A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users

Richard Nilsen
Nova Southeastern University, rn380@nova.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Steven Terrell
Nova Southeastern University, terrell@nova.edu

Dawn Beyer
Lockheed Martin, dawn.m.beyer@lmco.com

Abstract
Organizational information system users (OISUs) that are open to cyber threats vectors are contributing to major financial and information losses for individuals, businesses, and governments. Moreover, technical cybersecurity controls may be rendered useless due to a lack of cybersecurity competency of OISUs. The main goal of this research study was to propose and validate, using subject matter experts (SMEs), a reliable hands-on assessment prototype tool for measuring the knowledge, skills, and abilities (KSAs) that comprise the cybersecurity competency of an OISU. Primarily using the Delphi methodology, this study implemented four phases of data collection using cybersecurity SMEs for proposing and validating OISU: (a) KSAs, (b) KSA measures, (c) KSA measure weights, and (d) cybersecurity competency threshold. A fifth phase of data collection occurred measuring the cybersecurity competency of 54 participants. Phase 1 proposed and validated three OISU cybersecurity abilities, 23 OISU cybersecurity knowledge units (KU), and 22 OISU cybersecurity skill areas (SA). Phase 2 proposed and validated 90 KSA measures for 47 knowledge topics (KT) and 43 skill tasks (ST). Phase 3 proposed and validated the weights for four knowledge categories (KC) and four skill categories (SC). Phase 4 proposed and validated an OISU cybersecurity competency threshold (index score) of 80%. Phase 5 of this study measured the cybersecurity competency of 54 OISUs using the MyCyberKSAs^{TM} prototype cybersecurity competency assessment tool. Phase 5 conducted data analysis by computing levels of dispersion and one-way analysis of variance (ANOVA), which indicated that annual cybersecurity training and job function are significant, providing evidences for significant differences in OISU cybersecurity competency.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users

Richard Nilsen

Yair Levy

Steven Terrell

Dawn Beyer

Abstract

Organizational information system users (OISUs) that are open to cyber threats vectors are contributing to major financial and information losses for individuals, businesses, and governments. Moreover, technical cybersecurity controls may be rendered useless due to a lack of cybersecurity competency of OISUs. The main goal of this research study was to propose and validate, using subject matter experts (SMEs), a reliable hands-on assessment prototype tool for measuring the knowledge, skills, and abilities (KSAs) that comprise the cybersecurity competency of an OISU. Primarily using the Delphi methodology, this study implemented four phases of data collection using cybersecurity SMEs for proposing and validating OISU: (a) KSAs, (b) KSA measures, (c) KSA measure weights, and (d) cybersecurity competency threshold. A fifth phase of data collection occurred measuring the cybersecurity competency of 54 participants. Phase 1 proposed and validated three OISU cybersecurity abilities, 23 OISU cybersecurity knowledge units (KU), and 22 OISU cybersecurity skill areas (SA). Phase 2 proposed and validated 90 KSA measures for 47 knowledge topics (KT) and 43 skill tasks (ST). Phase 3 proposed and validated the weights for four knowledge categories (KC) and four skill categories (SC). Phase 4 proposed and validated an OISU cybersecurity competency threshold (index score) of 80%. Phase 5 of this study measured the cybersecurity competency of 54 OISUs using the MyCyberKSAs^{TM} prototype cybersecurity competency assessment tool. Phase 5 conducted data analysis by computing levels of dispersion and one-way analysis of variance (ANOVA), which indicated that annual cybersecurity training and job function are significant, providing evidences for significant differences in OISU cybersecurity competency.

Disciplines

Information Security | Management Information Systems | Technology and Innovation

Title

A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users

Abstract

Organizational information system users (OISUs) that are open to cyber threats vectors are contributing to major financial and information losses for individuals, businesses, and governments. Moreover, technical cybersecurity controls may be rendered useless due to a lack of cybersecurity competency of OISUs. The main goal of this research study was to propose and validate, using subject matter experts (SMEs), a reliable hands-on assessment prototype tool for measuring the knowledge, skills, and abilities (KSAs) that comprise the cybersecurity competency of an OISU. Primarily using the Delphi methodology, this study implemented four phases of data collection using cybersecurity SMEs for proposing and validating OISU: (a) KSAs, (b) KSA measures, (c) KSA measure weights, and (d) cybersecurity competency threshold. A fifth phase of data collection occurred measuring the cybersecurity competency of 54 participants. Phase 1 proposed and validated three OISU cybersecurity abilities, 23 OISU cybersecurity knowledge units (KU), and 22 OISU cybersecurity skill areas (SA). Phase 2 proposed and validated 90 KSA measures for 47 knowledge topics (KT) and 43 skill tasks (ST). Phase 3 proposed and validated the weights for four knowledge categories (KC) and four skill categories (SC). Phase 4 proposed and validated an OISU cybersecurity competency threshold (index score) of 80%. Phase 5 of this study measured the cybersecurity competency of 54 OISUs using the MyCyberKSAs^{TM} prototype cybersecurity competency assessment tool. Phase 5 conducted data analysis by computing levels of dispersion and one-way analysis of variance (ANOVA), which indicated that annual cybersecurity training and job function are significant, providing evidences for significant differences in OISU cybersecurity competency.

