

2016

# Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills

Melissa Carlton

Nova Southeastern University, [melissa.carlton.phd@gmail.com](mailto:melissa.carlton.phd@gmail.com)

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: [http://nsuworks.nova.edu/gscis\\_etd](http://nsuworks.nova.edu/gscis_etd)

 Part of the [Computer Sciences Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Melissa Carlton. 2016. *Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (979)  
[http://nsuworks.nova.edu/gscis\\_etd/979](http://nsuworks.nova.edu/gscis_etd/979).

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

Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On  
Measure of Non-IT Professionals' Cybersecurity Skills

by

Melissa Carlton

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

2016

We hereby certify that this dissertation, submitted by Melissa Carlton, 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

\_\_\_\_\_  
Date

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

\_\_\_\_\_  
Date

\_\_\_\_\_  
Michelle Ramim, Ph.D.  
Dissertation Committee Member

\_\_\_\_\_  
Date

Approved:

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

\_\_\_\_\_  
Date

College of Engineering and Computing  
Nova Southeastern University

2016

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

## Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills

By  
Melissa Carlton  
October 2016

Completing activities online are a part of everyday life, both professionally and personally. But, conducting daily operations, interacting, and sharing information on the Internet does not come without its risks as well as a potential for harm. Substantial financial and information losses for individuals, organizations, and governments are reported regularly due to vulnerabilities as well as breaches caused by insiders. Although advances in Information Technology (IT) have been significant over the past several decades when it comes to protection of corporate information systems (IS), human errors and social engineering appear to prevail in circumventing such IT protections. While most employees may have the best of intentions, without cybersecurity skills they represent the weakest link in an organization's IS security. Skills are defined as the combination of knowledge, experience, and ability to do something well. Cybersecurity skills correspond to the skills surrounding the hardware and software required to execute IS security to mitigate cyber-attacks.

The main goal of this research study was to develop a scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills. As opposed to IT professionals, end-users are one of the weakest links in the cybersecurity chain, due to their limited cybersecurity skills. Historically, non-IT professionals (i.e., office assistants, managers, executives) have access to sensitive data and represent 72% to 95% of cybersecurity threats to organizations. This study addressed the problem of threats to organizational IS due to vulnerabilities and breaches caused by employees. Current measures of cybersecurity skills of non-IT professionals are based on self-reported surveys and were found inaccurate. Prior IS and medical research found participants view scenarios as nonintrusive and unthreatening. Therefore, this research study utilized scenarios with observable hands-on tasks to measure and quantify cybersecurity skills of non-IT professionals.

This study included developmental research with a sequential-exploratory approach to combine qualitative and quantitative data collection. To ensure validity and reliability of the Cybersecurity Skills Index (CSI), a panel of 18 subject matter experts (SMEs) reviewed the CSI following the Delphi expert methodology. The SMEs' responses were incorporated into the development of an iPad application (app) prototype (MyCyberSkills™). Following the iPad app prototype development, eight SMEs

provided feedback on the scenarios, tasks, and scoring of the app using the Delphi technique. Furthermore, pilot testing of the app was conducted by manually collecting and scoring the hands-on task performance of a group of 21 non-IT professionals. The manually collected data were compared to the app computed results to ensure reliability and validity. All revisions were incorporated into the prototype prior to the start of the empirical research phase.

Once the iPad app prototype was completed and fully tested, the quantitative research phase used the prototype to collect data and document the results of the measure. Participants from multiple public organizations were asked to complete the scenarios-based, hands-on tasks as presented in the prototype. Following the pre-analysis data screening, this study used a combination of descriptive statistics and one-way analysis of variance (ANOVA) to address the research questions. Results from 188 participants indicate that educational level and experience using technology appear to be significant demographic variables when it comes to the level of cybersecurity skills demonstrated by non-IT professionals. Moreover, job function, hours accessing the Internet, or primary online activity did not appear to be significant variables when it comes to the level of cybersecurity skills of this population.

This research validated that the CSI benchmarking index could be used to assess an individual's cybersecurity skills level. As organizations continue to rely on the Internet for conducting their daily operations, understanding an employee's cybersecurity skills level is critical to securing an organization's IS. Moreover, the CSI operationalized into the MyCyberSkills™ iPad app prototype can be used to assess an organization's employee's demonstrated skills on cybersecurity tasks. Furthermore, assessing the cybersecurity skills levels of employees could provide an organization insight into what is needed to further mitigate threats due to vulnerabilities and breaches caused by employees. Discussions and implications for future research are provided.

## **Acknowledgements**

To my Lord and Savior, Jesus Christ, thank you for your saving grace and placement of those that crossed paths with me through this wonderful, yet challenging academic journey. This work is dedicated to my husband, Gordon, and my parents, Billy and Pam. Thank you for encouraging me to get a Ph.D. instead of a third Master degree. Your countless prayers, continuous love, and consistent support kept me going when I thought I could go no more.

My utmost appreciation and thankfulness to my advisor, Dr. Yair Levy, who has nurtured and challenged me. Your guidance and supervision through this rigorous academic journey has lead me to be transformed, realize my potential, and find my passion. It has been a distinct honor to work with you; I will miss our frequent phone chats most. I also wish to thank my committee members, Dr. Steven Terrell and Dr. Michelle Ramim, for all their insightful conversations and feedback throughout this process.

