, 5 points are awarded. If you create two strong passwords, 10 points are awarded. If passwords are reused, 0 points are awarded. If both passwords are not strong, 0 points are awarded.

The above answers related to the question and scoring about SSTP1 & SPR1 are: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in preventing unauthorized access to an IS by controlling access to systems (SAC)

SAC1. (Demonstrate the task of keeping a password confidential)
A situation is presented where a coworker is asking for your login credentials. The coworker makes a very convincing argument, where his job is on the line to meet a deadline. If you do not give the coworker your login credentials, 10 points are awarded. If you tell the coworker you need to consult with IT, 4 points are awarded. If you tell the coworker you need to consult with your supervisor, 2 points are awarded. If you give the coworker your password, 0 points are awarded.

The above answers related to the question and scoring about SAC1 is: _______

(1) Totally unacceptable
(2) Unacceptable

(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SAC2. (Demonstrate the task of locking a computer while not in use)
A situation is presented where you are going to leave your desk for a minute, to get a bottle of water. Is there anything you need to do before you leave your desk? If you lock the computer, 10 points are awarded. If you log off from your computer, 10 points are awarded. If you remove your PKI card, 10 points are awarded. If you shutdown the computer, 4 points are awarded. If you turn off the monitor, 2 points are awarded. If you leave without securing the computer, 0 points are awarded.

The above answers related to the question and scoring about SAC2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SAC3. (Demonstrate the task of reporting to IT or cybersecurity POCs that an access compromise has occurred)
A situation is presented where you log in to your computer and notice the wallpaper has been changed to a smiley face with text that says “you’ve been hacked lulz”. What should you do? If you contact IT or cybersecurity POCs, 10 points are awarded. If you run your antivirus to check for viruses, 4 points are

awarded. If you contact your supervisor, 4 points are awarded. If you reset your wallpaper, 0 points are awarded.

The above answers related to the question and scoring about SAC3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Skill in physically protecting an IS from an unauthorized user (SPS)

SPS1. (Demonstrate the task of reporting an unauthorized person on an IS to IT or cybersecurity POCs)
A situation is presented where you go to your desk, but a stranger is there searching through a work folder on your computer. How should you handle the situation? If you contact IT, security, cybersecurity POCs, or management, then 10 points are awarded. If you confront the stranger, 4 points are awarded. If you leave the area without reporting the incident, 0 points are awarded. If you assume the stranger is an IT technician and let the person continue to work, 0 points are awarded.

The above answers related to the question and scoring about SPS1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Skill in using an antivirus application to properly update the software when notified that antivirus requires an update (SAV)

SAV1. (Demonstrate the task of updating antivirus software when notified that an antivirus software update is available)
A situation is presented where you log in to your computer and a message appears that says the antivirus needs to be updated. You are shown a screenshot of a computer desktop with a pop-up by the operating system asking to update, or close to ignore. If you choose to update the antivirus software, 10 points are awarded. If you contact IT, 4 points are awarded. If you choose to ignore because the software will auto-update eventually, 0 points are awarded. If you choose to ignore because this may be a virus, 0 points are awarded.

The above answers related to the question and scoring about SAV1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Skill in configuring and using email in a manner that prevents sensitive information and PII loss (SES)
Email security is the secure use of email that ensures the protection of sensitive information and PII, as well as preventing the propagation of malicious code (Carlton et al., 2015; DISA, 2015; Wang, Li, & Cheng, 2014).

SES1. (Demonstrate the task of not downloading malicious code)
A situation is presented where you receive an email with an attachment. The attachment is called poker.txt, and the email says if you change it to poker.exe, you can run it and play a poker game. This email did come for a coworker. If you do not download the attachment, 10 points are awarded. If you contact IT for

assistance, 4 points are awarded. If you download the attachment, 0 points are awarded. If you download the attachment and virus scan it, 0 points are awarded.

The above answers related to the question and scoring about SES1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SES2. (Demonstrate the task of encrypting an email)
A situation is presented where you receive an email from your supervisor asking you to send a list of social security numbers. You are shown an email client window and asked an action to choose. If you encrypt the email and send the social security numbers, 10 points are awarded. If you reply to your supervisor that you cannot send this information via email, 4 points are awarded. If you reply to your supervisor that you will print the information and hand deliver it to him, 2 points are awarded. If you send the email without encrypting, 0 points are awarded.

The above answers related to the question and scoring about SES2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SES3. (Demonstrate the task of not using work email for personal use)
A situation is presented where you receive an email from a coworker that says “if you forward this to 20 people you will become rich”. If you delete or ignore the email, 10 points are awarded. If you reply to the sender, asking kindly to keep you off such emails, 10 points are awarded. If you forward the email to your friends, and ask the sender not to send you emails like this in the future, 2 points are awarded. If you choose to forward the email to your friends, 0 points are awarded.

The above answers related to the question and scoring about SES3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SES4. (Demonstrate the task of using digital signatures when sending emails)
A situation is presented where you need to email two-dozen coworkers an update on your project. You are presented with an email client with the email already filled out. This email does not include any sensitive information or PII. There are multiple actions that you are able to choose before sending the email such as: digitally signing the email, requesting a read receipt, requesting a delivery reciept, and having the email peer reviewed to check for sensitive information or PII. If you digitally sign the email, 10 points are awarded. All other options contribute 0 points.

The above answers related to the question and scoring about SES4 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SES5. (Demonstrate the task of virus-scanning Email attachments)
A situation is presented where you receive an email from a software vendor with an attachment. The attachment is a PDF file that contains updated instructions for their software that you have been waiting to receive. If you scan the PDF attachment, 10 points are awarded. If you download the file without scanning it first, 0 points are awarded. If you forward the email to IT to have the attachment virus scanned, 0 points are awarded. If you don't trust the source and delete the email, 0 points are awarded.

The above answers related to the question and scoring about SES5 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in cybersecurity incident reporting (SIR)

SIR1. (Demonstrate the task of reporting coworker misconduct that violates a company cybersecurity policy)
A situation is presented where you witness a coworker using peer-to-peer file sharing software. This software is not allowed by the company security policy. If you report the coworker to IT or cybersecurity POCs, 10 points are awarded. If you advise the coworker to uninstall the software and do not report the incident, 0 points are awarded. If you ask the coworker for a copy of the software, 0 points are awarded. If you ignore the incident since it is not your job to monitor cybersecurity, 0 points are awarded.

The above answers related to the question and scoring about SIR1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SIR2. (Demonstrate the task of reporting a ransomware attack)
A situation is presented where your system appears to have been infected with ransomware. Your system contains information such as customer credit card transactions and sensitive company information. The ransomware states that your system is now encrypted, and if you do not pay $500 to the specified account within 24 hours, you will not get the decryption key. If you report the incident to IT or cybersecurity POCs, 10 points are awarded. If you immediately unplug the computer and report the incident to IT or cybersecurity POCs, 10 points are awarded. If you immediately pay the ransom, 0 points are awarded. If you wait the 24 hours to see if the ransomware is a legitimate threat, 0 points are awarded.

The above answers related to the question and scoring about SIR2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Skill in avoiding suspicious and malicious Websites when using the Internet at work (SIU)

SIU1. (Demonstrate the task of identifying and avoiding a malicious popup window)
A situation is presented where you click on a Website and a popup is shown stating that your computer is infected. The popup has a link that says it will fix the infection. If you close the window, or leave the Webpage, and you do not click the link in the popup, 10 points are awarded. If you shutdown your computer to avoid a virus, 4 points are awarded. If you hold the power button to your computer to force a shutdown to avoid a virus, 2 points are awarded. If you click the link in the popup, 0 points are awarded.

The above answers related to the question and scoring about SIU1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SIU2. (Demonstrate the task of identifying and avoiding dubious or pornographic Websites)
A situation is presented where you need to find a rental car for your business trip. The first result in your search is Website called www.free-rides.xxx/redirect. If you do not click the link, 10 points are awarded. If you call IT for assistance, 4 points are awarded. If you click the link, 0 points are awarded. If you decide Website reservations are too risky and will rent a car when you get to the airport, 0 points are awarded.

The above answers related to the question and scoring about SIU2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable

(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SIU3. (Demonstrate the task of not using credit cards on non-secured Websites)
A situation is presented where you need to reserve a rental car for your business trip. You visit a rental car Website that was referred to you by your supervisor and select a car to reserve with your company/corporate credit card. The page on the Website where you enter the credit card number does not start with 'https' and does not have a symbol representing that the site is secure. If you choose to go to another Website, 10 points are awarded. If you call your supervisor for assistance, 4 points are awarded. If you call IT for assistance, 4 points are awarded. If you enter the credit card number, 0 points are awarded.

The above answers related to the question and scoring about SIU3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Skill in avoiding actions that increase exposure to malicious code downloading or execution (SMC)
Malicious code is capable of giving hackers access to a network or system, erase hard drives, and corrupt files (DISA, 2015). Examples of malicious code are viruses, worms, Trojan horses, spyware, and scripts (DISA, 2015).

SMC1. (Demonstrate the task of not using links within emails)

A situation is presented where you mistakenly leave your email in html view. You receive and an email from a coworker that only has a hyperlink that says, “click this link to see how much our boss makes”. If you do not click the link, 10 points are awarded. If you call IT for assistance, 4 points are awarded. If you call your supervisor for assistance, 4 points are awarded. If you click the link, 0 points are awarded.

The above answers related to the question and scoring about SMC1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SMC2. (Demonstrate the task of disabling automatic downloads in a Web browser)
A situation is presented where you need to download a file from the Internet. The Web browser allows you to select “enable automatic downloads”, or “disable automatic downloads” and just retrieve this single file. If you disable automatic downloads, 10 points are awarded. If you call IT for assistance, 2 points are awarded. If you call your supervisor for assistance, 2 points are awarded. If you enable automatic downloads, 0 points are awarded.

The above answers related to the question and scoring about SMC2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

SMC3. (Demonstrate the task of virus scanning a CD/DVD/thumb-drive)
A situation is presented where you are given a CD that has important work data that needs to be transferred to your computer. If you scan the CD for viruses before transferring the files, 10 points are awarded. If you call IT for assistance, 2 points are awarded. If you call your supervisor for assistance, 2 points are awarded. If you transfer the files without scanning for viruses, 0 points are awarded.

The above answers related to the question and scoring about SMC3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

SMC4. (Demonstrate the task of not forwarding infected files)
A situation is presented where you have a file on your computer that is infected and quarantined. If you email IT to report the incident and do not attach the infected file, 10 points are awarded. If you call IT about the issue, 10 points are awarded. If you leave the file in quarantine, 2 points are awarded. If you email IT and forward the infected file, 0 points are awarded.

The above answers related to the question and scoring about SMC4 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Skill in securely operating mobile computing devices (SMS)
Mobile computing is defined as "using portable computers capable of wireless networking" (Johansson & Andersson, 2015, p. 1).

SMS1. (Demonstrate the task of locking a mobile device when not in use)
A situation is presented where you are given a laptop to take to a training class in another city. You get to the training class and log in to your laptop. The trainer states that the first four hours of class are lecture, and there is no need for the laptop. If you lock the laptop while it's not being used, 10 points are awarded. If you shut down the laptop, 10 points are awarded. If you close your laptop, 4 points are awarded. If you leave the laptop open, and stay logged in, 0 points are awarded.