Keywords

Cybersecurity Competency, Cybersecurity Skills, Cybersecurity Knowledge, Cybersecurity Abilities, Cybersecurity KSAs

Introduction

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). 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). Inadequate cybersecurity competency of IS users continues to result in significant financial, information, and intellectual property loses for organizations as well as governments (Barlow, Warkentin, Ormond, & Dennis, 2013; Choi, Levy, & Hovav, 2013; Shaw, Chen, Harris, & Huang, 2009).

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 (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.

A literature review on SETA programs in the private sector and 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, yet it appears to be assumed constantly by organizational leaders and top management (Assante & Tobey, 2011; Evans & Reeder, 2010; Johnson, 2012). As such, there was a need to establish a definition and develop measurement of cybersecurity competency.

Background

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 critical vulnerability to organizational networks, which is of utmost importance since vulnerabilities are 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 void 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). Thus, 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. This study intended to build on the work of Behrens et al. (2012), as well as Toth and Klein (2013), by developing the MyCyberKSAs™ prototype cybersecurity competency assessment tool.

The MyCyberKSAs™ prototype cybersecurity competency assessment tool was in the form of an iPad application or can be run as 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.

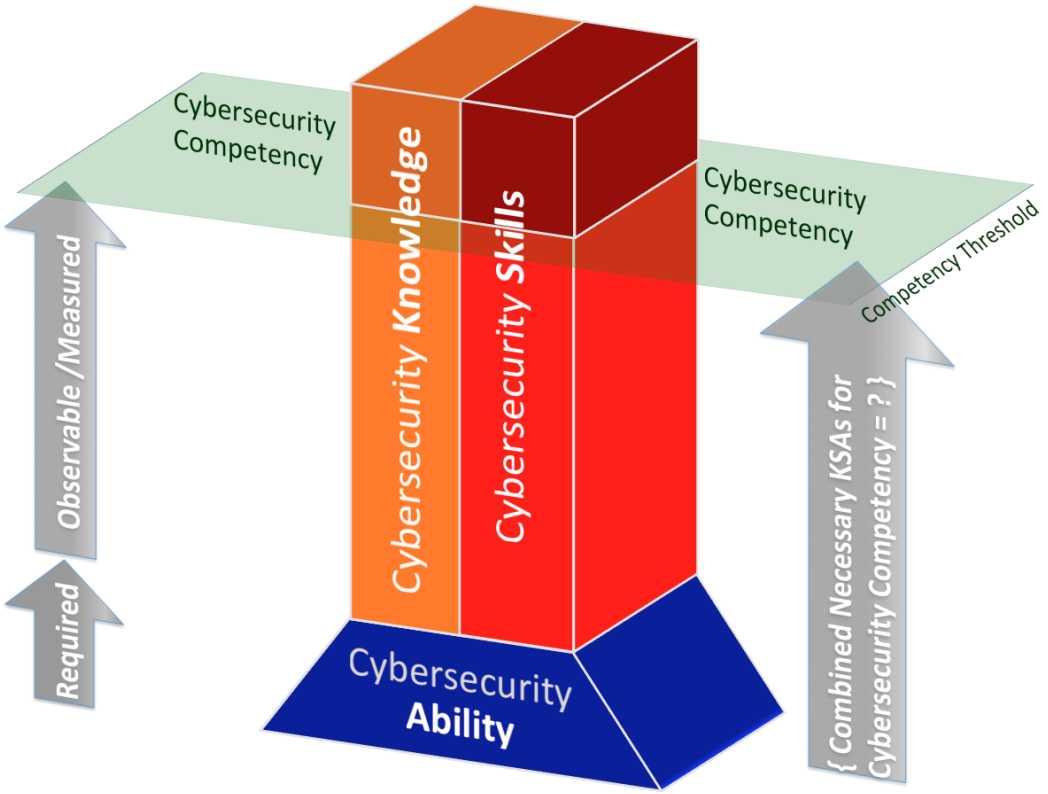

Figure 1. Model of Combined Necessary KSAs for Cybersecurity Competency Attainment for an Organizational Information System User (OSIU)

As such, when an individual possesses the required cybersecurity abilities, the increase in cybersecurity knowledge and skills based on experience will reach a certain level that can be identified as cybersecurity competency threshold. The intent of the uncovering of the cybersecurity competency threshold is to establish a minimum index score that needs to 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, such as done in this study (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 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 assessment prototype 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 assessment prototype tool scoring at which cybersecurity competency of OISUs is reached. The fifth specific goal of this study was to measure the cybersecurity competency of 50 OISUs and report the results of such assessments. Thus, 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} assessment prototype tool to collect cybersecurity competency data from 50 OISUs.

Methodology

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 from Nova Southeastern University. 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. 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, but aggregated information about the level of knowledge, experience, certifications, and additional indicators were used to ensure the SMEs are indeed cybersecurity experts and somewhat consistent across the phases. Phase 5 of this study used a sample of 54 OISUs from government and

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice

industry to test the prototype MyCyberKSAs™ cybersecurity competency assessment prototype tool. Pre-analysis data screening, a process used to detect issues with collected data, was conducted on data collection sets from each phase of this study (Levy, 2006).

Phase 1

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. Appendix A shows the initial KSA list gathered from literature review and USG documents for the Phase 1 Survey instrument for OISU cybersecurity KSA proposal and validation. In Phase 1 the SMEs had the ability to add, modify, or remove KSAs from the initial list, thus, proposing and validating all required OISU KSAs.

Phase 2

The instrument for Phase 2 presented knowledge units and skill tasks derived from the validated Phase 1 KSA list 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. Surrogating abilities significantly reduced the time commitment of MyCyberKSAs™ 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™ prototype tool size, surrogating for abilities was critical to maintain usability of the tool. Appendix B shows the knowledge topics (KTs) and skill tasks (STs) from the knowledge units (KUs) and skill areas (SA) for which assessment questions and vignettes were validated by SMEs.

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

http://digitalcommons.kennesaw.edu/ccerp 6

weighted, nor do abilities need to be weighted. The knowledge KSAs were divided into four knowledge categories, as shown in Appendix B. SMEs were asked to allocate 100 points among the knowledge categories. The skill KSAs were also divided into four skill categories as shown in Appendix B. SMEs were asked to allocate 100 points among the skill categories.

Phase 4

The instrument for Phase 4 requested SMEs proposed cybersecurity competency threshold values. The Phase 4 survey presented the SMEs with the results from Phases 1-3. Additionally, the SMEs were given a link to the MyCyberKSAs™ prototype assessment tool. The SME responses were then averaged to produce the cybersecurity competency threshold.

Phase 5

The instrument for Phase 5 used participants to test the MyCyberKSAs™ prototype tool. 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.

Proposed Samples

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, Hartman, and Krahn (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 an avoidance of 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, however, the qualifications of the experts across all phases in aggregated form are comparable. 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™ cybersecurity competency assessment tool.

Results

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. 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.

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.

Phase 2

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.

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 30 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.

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 knowledge categories (KCs) and four skill categories (SCs). 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). 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). The SMEs also validated weights for Overall Knowledge (OK) and Overall Skill (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. The results of Phase 3 are shown in Table 1.

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 1. Summary of Phase 3 Results

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 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. The SMEs proposed the OISU cybersecurity competency threshold of 80%.

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, mainly due to the extended time required to complete the assessment (about 45 minutes). Using the 50 OISU sample allowed for data analysis of cybersecurity competency by each demographic group. A summary of OISU cybersecurity competency scores is shown in Figure 2. As shown in Figure 2, 69% OISUs were measured as possessing cybersecurity competency for organizational information systems. Figures 3-9 show the summaries of cybersecurity competency means and standard deviations by demographic groups.

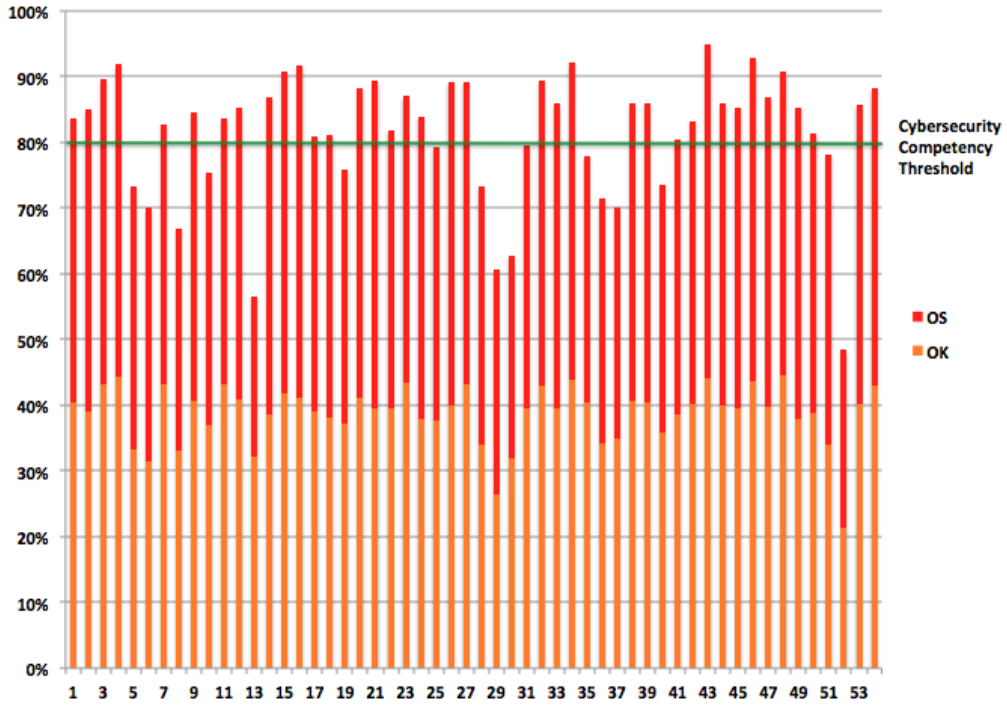

Figure 2. Summary of Phase 5 OISU Cybersecurity Competency Scores with OK and OS components (N = 54)