The above answers related to the question and scoring about SMS1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SMS2. (Demonstrate the task of disabling wireless capabilities when the IS is using a LAN)
A situation is presented where you are given a laptop to take to a training class in another city. You get to the training class and log in to your laptop. The trainer states that you have a LAN cable to connect to the network for class. If you disable Wi-Fi, 10 points are awarded. If you ensure your firewall is enabled, 4 points are awarded. If you ensure your antivirus is enabled, 4 points are awarded. If you do nothing but plug in the LAN cable, 0 points are awarded.

The above answers related to the question and scoring about SMS2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SMS3. (Demonstrate the task of encrypting sensitive information or PII when using a mobile device such as a laptop)
A situation is presented where you are given a laptop to take on a business trip in Chicago. While in Chicago, you finish a report that needs to be sent to management as soon as possible. This report contains sensitive information about your company. How do you transmit the information to your company from your Wi-Fi enabled laptop? If you send an encrypted email, 10 points are awarded. If you send an email with an encrypted document, you are awarded 10 points. If you decide emailing sensitive information from a Wi-Fi enabled laptop is too risky, 2 points are awarded. If you send an email that is not encrypted, 0 points are awarded.

The above answers related to the question and scoring about SMS3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SMS4. (Demonstrate the task of disabling wireless capabilities when the mobile device is not in use)
A situation is presented where you are given a laptop to take to a training class in Chicago. Class is breaking for lunch, and you are leaving your laptop in class. If you disable Wi-Fi while out for lunch, 10 points are awarded. If you shut down the laptop while out for lunch, 2 points are awarded. If you lock the computer, 2 points are awarded. If you leave the computer without disabling Wi-Fi or shutting down since the computer is in a secure environment, 0 points are awarded.

The above answers related to the question and scoring about SMS4 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in avoiding a phishing attempt (SP)
Phishing is defined as “a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion” (Jakobsson & Myers, 2007, p. 1).

SP1. (Demonstrate the task of not divulging sensitive information or PII to a phishing attempt)
A situation is presented where you are looking at your email inbox that contains several unread emails. The first email is from an unknown sender with a title that says, “Hurry…cash prizes expire today”. If you delete the email without opening, 10 points are awarded. If you open the email, but do not click the (phishing) link, 6 points are awarded. If you open the email, but do not click the link, and then contact IT regarding the situation, 2 points are awarded. If you open the email and click the link, 0 points are awarded.

The above answers related to the question and scoring about SP1 is: _______

(1) Totally unacceptable

(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

SP2. (Demonstrate the task of verifying the identity of an email sender to prevent the divulging of sensitive information or PII to a phishing attempt)
A situation is presented where you are looking at your email inbox that contains several unread emails. The second email is from someone you don't know, Mr. Solo, with a title that says, "Emergency! Response needed!" You open the email at it states that you must email your name and social security number to Mr. Solo at corporate HR to payroll issue. His email address appears to be h.solo.12@yourcompany.com. If you attempt to verify the identity of Mr. Solo and the authenticity of the email, 10 are points awarded. If you delete the email, or do not respond, 6 points are awarded. If you contact IT regarding the email, 4 points are awarded. If you respond to the email with your name and social security number, 0 points are awarded.

The above answers related to the question and scoring about SP2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

Skill in avoiding a spear-phishing attempt (SSP)

Spear-phishing is defined as “a type of phishing attack that targets particular individuals, groups of people, or organizations” (DISA, 2015).

SSP1. (Demonstrate the task of not divulging sensitive information or PII to a spear-phishing attack that mimics coworker)
A situation is presented where you are looking at your email inbox that contains several unread emails. The third email appears to be from Ann Jones in accounting, but the email address is suspicious, it’s not the company email. The email title says, “Hurry, it’s Ann Jones from finance, I need your social security number fast for payroll”. You open the email at it states that you must click on this link to send your name and social security number immediately. If you delete the email without opening, 10 points are awarded. If you contact IT (or cybersecurity POCs) regarding this phishing attempt, 10 points are awarded. If you open the email, but do not click the link, 6 points are awarded. If you click the link and give your name as well as social security number, 0 points are awarded.

The above answers related to the question and scoring about SSP1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SSP2. (Demonstrate the task of not divulging sensitive information or PII to a spear-phishing attack that states your name)
A situation is presented where you are looking at your email inbox that contains several unread emails. The fourth email is from an unknown source. The email title has your name and it says, “Rick Grimes, see what was posted on the Internet about you”. You open the email and it states that you can click on this link to remove your secrets from the Internet. If you delete the email, 10 points are awarded. If you contact IT (or cybersecurity POCs) regarding this spear-phishing attempt, 10 points are awarded. If you contact your supervisor for assistance, 2 points are awarded. If you open the email and click the link, 0 points are awarded.

The above answers related to the question and scoring about SSP2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in avoiding a whaling attempt (SW)
Whaling is a form of spear-phishing that targets high-level personnel (DISA, 2015).

SW1. (Demonstrate the task of not divulging sensitive information or PII to a whaling attack)
A situation is presented where you are looking at your email inbox that contains several unread emails. The fifth email is from an unknown source. The email title has says, “Immediately help the company President, Joe Thomas”. You open the email and it states that you need to reply with the phone number and date of birth of Joe Thomas, the company President, to confirm his identity against a possible media scandal. If you delete the email, 10 points are awarded. If you contact IT (or cybersecurity POCs) regarding this whaling attempt, 10 points are awarded. If you contact your supervisor for assistance, 2 points are awarded. If you reply with the requested information, 0 points are awarded.

The above answers related to the question and scoring about SW1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____

____

Skill in using authorized systems for sensitive information and PII data processing as well as transmissions (SSI)

SSI1. (Demonstrate the task of not using an unauthorized system when dealing with sensitive information and PII)
A situation is presented where you have a CD with a document you need to update. The document contains company credit card numbers and is only allowed on specific computers in the office, per company policy. The building is closing soon and this work needs to be completed for a morning meeting. If you do not take the CD home to work on it, 10 points are awarded. If you email the document to your personal email account at home, 0 points are awarded. If you take the CD home, 0 points are awarded. If you make a copy of the CD to take home, 0 points are awarded.

The above answers related to the question and scoring about SSI1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SSI2. (Demonstrate the task of not using non-secured text message to transmit sensitive information or PII)
A situation is presented where a coworker sends you a text message, requesting that you reply with the company expense credit card number and PIN, for an official business purchase. If you decline, and tell your coworker that sending the text is a security violation, 10 points are awarded. If you do not respond to the text and notify your supervisor, 10 points are awarded. If you send the information to your coworker, 0 points are awarded. If you send the credit card number to your coworker in one text, then send the PIN in a separate text, 0 points are awarded.

The above answers related to the question and scoring about SSI2 is: _______

(1) Totally unacceptable

(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Skill in using encryption to store data on approved removable media (SMU)

SMU1. (Demonstrate the task of using approved/appropriate removable media) A situation is presented where you need to place a document containing sensitive company information onto some form of removable media. The company policy allows CDs and DVDs, but not USB devices. If you use a CD, 10 points are awarded. If you use a DVD, 10 points are awarded. If you use a USB hard drive, 0 points are awarded. If you use a thumb drive, 0 points are awarded.

The above answers related to the question and scoring about SMU1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SMU2. (Demonstrate the task of encrypting data when using removable media) A situation is presented where you need to place a document containing sensitive company information onto a CD. If you encrypt the document for the CD, 10 points are awarded. If you change the file name to “chili recipe.doc” for the CD, 0 points are awarded. If change the file extension to “.exe” for the CD, 0 points are awarded. If you import the contents of the document into a spreadsheet, then hide the columns containing the sensitive information, 0 points are awarded.

The above answers related to the question and scoring about SMU2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in identifying sensitive information and PII (SSII)

SSII1. (Demonstrate the task of identifying an address and phone number as PII) A situation is presented where you need to dispose of a pile of documents. Several of the documents contain all of the addresses and phone numbers of everyone in the building. If you shred the documents, 10 points are awarded. If you recycle the documents, 0 points are awarded. If you throw the documents into the trash, 0 points are awarded. If you take the documents home for destruction, 0 points are awarded.

The above answers related to the question and scoring about SSII1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SSII2. (Demonstrate the task of identifying proprietary information as sensitive information)
A situation is presented where you receive an unencrypted email containing the technical specifications of the new secret product your company is developing. If you immediately notify IT (or cybersecurity POCs) by phone or in person to report the incident, 10 points are awarded. If you forward the email to IT (or cybersecurity POCs), 2 points are awarded. If you forward the email to your supervisor, 2 points are awarded. If you delete the email, 0 points are awarded.

The above answers related to the question and scoring about SSII2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in avoiding social engineering attempts of sensitive information and PII (SSE)

SSE1. (Demonstrate the task of identifying and avoiding social engineering attempts by text messages)
A situation is presented where you receive text message. The message says, “I’m the new guy Andy in IT. I forgot the office Wi-Fi password. Can you text it to me?” If you do not send the password, 10 points are awarded. If you contact IT (or cybersecurity POCs), 10 points are awarded. If you reply to Andy and tell him to come by your desk, 6 points are awarded. If you send the password, 0 points are awarded.

The above answers related to the question and scoring about SSE1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SSE2. (Demonstrate the task of identifying and avoiding social engineering by vishing surveys)
A situation is presented where you receive a phone call from Dan in HR. You have heard of Dan, but have never talked to him. He asks if you can take a quick survey about your IT equipment, to see if anything needs to be upgraded. If you ask Dan to come by your desk to confirm his identity, 10 points are awarded. If you decline to give Dan the information, and notify IT (or cybersecurity POCs), 10 points are awarded. If you hang up on Dan, 6 points are awarded. If you take the survey, 0 points are awarded.

The above answers related to the question and scoring about SSE2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

SSE3. (Demonstrate the task of identifying and avoiding social engineering by public conversations)
A situation is presented where you are at lunch with your coworker Harley, at the sandwich shop across the street from the office. Harley starts to talk about all of the credit card accounts bring processed in her office. If you stop this conversation, 10 points are awarded. If you let Harley talk about the credit card processing, but do not divulge any information yourself, 0 points are awarded. If you tell Harley that other people don’t need to hear this information, so she should speak more quietly, 0 points are awarded. If you let the conversation continue and participate freely, 0 points are awarded.

The above answers related to the question and scoring about SSE3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in using social networking without divulging sensitive information and PII (SSN)

SSN1. (Demonstrate the task of using a social network without divulging PII)
A situation is presented where you see on your social media account where a lot of your friends are replying to a post where they are stating the make and model of their first car. If you warn your friends that this is PII that they shouldn’t share, 10 points are awarded. If you do not post this information, 10 points are awarded. If you post this information, 0 points are awarded. If you post a picture of the car, 0 points are awarded.

The above answers related to the question and scoring about SSN1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

SSN2. (Demonstrate the task of using a social network without divulging sensitive information)

A situation is presented where you see on your social media account where people are posting their work phone number and job title to a post from a large business for a chance to win $50,000. If you warn your friends that this is sensitive information that they shouldn’t share, 10 points are awarded. If you do not post this information, 10 points are awarded. If you post this information, 0 points are awarded. If you post your home phone number and job title, 0 points are awarded.

The above answers related to the question and scoring about SSN2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in identifying the spillage of sensitive information and PII (SS)
Spillage occurs “when information is spilled from a higher classification or protection level to a lower classification or protection level” (DISA, 2015).