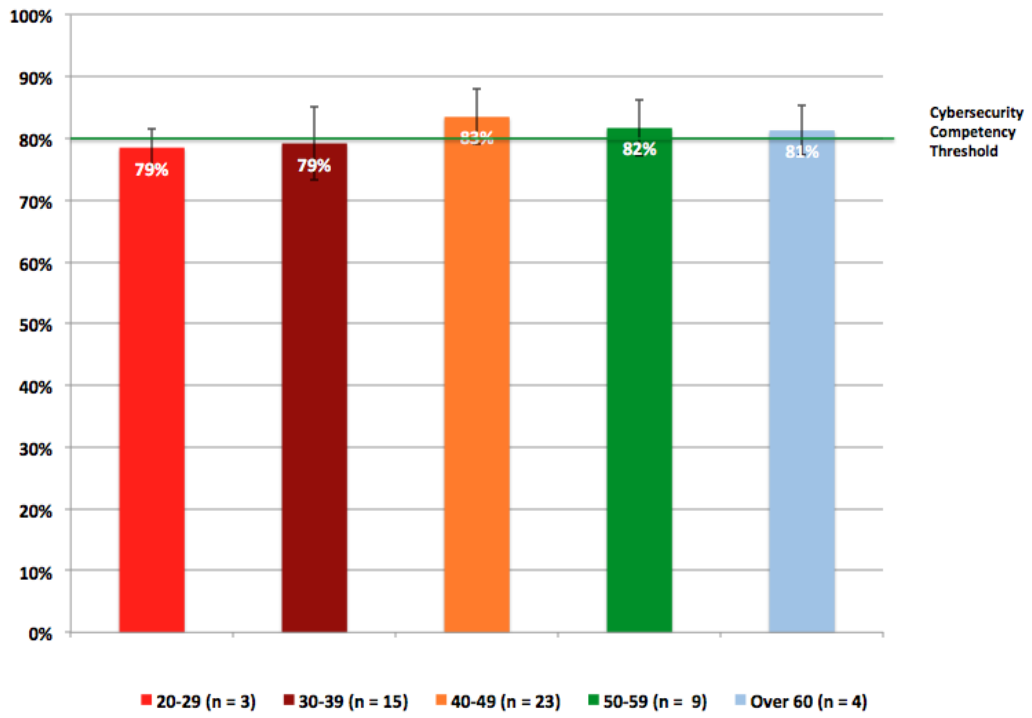

Figure 3. Summary of cybersecurity competency means and standard deviations by age (N = 54)

As shown in Figure 3, 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 3 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.

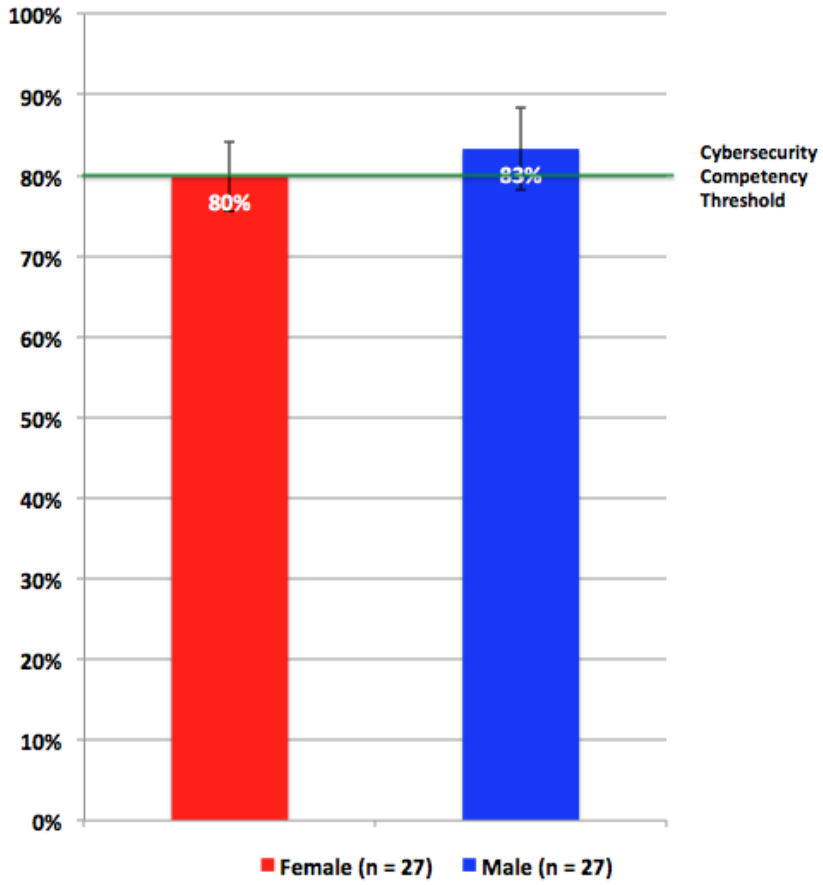

Figure 4. Summary of cybersecurity competency means and standard deviations by gender (N = 54)

Figure 4 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.

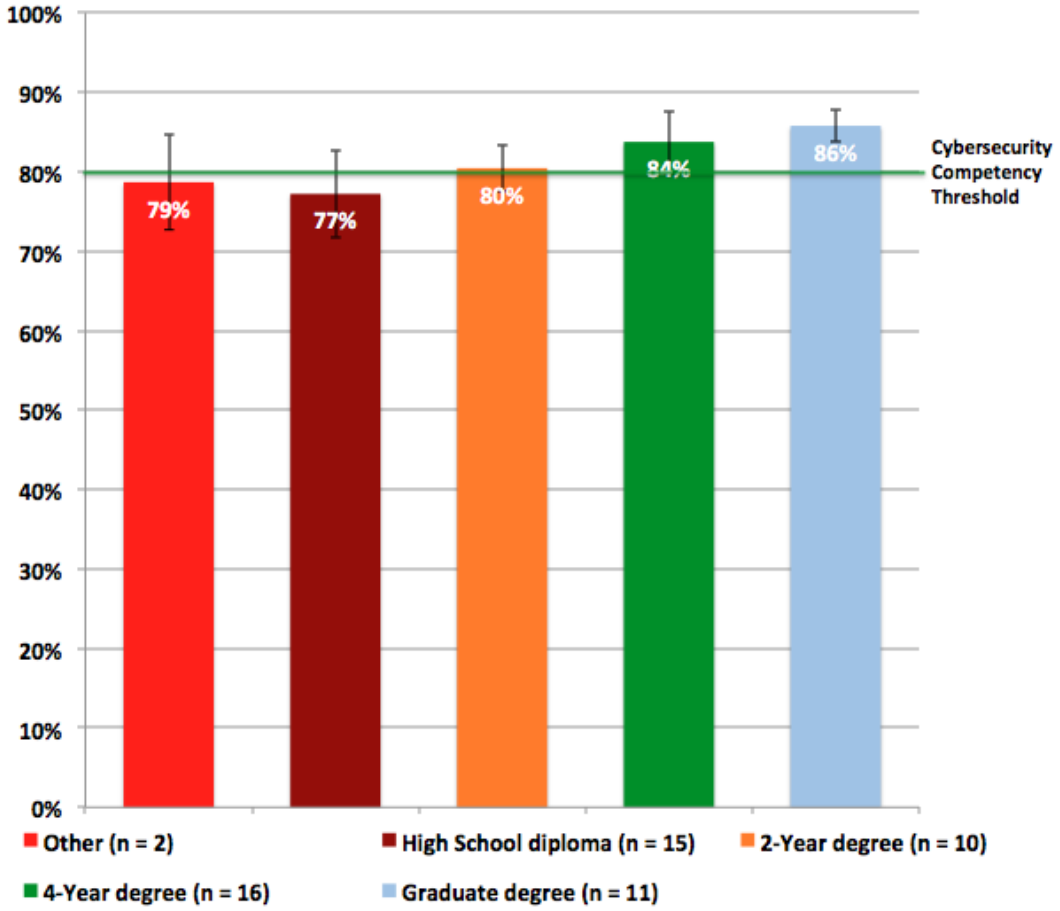

Figure 5. Summary of cybersecurity competency means and standard deviations by education (N = 54)

As shown in Figure 5, 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 5 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.