SS1. (Demonstrate the task of reporting a spillage incident)
A situation is presented where you receive an email that appears to have accidentally included social security numbers of customers. This email was sent to dozens of internal and external entities, and was not encrypted. If you report this incident to IT (or cybersecurity POCs), 10 points are awarded. If you reply to the sender that the email is a security violation, 2 points are awarded. If you delete the email, 0 points are awarded. If you it’s not your job to handle this situation, 0 points are awarded.

The above answers related to the question and scoring about SS1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in using encryption to transmit sensitive information and PII when using Webmail (SWM)

SWM1. (Demonstrate the task to use encryption when sending sensitive information or PII with Webmail)
A situation is presented where your supervisor asks for a list of coworker social security numbers. An option is presented to send the social security numbers, unencrypted, thru Webmail. If you send the social security numbers in an encrypted Webmail, 10 points are awarded. If you report the incident to IT or cybersecurity POCS, 0 points are awarded. If you send the social security numbers in an unencrypted email, 0 points are awarded. If you inform your supervisor that this would be a security violation, 0 points are awarded.

The above answers related to the question and scoring about SWM1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Is there any other feedback you would like to submit regarding the skill areas or skill tasks?

Feedback

Is there any other feedback you would like to submit regarding the content of this survey?

Appendix F

Phase 2 Round 2 Survey

Dear Cybersecurity Expert,

This survey will be completed using the Delphi method. All participants are subject matter experts in this area. This survey is a continuation of the Phase 2 Round 1 survey. Results and feedback from the Phase 2 Round 1 survey revealed that 29 of 90 proposed KSA measurement methods require refinement. This survey intends to validate methods for measuring the cybersecurity knowledge, skills, and abilities (KSAs) that an organizational information system user must possess. Such users include: IT personnel, secretaries, accountants, technical writers, physicians, etc.

Please respond to all questions as honestly and accurately as possible. By completing this survey you agree and understand that your responses are voluntary. Measures will be taken to ensure than responses are anonymous and cannot be traced to any individual. You may exit this survey at any time. In the event that you chose to exit this survey, your responses will not be recorded. By participating in this survey you certify that you are over the age of 18 years old.

Demographics

What is your age?

A) Under 20
B) 20-29
C) 30-39
D) 40-49
E) 50-59
F) Over 60

What is your gender?

A) Female
B) Male

What is your job function?

A) Administrative staff
B) Cybersecurity/IT staff
C) Engineer
D) Manager
E) Operations

F) Professional staff
G) Scientist
H) Security operator
I) Teacher/Professor
J) Technical staff
K) Other

How long have you been with your current organization?

A) Under 1 year
C) 1 – 5 years
D) 6 – 10 years
E) 11 – 15 years
F) 16 – 20 years
G) 21 – 25 years
H) 26 – 30 years
I) Over 30 years

Which describes your current employer?

A) Academia
B) Federal government employee
C) Private sector company
D) State government employee
E) Other

What is your highest level of education?

A) High school diploma
B) 2-year college (Associates degree)
C) 4-year college (Bachelors degree)
D) Graduate degree
E) Doctorate
F) Other

Which cybersecurity certifications do you possess?
____
____

Organizational Information System User Cybersecurity Knowledge Assessment

Cybersecurity as defined by the Association of Computing Machinery Joint Task Force (ACMJTF) on Cybersecurity Education (2016) is "computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (p. 1).

Knowledge is defined by Alavi and Leidner (2001) as "a justified belief that increases an entity's capacity for taking effective action" (p. 109).

Please evaluate the following cybersecurity knowledge measures and scoring of the measure answers for an organizational information system user (OISU) and rate their acceptability.
Note: questions in the form of "check all that apply" deduct points for incorrect selections. The need to deduct points for incorrect selections is needed to ensure maximum points are not achieved by simply "checking" all options, without penalty. Additionally, these "check all that apply" questions will have a minimum score of zero. Hence, multiple negative point selections for a question will not produce a negative score.

Knowledge of access control (KAC)
Access control is defined as "the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner" (Lopez, Oppliger, & Pernul, 2004, p. 580).

KAC1. (Possess knowledge regarding identifying the risk of writing down passwords)
When writing down a login password, it is best to hide the password under your keyboard where it is not visible.
A) Yes, this is easily accessible (0 points)
B) No, inside a desk drawer is more secure (0 points)
C) No, you should not write down your passwords, unless it will be stored in a secure container such as a safe (10 points)
D) No, you should place it on your monitor or somewhere visible, in case your coworkers need it to log in (0 points)
The above answers related to the question and scoring about KAC1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____

KAC2. (Possess knowledge regarding how often passwords should be changed)
Which is the most reasonable timeframe for changing passwords?

A) Daily (0 points)
B) Weekly (4 points)
C) Quarterly (10 points)
D) Never (0 points)
The above answers related to the question and scoring about KAC2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

Provide feedback and alternative **scoring** of the answers (optional):

KAC3. (Possess knowledge regarding identifying the need to keep passwords confidential)
Which of the following is an acceptable situation for giving a coworker your username and password?
A) To check email (0 points)
B) To send an important official business email (4 points)
C) To perform a critical work related function (2 points)
D) Never (10 points)
The above answers related to the question and scoring about KAC3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

Provide feedback and alternative **scoring** of the answers (optional):

____

____

KAC5. (Possess knowledge regarding restricting computer access from visitors)
A visitor from another company needs to email some files to his home office. The visitor asks to use your computer. Which of the following is the appropriate action?
A) Contact your IT/cybersecurity point of contact for guidance (8 points)
B) Ask a coworker for guidance (2 points)
C) Do not allow the visitor to use your computer (10 points)
D) Allow the visitor to use your computer, under your supervision (0 points)
The above answers related to the question and scoring about KAC5 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

KAC6. (Possess knowledge regarding understanding who is responsible if computer access is compromised)
Which of the following is true regarding access control to your work computer?
A) Who sits at your computer is primarily an IT responsibility (4 points)
B) Who sits at your computer is primarily your responsibility (10 points)
C) Who sits at your computer is primarily your supervisor's responsibility (2 points)
D) None of the above (0 points)
The above answers related to the question and scoring about KAC6 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable

(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of cybersecurity POCs (KCP)
Cybersecurity POCs include but are not limited to “computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information officers (CIOs), computer security program managers, and others who are responsible for preparing for, or responding to, security incidents” (Cichonski, Millar, Grance, & Scarfone, 2012, p .1)

KCP1. (Possess knowledge regarding the reporting of cyber incidents to IT or cybersecurity assistance POCs)
When should you report an incident to a cybersecurity point of contact?
A) When you forget your password (0 points)
B) When you leave your desk without locking access to the computer (2 points)
C) When you receive an email from an unknown source (4 points)
D) When a stranger is on your computer without your permission (10 points)
The above answers related to the question and scoring about KCP1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Knowledge of cybersecurity responsibilities (KCR)
Cybersecurity responsibilities include protecting sensitive information, protecting information systems, protecting PII, providing physical security, and potentially updating software (Gross & Rosson, 2007; Karantjias & Polemi, 2010).

KCR1. (Possess knowledge regarding the identification of cybersecurity responsibilities)
Which if the following are your cybersecurity responsibilities for your work computer? Check all that apply.
__ Protecting sensitive information (2 points)
__ Protecting my work computer (2 points)
__ Physically securing my work computer (2 points)
__ Reporting security incidents (2 points)
__ Protecting personally identifiable information (PII) (2 points)
The above answers related to the question and scoring about KCR1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of cyber threats (KCT)
Cyber threats are any sources or circumstances that have the potential to compromise the confidentiality, integrity, and availability of an information system (Jung, Han, & Suh, 1999; Mejias & Balthazard, 2014).

KCT1. (Possess knowledge regarding the identification of cyber threats)
Which of the following cyber threat definitions are true? Check all that apply.
A) An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access (10 points)
B) Spyware is when an attacker attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion (0 points)
C) A virus is typically an email message that claims to be from a legitimate source but when the user clicks on the link provided, he or she lands on a fake Web page (0 points)
D) Phishing is software secretly installed on a computer without the user's consent that monitors user activity or interferes with user control over a computer (0 points)
E) SPAM is software that can replicate itself and infect a computer without the permission or knowledge of the user (2 points)

The above answers related to the question and scoring about KCT1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KCT2. (Possess knowledge regarding a capability of computer viruses)
Which of the following is most true regarding computer viruses?
A) A virus is capable of erasing all data from a hard drive (10 points)
B) Antivirus software will always protect a computer from all viruses (0 points)
C) Viruses are only spread via emails or Websites (2 points)
D) Only emails with “exe” attachments contain viruses (1 point)
The above answers related to the question and scoring about KCT2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KCT3. (Possess knowledge regarding the purpose of phishing attempts)
Which of the following is most accurate regarding phishing attacks?
A) Phishing attacks are always detected by antivirus software (0 points)
B) Phishing attacks are rarely successful (2 points)
C) Phishing attacks may attempt to gain credit card numbers (10 points)

D) Phishing attacks may attempt to gain your access credentials (10 points)
The above answers related to the question and scoring about KCT3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KCT4. (Possess knowledge regarding the purpose of SPAM)
What is a purpose of SPAM?
E) SPAM emails are just harmless advertisements (4 points)
F) SPAM emails are often an identity theft attempt (10 points)
G) SPAM emails are a DDoS attack (2 points)
H) SPAM emails are often insider attacks (0 points)

The above answers related to the question and scoring about KCT4: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KCT5. (Possess knowledge regarding a capability of computer spyware)
Which of the following is most true regarding spyware?
A) Spyware is capable of stealing your usernames and passwords (10 points)
B) Antivirus software eliminates the risk of spyware (2 points)

C) Spyware is used to secure your computer from virus threats (0 points)
D) Spyware is not a major threat (2 points)

The above answers related to the question and scoring about KCT5 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KCT6. (Possess knowledge regarding the purpose of ransomware)
Which of the following is a purpose of ransomware?
A) Ransomware is a form of SPAM that attempts to trick the user into paying a ransom (2 points)
B) Ransomware will encrypt the files files on a computer and will not divulge the decryption key unless a ransom is paid (10 points)
C) Ransomware can replicate throughout a network and infect all connected systems (10 points)
D) Ransomware is typically a hoax attempting to steal money from a user (2 points)
The above answers related to the question and scoring about KCT6 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of cyber incident reporting (KIR)
Incident reporting is the act of reporting suspicious individuals, worker misconduct, and all security incidents (Parsons et al., 2014).

KIR1. (Possess knowledge regarding the reporting of cyber incidents regardless of consequence to company reputation)
When the reputation of the company/organization is at stake, it is _______ cybersecurity incidents?
__ acceptable to not report (0 points)
__ acceptable to report (10 points)
__ acceptable to cover-up (0 points)
__ acceptable to downgrade severity regarding (0 points)

The above answers related to the question and scoring about KIR1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of information handling (KIH)
Information handling is the access, creation, destruction, disposition, distribution, maintenance, receipt, storage, transmittal, and use of information (Bernard, 2007).