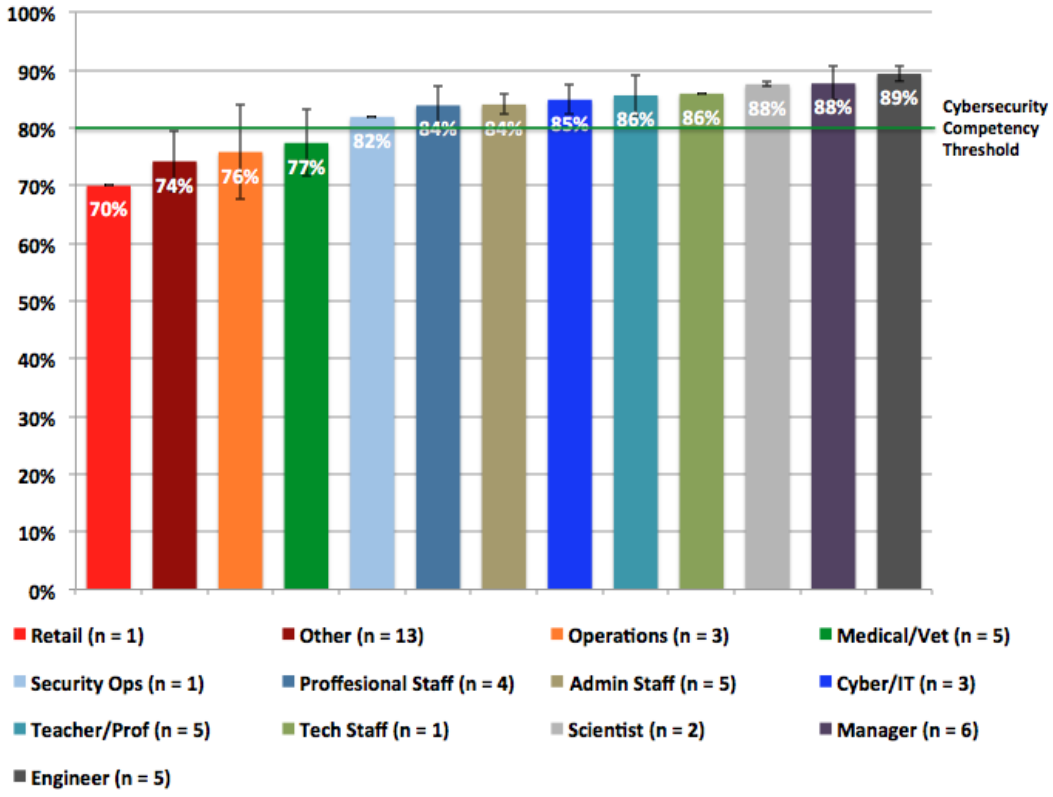

Figure 6. Summary of cybersecurity competency means and standard deviations by job function (N = 54)

Figure 6 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 6 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.

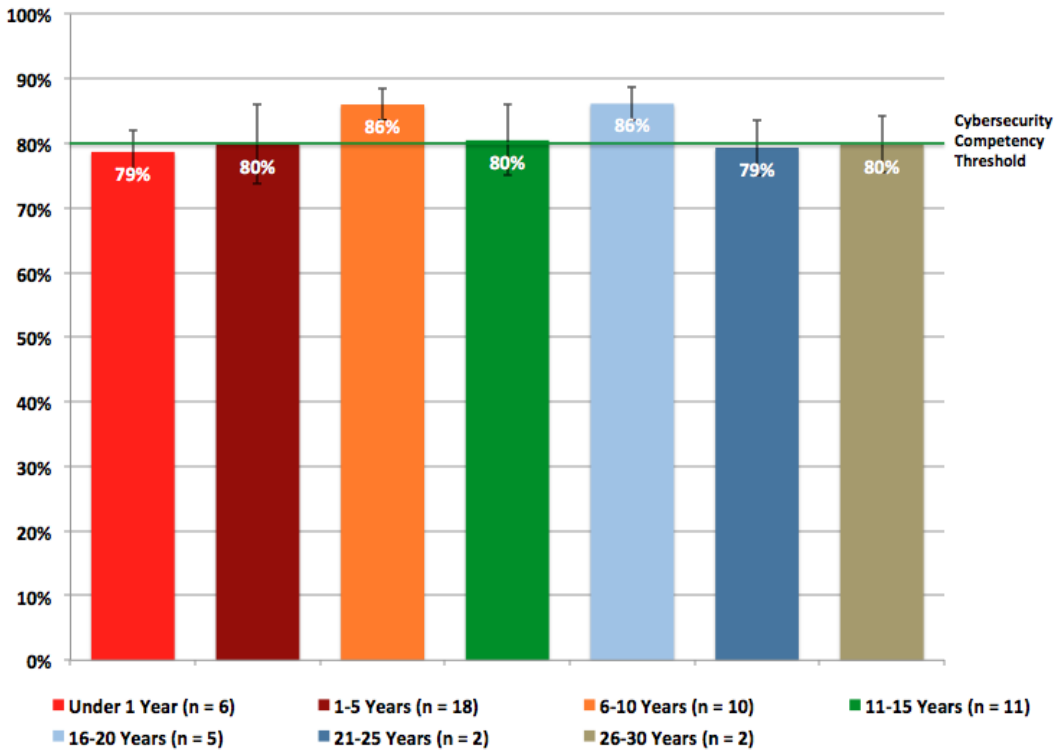

Figure 7. Summary of cybersecurity competency means and standard deviations by time with current employer (N = 54)

Figure 7 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 7 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.