KIH1. (Possess knowledge regarding the proper destruction of a CD or DVD)
What is the desired method for destroying a CD or DVD that contains sensitive work related information:
A) Throw into the trash (0 points)
B) Shred (10 points)
C) Write on the data side of the disk with a permanent marker (0 points)
D) Scratch the disk with a piece of metal, such as a key or screwdriver (2 points)
E) Break the disk in half (4 points)
The above answers related to the question and scoring about KIH1 is: _______

(1) Totally unacceptable

(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KIH3. (Possess knowledge regarding not posting sensitive information or PII to public domains)
Which of the following is true about posting sensitive information to a public domain? Check all that apply.
__ Posting sensitive information or PII to a public domain, such as the cloud, is acceptable if it is deleted within 5 minutes (0 points)
__ Posting sensitive information or PII to a public domain, such as the cloud, is acceptable since it is a secure web-service (0 points)
__ Posting sensitive information or PII to a public domain, such as the cloud, is typically discouraged, even when the files are encrypted (5 points)
__ Posting sensitive information or PII to a public domain, such as the cloud, may be a major cybersecurity incident (5 points)
The above answers related to the question and scoring about KIH3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of information privacy (KIP)

Information privacy is defined as "the claim of individuals, groups, or institutions to determine when, and to what extent, information about them is communicated to others" (Lallmahamood, 2007, p. 7).

KIP1. (Possess knowledge regarding the consequences for violating information privacy laws)
Which of the following is true regarding information privacy laws?
A) You may be found personally liable in court for breaking information privacy laws (5 points)
B) Your company may be found liable in court for your conduct when breaking information privacy laws (5 points)
C) Both A and B (10 points)
D) None of the above (0 points)
The above answers related to the question and scoring about KIP1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of Internet use (KIU)
An acceptable Internet use policy defines "guidelines for employees indicating both acceptable and unacceptable Internet usages, with the intention of controlling employee [behaviors] and actions which contribute to the incidence and severity of the [organization's] Internet risks" (Lichtenstein & Swatman, 1997, p. 1).

KIU1. (Possess knowledge regarding when it is acceptable to use work Internet for personal use)
Which of the following is most true regarding personal Internet use at work? Check all that apply.
__ Browsing the Internet for personal use during a lunch break is acceptable if company policy allows it (5 points)
__ Browsing the Internet for personal use is always acceptable if you have an Internet connection (0 points)
__ Browsing the Internet for personal use is acceptable if your company does not monitor Internet usage (0 points)

__ Personal Internet use should be done on your personal device (5 points)
The above answers related to the question and scoring about KIU1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of sensitive information and personally identifiable information (PII) (KSI)

Sensitive information is defined as "protected information that the owner does not want to reveal to others and not to be divulged outside the [organization] as well as Information about an individual's racial or ethnic origin, criminal record, sexual preferences or practices and other information that include political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, or a trade union" (Ajigini, Van der Poll, & Kroeze, 2012, p. 7).

PII is defined as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (McCallister el al., 2010, p. 7)

KSI1. (Possess knowledge regarding the identification of sensitive information identification)
Which of the following are classified as sensitive information? Check all that apply.
__ Credit card numbers (2 points)
__ Job title (0 points)
__ Health records (2 points)
__ Marriage license (2 points)
__ Bank statements (2 points)
__ Tax records (2 points)

The above answers related to the question and scoring about KSI1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

KSI2. (Possess knowledge regarding the identification of PII)
Which of the following is classified as personally identifiable information? Check all that apply.
__ Bank records (2 points)
__ Social security number (2 points)
__ Mothers maiden name (2 points)
__ Medical records (2 points)
__ Fingerprints (2 points)

The above answers related to the question and scoring about KSI2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of social networking security (KSN)
Social networking is defined as "web-based services allowing individuals to: (a) construct a profile within a bounded system, (b) articulate a list of other users with whom

they share a connection, and (c) view and interact with their list of connections and those made by others within that system" (Weeden, Cooke, & McVey, 2013, p. 250).

KSN1. (Possess knowledge regarding the repercussions of posting sensitive information and PII on social networking sites)
Which of the following is true regarding accidentally or intentionally leaking sensitive information from work on one of you social media accounts.
A) You may lose your job (3 points)
B) Your employer may be harmed, by being found liable in court (3 points)
C) You can be convicted, depending on the nature of the offense (3 points)
D) All of the above (10 points)
The above answers related to the question and scoring about KSN1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Knowledge of applications strong passwords (KSP)
Passwords are considered strong when "having more than eight characters, at least one change of case, a number that is not at the end, and a non-alphanumeric character such as # or * that is also not at the end of the password" (Keller, Powell, Horstmann, Predmore, & Crawford, 2005, p. 13).

KSP1. (Possess knowledge regarding the properties of a strong password for applications)
What constitutes a strong password?
A) Using a password that is a combination of 8 lower case letters and upper case letters (2 points)
B) Using a password that is a combination of 10 lower case letters, upper case letters, and numbers (4 points)
C) Using passphrase that is a combination of 12 lower case letters, upper case letters, numbers, and special characters (10 points)
D) None of the above (0 points)
The above answers related to the question and scoring about KSP1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

Is there any other feedback you would like to submit regarding the knowledge units or knowledge topics?

____

____

Organizational Information System User Cybersecurity Skill Assessment

Skill is defined as a goal-directed, well-organized set of actions that is acquired through practice and performed with economy of effort, which enables a person to do something well (Boyatzis & Kolb, 1995).

Please evaluate the following cybersecurity skill measures and scoring of the measures answers for an organizational information system user (OISU) and rate their acceptability.

Skill in preventing unauthorized access to an IS by controlling access to systems (SAC)

SAC2. (Demonstrate the task of locking a computer while not in use)
A situation is presented where you are going to leave your desk for a minute, to get a bottle of water. Is there anything you need to do before you leave your desk? If you lock the computer, 10 points are awarded. If you log off from your computer, 10 points are awarded. If you shutdown the computer, 4 points are awarded. If you turn off the monitor, 2 points are awarded. If you leave without securing the computer, 0 points are awarded.
The above answers related to the question and scoring about SAC2 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable

(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

Skill in configuring and using email in a manner that prevents sensitive information and PII loss (SES)
Email security is the secure use of email that ensures the protection of sensitive information and PII, as well as preventing the propagation of malicious code (Carlton et al., 2015; DISA, 2015; Wang, Li, & Cheng, 2014).

SES3. (Demonstrate the task of not using work email for personal use)
A situation is presented where you receive an email from a coworker that says “if you forward this to 20 people you will become rich”. If you delete or ignore the email, 10 points are awarded. If you reply to the sender, asking kindly to keep you off such emails, 10 points are awarded. If you forward the email to your friends, and ask the sender not to send you emails like this in the future, 0 points are awarded. If you choose to forward the email to your friends, 0 points are awarded.

The above answers related to the question and scoring about SES3 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

SES5. (Demonstrate the task of virus-scanning Email attachments)

A situation is presented where you receive an email from a software vendor with an attachment. The attachment is a PDF file that contains updated instructions for their software that you have been waiting to receive. If you immediately scan the PDF attachment after downloading, 10 points are awarded. If you don't know what to do and ask your supervisor for assistance, 4 points are awarded. If you forward the email to IT to have the attachment virus scanned, 2 points are awarded. If you don't trust the source and delete the email, 0 points are awarded.

The above answers related to the question and scoring about SES5 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:
____
____

Provide feedback and alternative **scoring** of the answers (optional):
____
____

Skill in securely operating mobile computing devices (SMS)
Mobile computing is defined as "using portable computers capable of wireless networking" (Johansson & Andersson, 2015, p. 1).

SMS1. (Demonstrate the task of locking a mobile device when not in use)
A situation is presented where you are given a laptop to take to a training class in another city. You get to the training class and log in to your laptop. The trainer states that the first four hours of class are lecture, and there is no need for the laptop. If you lock the laptop while it's not being used, 10 points are awarded. If you shut down the laptop, 10 points are awarded. If you close your laptop, 4 points are awarded. If you leave the laptop open, and stay logged in, 0 points are awarded.

The above answers related to the question and scoring about SMS1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable

(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

SMS4. (Demonstrate the task of disabling wireless capabilities when the mobile device is not in use)
A situation is presented where you are given a laptop to take to a training class in Chicago. Class is breaking for lunch, and you are leaving your laptop in class. If you disable Wi-Fi while out for lunch, 10 points are awarded. If you shut down the laptop while out for lunch, 10 points are awarded. If you lock the computer, 2 points are awarded. If you leave the computer without disabling Wi-Fi or shutting down since the computer is in a secure environment, 0 points are awarded.

The above answers related to the question and scoring about SMS4 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____
____

Provide feedback and alternative **scoring** of the answers (optional):

____
____

Skill in using authorized systems for sensitive information and PII data processing as well as transmissions (SSI)

SSI1. (Demonstrate the task of not using an unauthorized system when dealing with sensitive information and PII)
A situation is presented where you have a CD with a document you need to update. The document contains company credit card numbers and is only allowed on specific computers in the office, per company policy. The building is closing soon and this work needs to be completed for a morning meeting. If you do not take the CD home to work on it, 10 points are awarded. If you email the document to your personal email account at home to work on it, 0 points are awarded. If you

take the CD home to work on it, 0 points are awarded. If you make a copy of the CD to take home to work on it, 0 points are awarded.

The above answers related to the question and scoring about SSI1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

____

____

Skill in using encryption to transmit sensitive information and PII when using Webmail (SWM)

SWM1. (Demonstrate the task to use encryption when sending sensitive information or PII with Webmail)
A situation is presented where your supervisor asks for a list of coworker social security numbers. An option is presented to send the social security numbers, unencrypted, thru Webmail. If you respond to your supervisor regarding your security concerns and do not include the social security numbers, 10 points are awarded. If you print the information and give it to your supervisor, 10 points are awarded. If you do not send the email and report this as a security incident, 0 points are awarded. If you send the unencrypted email, 0 points are awarded.

The above answers related to the question and scoring about SWM1 is: _______

(1) Totally unacceptable
(2) Unacceptable
(3) Slightly unacceptable
(4) Neutral
(5) Moderately acceptable
(6) Acceptable
(7) Perfectly acceptable

Provide feedback and alternative **method** if 4 or lower:

____

____

Provide feedback and alternative **scoring** of the answers (optional):

Is there any other feedback you would like to submit regarding the skill areas or skill tasks?

Feedback

Is there any other feedback you would like to submit regarding the content of this survey?

Appendix G

Phase 3 Email to Expert Panel

Dear Cybersecurity Expert,

We need your help in providing expert validation for an upcoming doctoral research study. I am a Ph.D. Candidate in Information Systems at the College of Engineering and Computing, Nova Southeastern University. My research is seeking to develop a prototype tool that will determine the cybersecurity competency of an organizational information system user. Such users include: IT personnel, secretaries, accountants, technical writers, physicians, etc. To develop the prototype tool, I need assistance from those that have knowledge in cybersecurity for four phases of data collection. This phase of research, Phase 3, requires assistance from experts to propose as well as validate weights for cybersecurity knowledge and skills.

The surveys you will receive will follow the Delphi method. This may require one or two additional rounds of the survey to be completed to form a consensus. Once a consensus is achieved, the study will proceed to the next phase. All participants are subject matter experts in this area.

By participating in this study you agree and understand that your responses are voluntary. Measures will be taken to ensure that responses are anonymous and cannot be traced to any individual. You may stop participating in this study at any time. In the event that you no longer participate in this study, your responses will not be recorded. By participating in this study you certify that you are over the age of 18 years old. If you are willing to participate, please click on the following link for access: www.nova.edu/~rn380

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study.

If you wish to receive the findings of the study, please send contact me via email and I will provide you with information about the academic research publication(s) resulting from this study.

Regards,
Richard Nilsen, PhD Candidate
E-mail: rn380@nova.edu

Appendix H

Phase 3 Survey

Dear Cybersecurity Expert,

This survey will be completed using the Delphi method. All participants are subject matter experts in this area. This survey intends propose and validate weights for the knowledge, skills, and abilities for organizational information system users that were defined in the previous phases of this study.

Please respond to all questions as honestly and accurately as possible. By completing this survey you agree and understand that your responses are voluntary. Measures will be taken to ensure than responses are anonymous and cannot be traced to any individual. You may exit this survey at any time. In the event that you chose to exit this survey, your responses will not be recorded. By participating in this survey you certify that you are over the age of 18 years old.

Demographics

What is your age?

(A) Under 20
(B) 20-29
(C) 30-39
(D) 40-49
(E) 50-59
(F) Over 60

What is your gender?

(A) Female
(B) Male

What is your job function?

(A) Administrative staff
(B) Cybersecurity/IT staff
(C) Engineer
(D) Manager
(E) Operations
(F) Professional staff
(G) Scientist
(H) Security operator
(I) Teacher/Professor
(J) Technical staff

(K) Other

How long have you been with your current organization?

(A) Under 1 year
(B) 1 – 5 years
(C) 6 – 10 years
(D) 11 – 15 years
(E) 16 – 20 years
(F) 21 – 25 years
(G) 26 – 30 years
(H) Over 30 years

Which describes your current employer?

(A) Academia
(B) Federal government employee
(C) Private sector company
(D) State government employee
(E) Other

What is your highest level of education?

(A) High school diploma
(B) 2-year college (Associates degree)
(C) 4-year college (Bachelors degree)
(D) Graduate degree
(E) Doctorate
(F) Other

Which cybersecurity certifications do you possess?

____

____

To weight importance, please allocate 100 points among the Knowledge Categories.

Knowledge Categories

Item	**Knowledge Category**	
ASKC	Application Security Knowledge Category http://www.nova.edu/~rn380/ASKC.htm	_______points
ISKC	Information Security Knowledge Category http://www.nova.edu/~rn380/ISKC.htm	_______points
INSKC	Internet and Network Security Knowledge Category http://www.nova.edu/~rn380/INSKC.htm	_______points
PSKC	Physical Security Knowledge Category http://www.nova.edu/~rn380/PSKC.htm	_______points

Is there any other feedback you would like to submit regarding the Knowledge Category weights?

____

____

To weight importance, please allocate 100 points among the Skill Categories.

Skill Unit Groups

Item	**Skill Category**	
ASSC	Application Security Skill Category http://www.nova.edu/~rn380/ASSC.htm	_______points
ISSC	Information Security Skill Category http://www.nova.edu/~rn380/ISSC.htm	_______points
INSSC	Internet and Network Skill Security Category http://www.nova.edu/~rn380/INSSC.htm	_______points
PSSC	Physical Security Skill Category http://www.nova.edu/~rn380/PSSC.htm	_______points

To weight importance, please allocate 100 points between Knowledge Units and Skill Units.

Total Units

Item	**Category**	
All KUs	Overall Knowledge http://www.nova.edu/~rn380/OK.htm	_______points
All SUs	Overall Skills http://www.nova.edu/~rn380/OS.htm	_______points

Is there any other feedback you would like to submit regarding the Overall weights?

____

____

Is there any other feedback you would like to submit regarding the content of this survey?

____

____

Appendix I

Phase 4 Email to Expert Panel

Dear Cybersecurity Expert,

We need your help in providing expert validation for an upcoming doctoral research study. I am a Ph.D. Candidate in Information Systems at the College of Engineering and Computing, Nova Southeastern University. My research is seeking to develop a prototype tool that will determine the cybersecurity competency of an organizational information system user. Such users include: IT personnel, secretaries, accountants, technical writers, physicians, etc. To develop the prototype tool, I need assistance from those that have knowledge in cybersecurity for four phases of data collection. This phase of research, Phase 4, requires assistance from experts to validate a cybersecurity competency threshold (overall score) using the results from the first three phases, which an organizational information system user would need to achieve in order to be granted Internet and network privileges.

The surveys you will receive will follow the Delphi method. This may require one or two additional rounds of the survey to be completed to form a consensus. Once a consensus is achieved, the study will proceed to the next phase. All participants are subject matter experts in this area.

By participating in this study you agree and understand that your responses are voluntary. Measures will be taken to ensure that responses are anonymous and cannot be traced to any individual. You may stop participating in this study at any time. In the event that you no longer participate in this study, your responses will not be recorded. By participating in this study you certify that you are over the age of 18 years old. If you are willing to participate, please click on the following link for access: www.nova.edu/~rn380

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study.

If you wish to receive the findings of the study, please send contact me via email and I will provide you with information about the academic research publication(s) resulting from this study.

Regards,
Richard Nilsen, PhD Candidate
E-mail: rn380@nova.edu

Appendix J

Phase 4 Survey

Dear Cybersecurity Expert,

This survey will be completed using the Delphi method. All participants are subject matter experts in this area. The goal of this phase of research is to propose and validate the cybersecurity competency threshold that an organizational information system user must meet or exceed to be granted access to organizational information systems. Such users include: IT personnel, secretaries, accountants, technical writers, physicians, etc. All SME inputs will be averaged to produce a single score.

By completing this survey you agree and understand that your responses are voluntary. Measures will be taken to ensure than responses are anonymous and cannot be traced to any individual. You may exit this survey at any time. In the event that you chose to exit this survey, your responses will not be recorded. By participating in this survey you certify that you are over the age of 18 years old.

Demographics

What is your age?

(A) Under 20
(B) 20-29
(C) 30-39
(D) 40-49
(E) 50-59
(F) Over 60

What is your gender?

(A) Female
(B) Male

What is your job function?

(A) Administrative staff
(B) Cybersecurity/IT staff
(C) Engineer
(D) Manager
(E) Operations
(F) Professional staff
(C) Scientist
(D) Security operator
(E) Teacher/Professor

(F) Technical staff
(G) Other

How long have you been with your current organization?

(A) Under 1 year
(B) 1 – 5 years
(C) 6 – 10 years
(D) 11 – 15 years
(E) 16 – 20 years
(F) 21 – 25 years
(G) 26 – 30 years
(H) Over 30 years

Which describes your current employer?

(A) Academia
(B) Federal government employee
(C) Private sector company
(D) State government employee
(E) Other

What is your highest level of education?

(A) High school diploma
(B) 2-year college (Associates degree)
(C) 4-year college (Bachelors degree)
(D) Graduate degree
(E) Doctorate
(F) Other

Which cybersecurity certifications do you possess?

____

The following knowledge and skill categories are weighted as:
Application Security Knowledge Category 21.6875%
http://www.nova.edu/~rn380/ASKC.htm
Information Security Knowledge Category 28.0625%
http://www.nova.edu/~rn380/ISKC.htm
Internet and Network Security Knowledge Category 27.4375%
http://www.nova.edu/~rn380/INSKC.htm
Physical Security Knowledge Category 22.8125%
http://www.nova.edu/~rn380/PSKC.htm

The following skill categories are weighted as:

Application Security Skill Category	22.25%
http://www.nova.edu/~rn380/ASSC.htm	
Information Security Skill Category	27.125%
http://www.nova.edu/~rn380/ISSC.htm	
Internet and Network Skill Knowledge Category	28.0625%
http://www.nova.edu/~rn380/INSSC.htm	
Physical Security Skill Category	22.5625%
http://www.nova.edu/~rn380/PSSC.htm	

The following is a summary of the overall knowledge and overall skill weights:

Overall Knowledge	47.3125%
http://www.nova.edu/~rn380/OK.htm	
Overall Skills	52.6875%
http://www.nova.edu/~rn380/OS.htm	

The content of this research has been used to develop the MyCyberKSAs^{TM} prototype tool for assessing the cybersecurity competency of organizational information system users. If needed, MyCyberKSAs^{TM} can be found at: www.nova.edu/~rn380

What percentage of points does an organizational information system user need to achieve to be considered as having cybersecurity competency: _____%

Is there any other feedback you would like to submit regarding the cybersecurity competency proposal?

____

____

Is there any other feedback you would like to submit regarding the content of this survey?

____

____

Appendix K

Phase 5 Solicitation to Prototype Tool Test Participants

Dear Participant,

We need your help testing for a Website developed from doctoral research study. I am a Ph.D. Candidate in Information Systems at the College of Engineering and Computing, Nova Southeastern University. The main goal of this research is to develop a prototype tool that will determine the cybersecurity competency of an organizational information system user.

By participating in this study you agree and understand that your responses are voluntary. Measures will be taken to ensure that responses are anonymous and cannot be traced to any individual. You may stop participating in this study at any time. In the event that you no longer participate in this study, your responses will not be recorded. By participating in this study you certify that you are over the age of 18 years old. If you are willing to participate, please click on the following link: www.nova.edu/~rn380

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study.

Regards,
Richard Nilsen, PhD Candidate
E-mail: rn380@nova.edu

Appendix L

Phase 5 Survey

Dear Participants,

This survey intends to measure your perceptions of the MyCyberKSAs^{TM} Website. The MyCyberKSAs^{TM} Website is an assessment tool to measure the cybersecurity competency of organizational information system users.

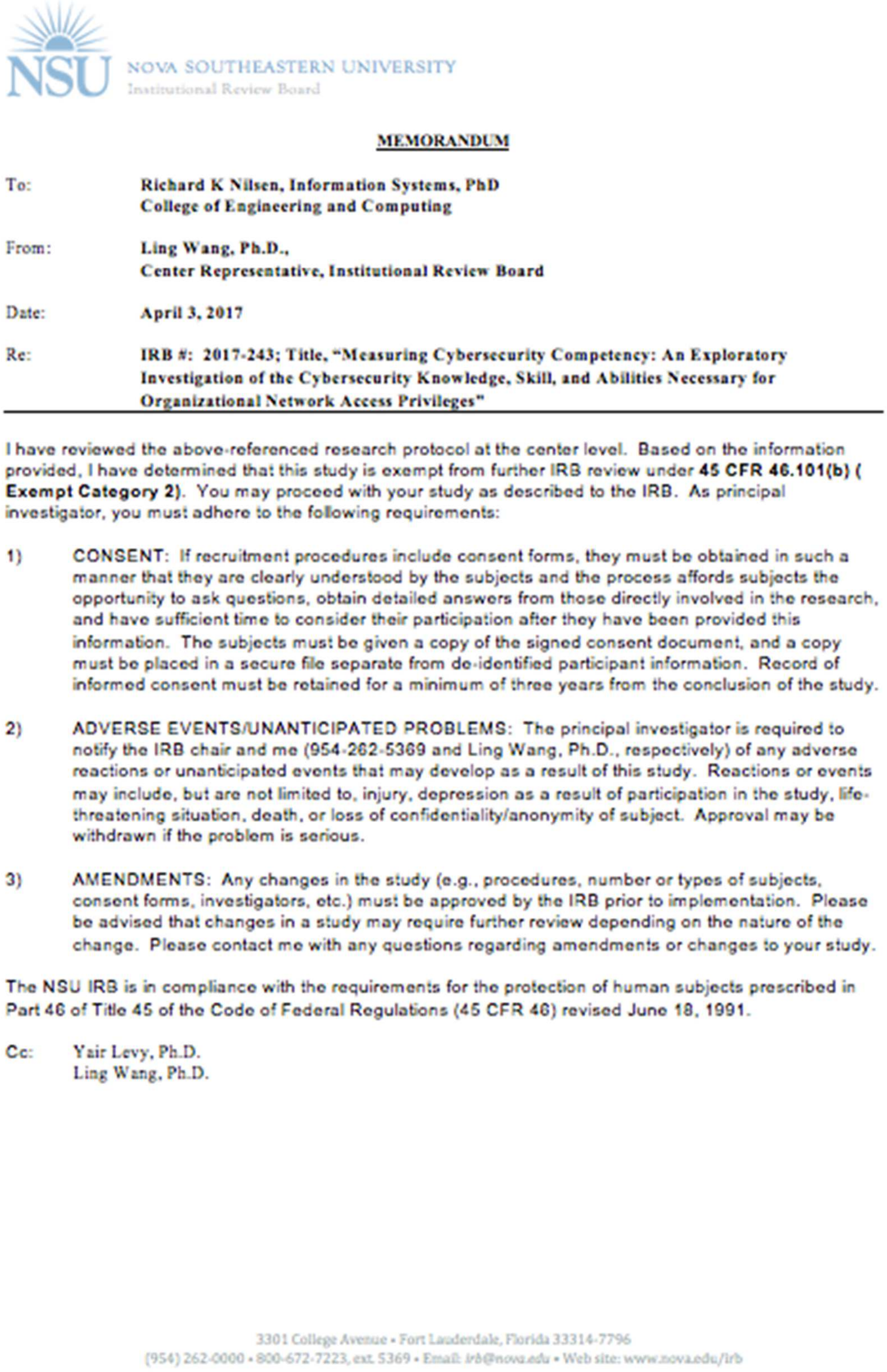
By completing this survey you agree and understand that your participation is voluntary. Please respond to all questions as honestly and accurately as possible. Measures will be taken to ensure than responses to this survey are anonymous and cannot be traced to any individual. Additionally, your activity on using the MyCyberKSAs^{TM} tool will be anonymous as well. You may exit this survey at any time. In the event that you chose to exit this survey, your responses will not be recorded. By participating in this survey you certify that you are over the age of 18 years old.