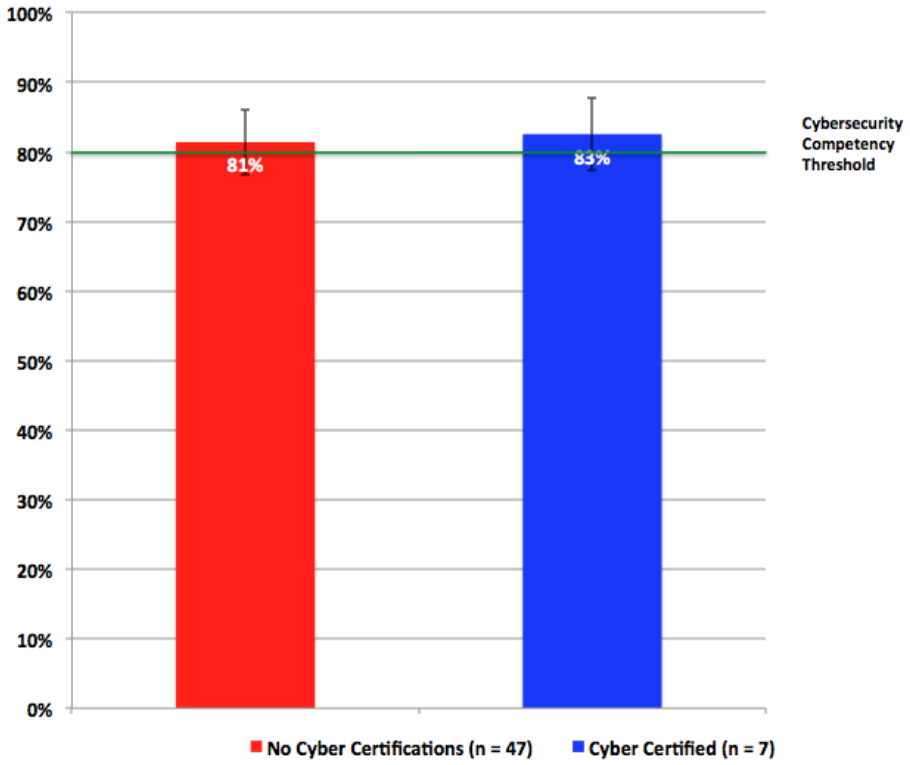

Figure 8. Summary of cybersecurity competency means and standard deviations for OISUs with and without cybersecurity certification (N = 54)

Figure 8 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.

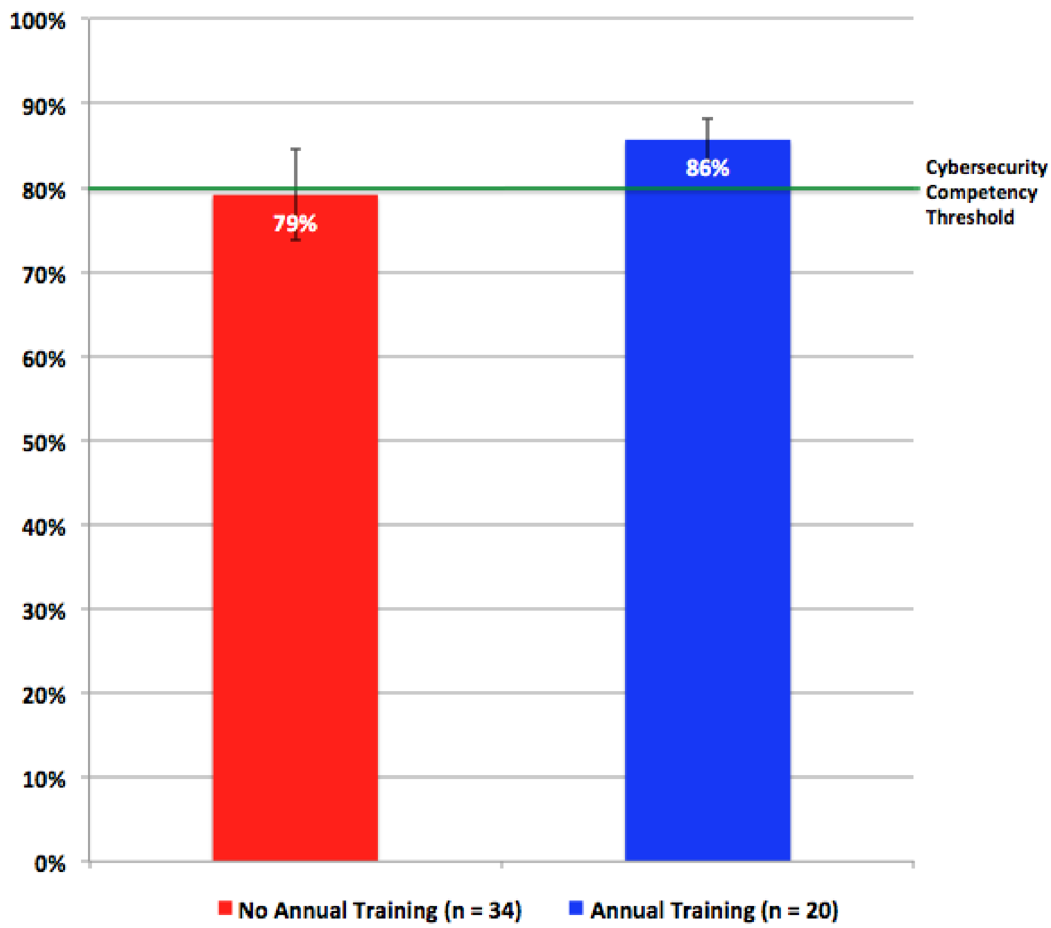

Figure 9. Summary of cybersecurity competency means and standard deviations for OISUs with and without annual cybersecurity training (N = 54)

As shown in Figure 9, 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 9 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.