The data collected from this survey will be published as part of a doctoral dissertation.

If you are willing to participate, please click on the following link for access:
http://www.nova.edu/~rn380

Appendix M

Institutional Review Board Approval Letter



NSU NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To:	**Richard K Nilsen, Information Systems, PhD** **College of Engineering and Computing**
From:	**Ling Wang, Ph.D.,** **Center Representative, Institutional Review Board**
Date:	**April 3, 2017**
Re:	**IRB #: 2017-243; Title, "Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skill, and Abilities Necessary for Organizational Network Access Privileges"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt Category 2)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-0000 • 800-672-7223, ext. 5369 • Email: irb@nova.edu • Web site: www.nova.edu/irb

References

Ab Rahman, N. & Choo, K. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45-69.

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, *4*(1), 290-301.

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183-196.

Ahmad, M. S., & Bamnote, G. R. (2013). Data leakage detection and data prevention using algorithm. *International Journal Of Computer Science And Applications*, *6*(2), 394-399.

Ahmed, A., Ishman, S. L., Laeeq, K., & Bhatti, N. I. (2013). Assessment of improvement of trainee surgical skills in the operating room for tonsillectomy. *The Laryngoscope*, *123*(7), 1639-1644.

Ahn, J., Lee, S. W., & Kim, H. (2016). NFC based privacy preserving user authentication scheme in mobile office. *International Journal of Computer and Communication Engineering*, *5*(1), 61.

Ajigini, O. A., Van der Poll, J. A., & Kroeze, J. H. (2012). Towards a management framework to protect sensitive information during migrations. *Proceedings of the 2nd International Conference on Design and Modeling in Science, Education and Technology,* Orlando, FL, pp. 6-13.

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly, 25*(1), 107-136.

Ardiley, S. (2012). History of the common access card (CAC). *Security Info Watch*. Retrieved Feb 13, 2016, from: http://www.securityinfowatch.com/article/10653434/history-ofthe-common-access-card-cac

Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 1-- Attackers. *IEEE Security & Privacy*, *13*(1), 71-76.

Arnold, H., Erner, M., Möckel, P., & Schläffer, C. (2010). Integration of academic research into innovation projects: the case of collaboration with a university research institute. *Applied Technology and Innovation Management*. Springer Berlin Heidelberg, pp. 25-35.

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services, *Computers in Human Behavior*, *45*(1), 93-98.

Aryee, S., Walumbwa, F. O., Seidu, E. Y., & Otaye, L. E. (2016). Developing and leveraging human capital resource to promote service quality testing a theory of performance. *Journal of Management*, *42*(2), 480-499.

Assante, M., & Tobey, D. (2011). Enhancing the cybersecurity workforce. *IT Professional*, *13*(1), 12-15.

Association of Computing Machinery Joint Task Force on Cybersecurity Education [ACMJTF] (2016). *ACM Joint Task Force on Cybersecurity Education*. Retrieved Oct 11, 2016, from: http://www.csec2017.org

Avison, D. E., & Wood-Harper, A. T. (1986). Multiview—an exploration in information systems development. *Australian Computer Journal*, *18*(4), 174-179.

Baker, M. (2013). *State of cyber workforce development.* Software Engineering Institute, Carnegie Mellon University. Retrieved June 23, 2015, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.395.9178&rep=rep1&type=pdf

Bang, S. K., Chung, S., Choh, Y., & Dupuis, M. (2013). A grounded theory analysis of modern web applications: knowledge, skills, and abilities for DevOps. *Proceedings of the 2nd annual conference on Research in information technology,* Orlando, FL, pp. 61-62.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*, 145-159.

Barnowski, L., & Anderson, L. (2005). Examining rating source variation in work behavior to KSA linkages. *Personnel Psychology, 58*(1), 1041-1054.

Barnum, S., & McGraw, G. (2005). Knowledge for software security. *IEEE Security & Privacy*, *3*(2), 74-78.

Behrens, S., Alberts, C., & Ruefle, R. (2012). *Competency lifecycle roadmap: toward performance readiness.* Software Engineering Institute, Carnegie Mellon University. Retrieved May 29, 2015, from http://www.sei.cmu.edu/library/abstracts/reports/12tn020.cfm

Bernard, R. (2007). Information lifecycle security risk assessment: A tool for closing security gaps. *Computers & Security*, *26*(1), 26-30.

Bishop, M. (2003). What is computer security? *IEEE Security & Privacy*, *1*(1), 67-69.

Bonner, A., & Stewart, G. (2001). Development of competency based standards: An application of the Delphi research technique. *Nurse Researcher*, *9*(1), 63-73.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security*, *28*(3), 130-137.

Bowen, B., Devarajan, R., & Stolfo, S. (2012). Measuring the human factor of cyber security. *Homeland Security Affairs, 5*(2), 1-7.

Boyatzis, R. E., & Kolb, D. A. (1995). From learning styles to learning skills: the executive skills profile. *Journal of Managerial Psychology*, *10*(5), 3-17.

Bratianu, C. (2016). Knowledge dynamics. *Management Dynamics in the Knowledge Economy*, *4*(3), 323.

Broucek, V., & Turner, P. (2014). Considerations for e-forensics: insights into implications of uncoordinated technical, organisational and legal responses to illegal or inappropriate on-line behaviours. *International Journal of Computing*, *4*(2), 17-25.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM*, *57*(2), 24-27.

Calder, B., Phillips, L., & Tybout, A. (1982). The concept of external validity. *Journal of Consumer Research*, *9*(3), 240-244.

Camerer, C., & Hogarth, R. (1999). The effects of financial incentives in experiments: A review and capital-labor-production framework. *Journal of Risk and Uncertainty, 19*(1-3), 7-42.

Campbell, S. G., O'Rourke, P., & Bunting, M. F. (2015). Identifying dimensions of cyber aptitude: The design of the cyber aptitude and talent assessment. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Los Angeles, California, pp. 721-725.

Cankaya, Y. (2015). Technical note: exploiting problem definition study for cyber security simulations. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, *12*(4), 363-368.

Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills of non-IT professionals. *Proceedings of the 2015 IEEE SoutheastCon,* Ft. Lauderdale, Florida, pp. 1-6.

Carlton, M., Levy, Y**.**, Ramim, M. M., & Terrell, S. R. (2015). Development of the MyCyberSkills™ iPad app: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills. *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC - Workshop on Information Security and Privacy (WISP) 2015*, Ft. Worth, Texas.

Chen, T., Shore, D., Zaccaro, S., Dalal, R, Tetrick, L., & Gorab, A. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy, 12*(5), 61-67.

Choi, M., Levy, Y., & Hovav, A. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC - Workshop on Information Security and Privacy (WISP) 2013*, Milan, Italy, pp. 1-16.

Choi, M., & Song, J. (2016). A theoretical review of neutralization in security policy. *Indian Journal of Science and Technology*, *9*(46), 1-4.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1-147.

Colman, A. (2015). Near vision. A Dictionary of Psychology. Retrieved 24 Jul. 2016, from: http://www.oxfordreference.com/view/10.1093/acref/9780199657681.001.0001/acref-9780199657681-e-5379

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering cybersecurity education in the US: An analysis of the critical factors. *Proceedings of the of the 2014 47th Hawaii International Conference on System Sciences,* Waikoloa, HI, pp. 2006-2014.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849-1858.

Creswell, J. (2002). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Upper Saddle River, NJ: Merrill Prentice Hall.

Czabanowska, K., Klemenc-Ketis, Z., Potter, A., Rochfort, A., Tomasik, T., Csiszar, J., & Van den Bussche, P. (2012). Development of a competency framework for quality improvement in family medicine: a qualitative study. *Journal of Continuing Education in the Health Professions*, *32*(3), 174-180.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.

Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science*, *9*(3), 458-467.

Defense Information Systems Agency [DISA] (2015). *Cyber Awareness Challenge version 2.0*. Retrieved July 28, 2015, from: http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm

Deshpande, P. M., Joshi, S., Dewan, P., Murthy, K., Mohania, M., & Agrawal, S. (2015). The Mask of ZoRRo: preventing information leakage from documents. *Knowledge and Information Systems*, *45*(3), 705-730.

Dhepe, Y., & Akarte, S. (2013). Security issues facing computer users: An overview. *International Journal of Computer Science and Applications*, *6*(2), 263-267.

Dienes, Z., & Perner, J. (1999). A theory of implicit and explicit knowledge. *Behavioral and Brain Sciences, 22*(5)*,* 735-808.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3), 189-198.

Doneda, D., & Almeida, V. (2015). Privacy governance in cyberspace. *IEEE Internet Computing*, *19*(3), 50-53.

Draganidis, F., & Mentzas, G. (2006). Competency based management: a review of systems and approaches. *Information Management & Computer Security*, *14*(1), 51-64.

Dye, S. M., & Scarfone, K. (2014). A standard for developing secure mobile applications. *Computer Standards & Interfaces*, *36*(3), 524-530.

Duffield, C. (1993). The Delphi technique: a comparison of results obtained using two expert panels. *International Journal of Nursing Studies*, *30*(3), 227-237.

Evans, K., & Reeder, F. (2010). *A human capital crisis in cybersecurity: Technical proficiency matters*. Center for Strategic and International Studies. Retrieved July 27, 2015, from: http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf

Fetters, M. D., Motohara, S., Ivey, L., Narumoto, K., Sano, K., Terada, M., Tsuda, T., & Inoue, M. (2017). Utility of self-competency ratings during residency training in family medicine education-emerging countries: findings from Japan. *Asia Pacific Family Medicine*, *16*(1), 1.

Foster, I. D., Larson, J., Masich, M., Snoeren, A. C., Savage, S., & Levchenko, K. (2015, October). Security by any other name: On the effectiveness of provider based email security. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 450-464.

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security*, *27*(7), 235-240.

Garavan, T. N., & McGuire, D. (2001). Competencies and workplace learning: some reflections on the rhetoric and the reality. *Journal of Workplace Learning*, *13*(4), 144-164.

Garfinkel, S. (2012). The cybersecurity risk. *Communications of the ACM*, *55*(6), 29-32.

Gaurav, R., Kumar, S., Venkatesan, S., & Babu, D. R. (2015). An enhanced approach in cloud computing to reduce security risks and minimize data loss in railways. *International Journal of Electrical Sciences Electrical Sciences & Engineering (IJESE), (1)*1, 12-18.

Garvey, P. R., Moynihan, R. A., & Servi, L. (2013). A macro method for measuring economic‐benefit returns on cybersecurity investments: The table top approach. *Systems Engineering*, *16*(3), 313-328.

Gebbie, K., & Merrill, J. (2002). Public health worker competencies for emergency response. *Journal of Public Health Management and Practice*, *8*(3), 73-81.

Grisham, T. (2009). The Delphi technique: A method for testing complex and multifaceted topics. *International Journal of Managing Projects in Business*, *2*(1), 112-130.

Gross, J. B., & Rosson, M. B. (2007). Looking for trouble: Understanding end-user security management. *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology,* Cambridge, MA, pp. 1-10.

Grus, C. L., Falender, C., Fouad, N. A., & Lavelle, A. K. (2016). A culture of competence: A survey of implementation of competency-based education and assessment. *Training and Education in Professional Psychology*, *10*(4), 198-205.

Hagen, J., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security*, *17*(5), 388-407.

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security, 66*(1), 52-65.

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat–Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior*, *61*, 372-377.

Hassanzadeh, A., Modi, S., & Mulchandani, S. (2015). Towards effective security control assignment in the Industrial Internet of Things. *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Reston, VA*, pp. 795-800.

Hasson, F., & Keeney, S. (2011). Enhancing rigour in the Delphi technique research. *Technological Forecasting and Social Change*, *78*(9), 1695-1704.

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, *32*(4), 1008-1015.

Hayton, J. C. (2005). Competing in the new economy: the effect of intellectual capital on corporate entrepreneurship in high‐technology new ventures. *R&D Management*, *35*(2), 137-155.

Haywood, S. H., Goode, T., Gao, Y., Smith, K., Bronheim, S., Flocke, S. A., & Zyzanski, S. (2014). Psychometric evaluation of a cultural competency assessment instrument for health professionals. *Medical Care*, *52*(2), 7-15.

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security, 4*(4), 3-20.

Hester, E. D., & Joseph, W. B. (1998). Industry corner: smart cards for an information-hungry world. *Business Economics*, *33*(1), 54-58.

Hill, K., & Fowles, J. (1975). The methodological worth of the Delphi forecasting technique. *Technological Forecasting and Social Change*, 7, 179-192.

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, *26*(4), 383-402.

Hird, J., Hawley, M., & Machin, C. (2016). Air Traffic Management Security Research in SESAR. *International Conference on Availability, Reliability and Security (ARES), 2016 11th,* Salzburg, Austria*,* pp. 486-492.

Hoffman, R. R., & Branlat, M. (2016). To know or not to know, what is the need?. *IEEE Intelligent Systems*, *31*(1), 78-82.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

Honts, C., Prewett, M., Rahael, J., & Grossenbacher, M. (2012). The importance of team processes for different team types. *Team Performance Management: An International Journal*, *18*(5/6), 312-327.

Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards automating social engineering using social networking sites. *Proceedings from CSE'09: International Conference on Computational Science and Engineering 2009, Miami, FL,* pp. 117-124.

Ioannou, A., & Hannafin, R. D. (2008). Course management systems: Time for users to get what they need. *TechTrends*, *52*(1), 46.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Imgraben, J., Engelbrecht, A., & Choo, K. K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347-1360.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), 75-78.

Jacob, S. M., & Chalia, D. S. (2015). Research highlights: July-September 2015. *Indian Journal of Research in Homoeopathy*, *9*(3), 202.

Jackson, D., Firtko, A., & Edenborough, M. (2007). Personal resilience as a strategy for surviving and thriving in the face of workplace adversity: a literature review. *Journal of Advanced Nursing*, *60*(1), 1-9.

Jakobsson, M., & Myers, S. (2007). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Hoboken, NJ: Wiley-Interscience.

Jansen, K. J., & Kristof-Brown, A. (2006). Toward a multidimensional theory of person-environment fit. *Journal of Managerial issues, 18*(2), 193-212.

Jiang, B., & Ormeling, F. (2000). Mapping cyberspace: Visualizing, analysing and exploring virtual worlds. *The Cartographic Journal*, *37*(2), 117-122.

Johansson, D., & Andersson, K. (2015). Mobile e-Services: State of the art, focus areas, and future directions. *International Journal of E-Services and Mobile Applications*, *7*(2), 1-24.

Johnson, C. (2012). CyberSafety: on the interactions between cybersecurity and the software engineering of safety-critical systems. *Achieving System Safety,* 85-96.

Jou, M., Lin, Y. T., & Wu, D. W. (2016). Effect of a blended learning environment on student critical thinking and knowledge transformation. *Interactive Learning Environments*, *24*(6), 1131-1147.

Jung, C., Han, I., & Suh, B. (1999). Risk analysis for electronic commerce using case-based reasoning. *International Journal of Intelligent Systems in Accounting, Finance & Management*, *8*(1), 61-73.

Kalloniatis, C., Mouratidis, H., & Islam, S. (2013). Evaluating cloud deployment scenarios based on security and privacy requirements. *Requirements Engineering*, *18*(4), 299-319.

Kaplanski, P. (2010). Description logic based generator of data centric applications. *2010 2nd International Conference on Information Technology (ICIT),* Gdansk, Poland, pp. 53-56.

Kay, C., & Moncarz, E. (2004). Knowledge, skills, and abilities for lodging management. *Cornell Hotel and Restaurant Administration Quarterly*, *45*(3), 285-298.

Kay, D., Pudas, T., & Young, B. (2012). Preparing the pipeline: The U.S. cyber workforce for the future. *Defense Horizons, 72*(1), 1-16.

Karantjias, A., & Polemi, N. (2010). Assessment of advanced cryptographic antiviral techniques. *International Journal of Electronic Security and Digital Forensics*, *3*(1), 60-72.

Kegan, R. (1995). *In over our heads: The mental demands of modern life*. Harvard University Press.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management*, *22*(2), 7-19.

Keenan, J. M., Betjemann, R. S., & Olson, R. K. (2008). Reading comprehension tests vary in the skills they assess: Differential dependence on decoding and oral comprehension. *Scientific Studies of Reading*, *12*(3), 281-300.

Keeney, R. L. (1999). The value of Internet commerce to the customer. *Management Science*, *45*(4), 533-542.

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice*, *13*(5), 66.

Korndorffer, J. R., Scott, D. J., Sierra, R., Brunner, W. C., Dunne, J. B., Slakey, D. P., & Hewitt, R. L. (2005). Developing and testing competency levels for laparoscopic skills training. *Archives of Surgery*, *140*(1), 80-84.

Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social engineering threats and awareness: a survey. *European Journal of Advances in Engineering and Technology*, *2*(11), 15-19.

Lallmahamood, M. (2007). An examination of individual's perceived security and privacy of the Internet in Malaysia and the influence of this on their intention to use e-commerce: Using an extension of the technology acceptance model. *Journal of Internet Banking and Commerce*, *12*(3), 1-26.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58-74.

Lemoudden, M., Bouazza, N., Ouahidi, B. E., & Bourget, D. (2013). A survey of cloud computing security overview of attack vectors and defense mechanisms. *Journal of Theoretical and Applied Information Technology*, *54*(2), 325-330.

Lesemann, D. J. (2016). Once More Unto the Breach: An Analysis of Legal, Technological, and Policy Issues Involving Data Breach Notification Statutes. *Akron Intellectual Property Journal*, *4*(2), 203-237.

Lesk, M. (2011). Cybersecurity and economics. *IEEE Security & Privacy*, *9*(6), 76-79.

Levy, Y. (2006). *Accessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.

Levy, Y., & Ramim, M. M. (2015). The effect of competence-based simulations on management skills enhancements in e-learning courses. *Proceeding of the Chais 2015 Conference on Innovative and Learning Technologies Research,* The Open University of Israel, Raanana, Israel, *pp. 34-41*.

Levy, Y., & Ramim, M. M. (2016). Towards an evaluation of cyber risks and identity information sharing practices in e-learning, social networking, and mobile texting apps. *Proceeding of the Chais 2016 Conference on Innovative and Learning Technologies Research,* The Open University of Israel, Raanana, Israel, *pp. 60E-69E*.

Lewin, K. (1943). Defining the 'field at a given time'. *Psychological Review*, *50*(3), 292-310.

Lichtenstein, S. & Swatman, P. (1997). Internet acceptable usage policy: Arguments and perils. in *Proceedings of 1st Pacific Asia Workshop on Electronic Commerce (PAWEC)*, Brisbane, Australia. pp. 1 – 19.

Lindner, J. R., Murphy, T. H., & Briers, G. E. (2001). Handling nonresponse in social science research. *Journal of Agricultural Education*, *42*(4), 43-53.

Linstone, H., & Turoff, M. (1975). *The Delphi method: Techniques and applications*. Reading, MA: Addison-Wesley.

Lopez, J., Oppliger, R., & Pernul, G. (2004). Authentication and authorization infrastructures (AAIs): a comparative survey. *Computers & Security*, *23*(7), 578-590.

Lorentzen, C., Fiedler, M., & Johnson, H. (2013). On user perception of safety in online social networks. *International Journal of Communication Networks and Distributed Systems*, *11*(1), 77-91.

Lowry, M. R. (1992). Software engineering in the twenty-first century. *AI magazine*, *13*(3), 71-87.

Lu, B., Guo, X., Luo, N., & Chen, G. (2015). Corporate blogging and job performance: Effects of work-related and wonwork-related participation. *Journal of Management Information Systems*, *32*(4), 285-314.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38.

Marcolin, B. L., Compeau, D. R., Munro, M. C., & Huff, S. L. (2000). Assessing user competence: Conceptualization and measurement. *Information Systems Research, 11*(1), 37-60.

Manley, R., & Zinser, R. (2012). A Delphi study to update CTE teacher competencies. *Education & Training*, *54*(6), 488-503.

Marchetti, M., Pierazzi, F., Colajanni, M., & Guido, A. (2016). Analysis of high volumes of network traffic for Advanced Persistent Threat detection. *Computer Networks*, *109*, 127-141.

Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering, 17*(3), 17-24.

McCallister, E., Grance, T., Scarfone, K. (2010). Guide to protecting the confidentiality of personally identifiable information (PII). *NIST Special Publication*, *800*(122), 1-59.

Medlin, B. D., & Cazier, J. A. (2011). A Study of Hard Drive Forensics on Consumers' PCs: Data Recovery and Exploitation. *Journal of Management Policy and Practice*, *12*(1), 27.

Mejias, R. J., & Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security*, *10*(4), 160-185.