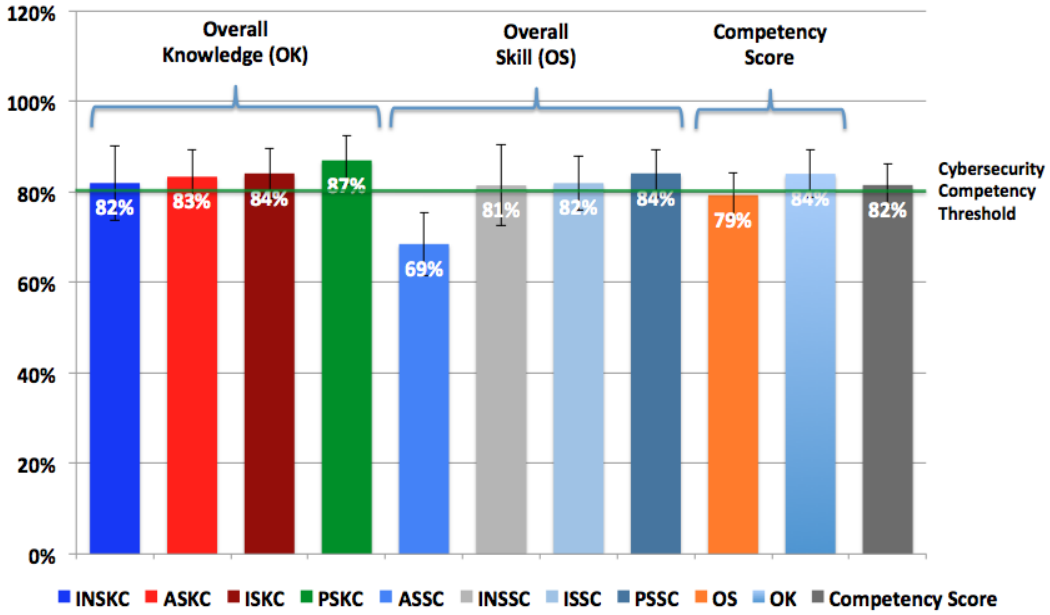

Figure 10. Summary of means and standard deviations for KCs, SCs, OK, OS, and cybersecurity competency scores

Figure 10 shows that the mean OK scores for OISUs was 5% higher than the mean 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.

		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

Table 4. ANOVA Results by Demographics (N = 54)

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

Table 4 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.

Conclusions

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.

This research study attempts to increase the body of knowledge by providing an approach for organizations to build their own OISU cybersecurity competency assessment tools. The results of this study suggest that age, gender, cybersecurity certification, and time with company are not significant. Moreover, the results of this study indicates 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 indicates that annual cybersecurity training is effective in increasing the OISU cybersecurity competency. Furthermore, a result of this study suggests that job function causes positive increases to cybersecurity competency.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

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.

Assante, M., & Tobey, D. (2011). Enhancing the cybersecurity workforce. *IT Professional*, *13*(1), 12-15.

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.

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

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.

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.

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.

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

Doneda, D., & Almeida, V. (2015). Privacy governance in cyberspace. *IEEE Internet Computing*, *19*(3), 50-53.

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

Garfinkel, S. (2012). The cybersecurity risk. *Communications of the ACM*, *55*(6), 29-32.

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.

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.

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.

Jacob, S. M., & Chalia, D. S. (2015). Research highlights: July-September 2015. *Indian Journal of Research in Homoeopathy*, *9*(3), 202.

Johnson, C. (2012). CyberSafety: on the interactions between cybersecurity and the software engineering of safety-critical systems. *Achieving System Safety*, 85-96.

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.

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.

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

O'Neil, L. R., Assante, M. J., & Tobey, D. H. (2012). *SmartGrid cybersecurity: Job performance model report.* National Technical Information Service, Alexandria, VA.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy, 10*(3), 76-79.

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.

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.

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.

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.

Terrell, S. R. (2012). Statistics translated: A step-by-step guide to analyzing and interpreting data. New York, NY: The Guilford Press.

Toth, P., & Klein, P. (2013). A role-based model for federal information technology/cyber security training. *NIST Special Publication*, *800*(16), 1-152.

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.

Appendix A

Phase 1 Survey KSAs from literature review and USG documents

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	Parsons et al., 2014;

		handling	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
	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
Skill	S7	Skill in avoiding actions that	Barlow et al., 2013; DISA,

	increase exposure to malicious code downloading or execution	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
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

Appendix B
Phase 2 Survey KSA measures of KTs and STs

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
	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

Submission to KSU Proceedings on Cybersecurity Education, Research and Practice [ ]

	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
	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

https://digitalcommons.kennesaw.edu/ccerp 38

	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
	Knowledge of Internet use	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
	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
Physical Security Knowledge Category	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

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
Application Security Skill Category	Skill in managing cookie settings and usage	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
	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
Information Security	Skill in identifying the spillage of sensitive	SS1	Demonstrate the task of reporting a spillage incident

Skill Category	information and PII		
	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
	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
Internet and Network Security Skill Category	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-	SSP1	Demonstrate the task of not divulging

	phishing attempts of sensitive information and PII		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
	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
Physical Security Skill Category	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