Microsoft (2016a). *Email encryption in Microsoft Office 365.* Retrieved Feb 5, 2016, from: https://technet.microsoft.com/en-us/library/dn948533.aspx

Microsoft (2016b). *File and folder permissions.* Retrieved Feb 5, 2016, from: https://msdn.microsoft.com/en-us/library/bb727008.aspx

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity challenges and compliance issues within the US healthcare sector. *International Journal of Business and Social Research*, *5*(2), 55-66.

Mujeye, S., & Levy, Y. (2013). Complex passwords: How far is too far? The role of cognitive load on employee productivity. *Online Journal of Applied Knowledge Management*, *1*(1), 122-132.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. *Proceeding from the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER),* Bangkok, Thailand, pp. 256-262.

Nagarjuna, B. V. R. R., & Sujatha, V. (2013). An innovative approach for detecting targeted malicious e-mail. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *2*, 422-428.

National Institute of Standards and Technology [NIST], (2012). *National initiative for cybersecurity education (NICE) strategic plan: Building a digital nation*. Retrieved June 7, 2015, from: http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

National Institute of Standards and Technology [NIST], (2014). *Framework for improving critical infrastructure cybersecurity*. Retrieved June 7, 2015, from: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Security Council [NSC]. (2015), The comprehensive national cybersecurity initiative, *The White House: Foreign Policy,* 2015. Retrieved June 9, 2015, from: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

Nguyen, D. Q. (1998). The essential skills and attributes of an engineer: A comparative study of academics, industry personnel and engineering students. *Global Journal of Engineering Education*, *2*(1), 65-75.

Newsome, B., & Jarmon, J. (2016). *A practical introduction to homeland security and emergency management: From home to abroad*. Thousand Oaks, CA: Sage.

Nonaka, I. (1991). The knowledge-creating company. *Harvard Business Review*, *69*(6), 96-104.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, *5*(1), 14-37.

Nonaka, I., & Konno, N. (1998). The concept of "Ba": Building a foundation for knowledge creation. *California Management Review, 40*(3), 40-54.

North Ireland Business Information [NIBusinessInfo]. (2016). *Sample IT policies, disclaimers and notices*. Retrieved Feb 5, 2016: https://www.nibusinessinfo.co.uk/content/sample-acceptable-email-use-policy

O'Neil, L. R., Assante, M. J., & Tobey, D. H. (2012). *SmartGrid cybersecurity: Job performance model report.* National Technical Information Service, Alexandria, VA.

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.

Oxford Dictionary Online [Oxford], 2016. Policy. Retrieved Feb 9, 2016 from: http://www.oxforddictionaries.com/us/definition/american_english/policy

Park, J. S., & Sandhu, R. (2000). Secure cookies on the Web. *IEEE Internet Computing*, *4*(4), 36.

Parkinson, S., Somaraki, V., & Ward, R. (2016). Auditing file system permissions using association rule mining. *Expert Systems with Applications*, *55*, 274-283.

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.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy, 10*(3), 76-79.

Penciner, R., Langhan, T., Lee, R., Mcewen, J., Woods, R. A., & Bandiera, G. (2011). Using a Delphi process to establish consensus on emergency medicine clerkship competencies. *Medical Teacher*, *33*(6), e333-e339.

Phelan, K. V., & Mills, J. E. (2010). An exploratory study of knowledge, skills, and abilities (KSAs) needed in undergraduate hospitality curriculums in the convention industry. *Journal of Human Resources in Hospitality & Tourism*, *10*(1), 96-116.

Pittenger, M. (2016). Addressing the security challenges of using containers. *Network Security*, *2016*(12), 5-8.

Plotkin, S. A. (2008). Correlates of vaccine-induced immunity. *Clinical Infectious Diseases*, *47*(3), 401-409.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638-646.

Poteet, J. A. (1980). Informal assessment of written expression. *Learning Disability Quarterly*, *3*(4), 88–98.

Powell, C. (2003). The Delphi technique: myths and realities. *Journal of Advanced Nursing*, *41*(4), 376-382.

Prager, I. G., Moran, G., & Sanchez, J. (1997). Job analysis of felony assistant public defenders: The most important tasks and most useful knowledge, skills, and abilities. *Psychology, Crime and Law*, *3*(1), 37-49.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly, 34*(4), 757-778.

Ramim, M., & Lichvar, B. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, *2*(1), 122-136.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826.

Sabeil, E., Manaf, A., Ismail, Z., & Abas, M. (2011). Cyber forensics competency-based framework – A review. *International Journal of New Computer Architectures and their Applications*, *1*(4), 991-1000.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, *9*(2), 107-118.

Saxena, N., Choi, B. J., & Lu, R. (2016). Authentication and authorization scheme for various user roles and devices in smart grid. *IEEE Transactions on Information Forensics and Security*, *11*(5), 907-921.

Schoder, D., Fischbach, K. (2003). Peer-to-peer prospects. *Communications of the ACM, 46*(2), 27 -29.

Seuring, S., & Müller, M. (2008). Core issues in sustainable supply chain management–a Delphi study. *Business Strategy and the Environment*, *17*(8), 455-466.

Shahidi, N., Ou, G., Telford, J., & Enns, R. (2015). When trainees reach competency in performing ERCP: a systematic review. *Gastrointestinal Endoscopy*, *81*(6), 1337-1342.

Shaw, R., Chen, C., Harris, A., & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100.

Shepherd, M. M., & Mejias, R. J. (2016). Nontechnical Deterrence Effects of Mild and Severe Internet Use Policy Reminders in Reducing Employee Internet Abuse. *International Journal of Human-Computer Interaction*, *32*(7), 557-567.

Shippmann, J., Ash, R., Batjtsta, M., Carr, L., Eyde, L., Hesketh, B., Kehoe, J., Pearlman, K., Prien, E. & Sanchez, J. (2000). The practice of competency modeling. *Personnel Psychology*, *53*(3), 703-740.

Shulman, L. (1987). Knowledge and teaching: Foundations of the new reform. *Harvard Educational Review, 57*(1), 1-23.

Smith, M. J., Wagner, C., Wallace, K. J., Pourabdollah, A., & Lewis, L. (2016). The contribution of nature to people: Applying concepts of values and properties to rate the management importance of natural elements. *Journal of Environmental Management*, *175*, 76-86.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224.

Sizer, P. S., Felstehausen, V., Sawyer, S., Dornier, L., Matthews, P., & Cook, C. (2007). Eight critical skill sets required for manual therapy competency: a Delphi study and factor analysis of physical therapy educators of manual therapy. *Journal of Allied Health*, *36*(1), 30-40.

Skinner, R., Nelson, R., Chin, W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems*, *37*(1), 2.

Skulmoski, G., Hartman, F., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education: Research, 6*(1), 1-21.

Smith, D. (2015). Securing the law firm. *Computer Fraud & Security*, *2015*(4), 5-7.

Staggers, N., Gassert, C. A., & Curran, C. (2002). A Delphi study to determine informatics competencies for nurses at four levels of practice. *Nursing Research*, *51*(6), 383-390.

Straub, D. (1989). Validating instruments in MIS research. *MIS Quarterly, 13(2)*, 147-169.

Straub, D., Rai, A., & Klein, R. (2004). Measuring firm performance at the network level: A nomology of the business impact of digital supply networks. *Journal of Management Information Systems*, *21*(1), 83-114.

Succar, B., Sher, W., & Williams, A. (2013). An integrated approach to BIM competency assessment, acquisition and application. *Automation in Construction*, *35*, 174-189.

Sugii, J., & Nojiri, K. (2015). Device management technology for preventing data leakage. *FUJITSU Scientific and Technical Journal*, *51*(2), 99-104.

Sumsion T. (1998). The Delphi technique: an adaptive research tool. *British Journal of Occupational Therapy, 61*(4), 153-156.

Symantec (2016). *Webmail security and associated best practices.* Retrieved Jul 22, 2016, from: http://www.symantec.com/connect/blogs/webmail-security-and-associated-best-practices

Tan, A. Z., Chua, W. Y., & Chang, K. T. (2014). Location Based Services and Information Privacy Concerns among Literate and Semi-literate Users. *2014 47th Hawaii International Conference on System Sciences (HICSS)*, pp. 3198-3206.

Terkan, R. (2013). Effective marketing at education: Importance of communication materials. *International Review of Management and Marketing*, *3*(4), 146-152.

Terrell, S. R. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York, NY: The Guilford Press.

Tobey, D. (2015). A vignette-based method for improving cybersecurity talent management through cyber defense competition design. *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, Newport Beach, CA, pp. 31-39.

Toth, P., & Klein, P. (2013). A role-based model for federal information technology/cyber security training. *NIST Special Publication*, *800*(16), 1-152.

Torkzadeh, G., & Dhillon, G. (2002). Measuring factors that influence the success of Internet commerce. *Information Systems Research*, *13*(2), 187-204.

Trippe, D., Moriarty, K., Russell, T., Carretta, T., & Beatty, A. (2014). Development of a cyber/information technology knowledge test for military enlisted technical training qualification. *Military Psychology*, *26*(3), 182-198.

Verma, R., Kantarcioglu, M., Marchette, D., Leiss, E., & Solorio, T. (2015). Security analytics: essential data analytics knowledge for cybersecurity professionals and students. *IEEE Security & Privacy*, *13*(6), 60-65.

Wang, Y., Li, C., & Cheng, N. (2014). Internet security protection in personal sensitive information. *Computational Intelligence and Security (CIS), 2014 Tenth International Conference on,* Kunming, Yunnan Province, China*,* pp. 628-632.

Wang, N., Schnipke, D., & Witt, E. A. (2005). Use of knowledge, skill, and ability statements in developing licensure and certification examinations. *Educational Measurement: Issues and Practice*, *24*(1), 15-22.

Warkentin, M., Straub, D., & Malimage, K. (2012). Measuring secure behavior: A research commentary. *Proceedings of the Annual Symposium on Information Assurance (ASIA) 2012,* Albany, New York, pp. 1-8.

Warren, M. (2015). Modern IP theft and the insider threat. *Computer Fraud & Security*, *2015*(6), 5-10.

Watson II, J. C., & Portenga, S. T. (2014). An overview of the issues affecting the future of certification in sport psychology. *Athletic Insight*, *6*(3), 261-276.

Weber, M. R., Crawford, A., Rivera, D., & Finley, D. A. (2011). Using Delphi panels to assess soft skill competencies in entry level managers. *Journal of Tourism Insights*, *1*(1), 12.

Weeden, S., Cooke, B., & McVey, M. (2013). Underage children and social networking. *Journal of Research on Technology in Education*, *45*(3), 249-262.

Worrell, J., Di Gangi, P., & Bush, A. (2013). Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems*, *14*(3), 193-208.

Yule, S., Flin, R., Paterson‐Brown, S., Maran, N., & Rowley, D. (2006). Development of a rating system for surgeons' non‐technical skills. *Medical Education*, *40*(11), 1098-1104.

Zhao, J., Ha, S., & Widdows, R. (2016). The influence of social capital on knowledge creation in online health communities. *Information Technology and Management*, *17*(4), 311-321.

Zhauniarovich, Y., Russello, G., Conti, M., Crispo, B., & Fernandes, E. (2014). MOSES: supporting and enforcing security profiles on smartphones. *IEEE Transactions on Dependable and Secure Computing*, *11*(3), 211-223.

Zipf, G. K. (2016). *Human behavior and the principle of least effort: An introduction to human ecology*. Ravenio Books.