I want to express my gratitude to Dr. Gary Margules, Roxana Ross, and their team in Nova Southeastern University (NSU)'s Tech Transfer department as well as NSU's Cybersecurity Incubator partner, Abanacle, for making the MyCyberSkills™ tool available to many others beyond this research. Thank you, Felix, Jem, Trevor, and Andrea, for your assistance; I learned so much from each of you. To Banyon, Randy, the members of First Baptist Church, the Chick-Fil-A crew, and numerous others, thank you for your support while I fulfilled my dream of achieving a Ph.D. in Information Systems.

Finally, to the person that has been lead here, especially the future Ph.D. candidate, I pray you find the nugget of information you are seeking and are lifted on the shoulders of giants as I was throughout this life changing process. Be encouraged and follow the breadcrumbs that will lead you to your destination. More importantly, take time to enjoy the journey.

## Table of Contents

<b>Abstract</b>	<b>iii</b>
<b>Acknowledgements</b>	<b>v</b>
<b>List of Tables</b>	<b>ix</b>
<b>List of Figures</b>	<b>xi</b>

### Chapters

<b>1. Introduction</b>	<b>1</b>
Background	1
Problem Statement	2
Dissertation Goal	4
Research Questions	9
Relevance and Significance	10
Relevance	10
Significance	11
Barriers and Issues	11
Limitations and Delimitations	13
Limitations	13
Delimitations	14
Definition of Terms	14
Summary	17
<b>2. Review of the Literature</b>	<b>18</b>
Introduction	18
Skills and Competencies	19
Skills Defined	19
Competence vs. Skills	22
Information Technology Skills	25
Data Breaches	28
Social Engineering	32
Malware	34
Personally Identifiable Information	37
Phishing	41
Social Media	43
Work Information Systems Security	46
Confidential Information Exposure	48
Password Exploitations	51
Cybersecurity	54

Cybersecurity Skills Shortage	57
Cybersecurity Risk Mitigation and Tools	60
Summary of What is Known and Unknown	65
<b>3. Methodology</b>	<b>67</b>
Overview of Research Design	67
Instrument Development	69
Expert Panel	71
Scenario Method	73
Hands-On Tasks and Skill Assessments	74
MyCyberSkills™ iPad App Development	74
Reliability and Validity	77
Reliability	78
Validity	79
Pilot-Test Initial App	79
Design and Empirical Study: Revised App	81
Population and Sample	81
Data Collection	82
Data Analysis	83
Resources	83
Summary	85
<b>4. Results</b>	<b>87</b>
Overview	87
Qualitative Research and Expert Panel (Phase One)	87
Qualitative and Quantitative Research (Phase Two)	90
Quantitative Research (Phase Three)	93
Pre-Analysis Data Screening	93
Demographic Analysis	96
Data Analysis	104
Summary	118
<b>5. Conclusions, Implications, Recommendations, and Summary</b>	<b>120</b>
Conclusions	120
Discussion	121
Implications	122
Recommendations and Future Research	123
Summary	124
<b>Appendices</b>	
A. Site Approval Letter	129
B. Institutional Review Board Approval Letter	130
C. Expert Recruitment Email	131
D. Expert Qualitative and Quantitative Questionnaire	133
E. Pilot Study Recruitment Email	136
F. Pilot Study Informed Consent Form	138



G. Research Study Recruitment Flyer 141  
H. Research Study Informed Consent Form 142

**References 145**

## **List of Tables**

### **Tables**

1. Summary of Skills Defined 20
2. Summary of Competence vs. Skills 23
3. Summary of Information Technology Skills 26
4. Summary of Data Breaches 31
5. Summary of Social Engineering 34
6. Summary of Malware 36
7. Summary of Personally Identifiable Information 39
8. Summary of Phishing 42
9. Summary of Social Media 44
10. Summary of Work Information Systems Security 47
11. Summary of Confidential Information Exposure 50
12. Summary of Password Exploitations 53
13. Summary of Cybersecurity 56
14. Summary of Cybersecurity Skills Shortage 59
15. Summary of Cybersecurity Risk Mitigation and Tools 64
16. Rankings of the Top Nine Cybersecurity Skills 90
17. Cybersecurity Skills Index and SMEs Ranked Cybersecurity Skills 91
18. Delphi Expert Panel Suggested Adjustments to Initial Prototype 92
19. Means and Standard Deviations for the Population (N=188) 95

20. Descriptive Statistics of the Population (N=188)	97
21. Descriptive Statistics for Each Group in the Population	99
22. Means and Standard Deviations for Each Group of the Population	101
23. ANOVA Results for Each Recruitment Location (N=188)	104
24. ANOVA Results for Age Group (N=188)	106
25. ANOVA Results for Gender (N=188)	108
26. ANOVA Results for Job Function (N=188)	110
27. ANOVA Results for Hours Accessing the Internet (N=188)	112
28. ANOVA Results for Primary Activity (N=188)	114
29. ANOVA Results for Education (N=188)	115
30. ANOVA Results for Experience Using Technology (N=188)	117

## List of Figures

### Figures

1. Skill Development Stages Over Time 20
2. NIST's Cybersecurity Framework Functions 63
3. Overview of the Research Design Process 68
4. CSI Development Process 71
5. Conceptual Design of the CSI Operationalized Within the MyCyberSkills™ iPad App Prototype 75
6. Scenario-Based, Hands-On Task Skill Levels 77
7. Means of the Individual Skills, Skill Categories, and Overall CSI 95
8. Means of the Individual Skills, Skill Categories, and Overall CSI for Group A (Members of Public Place of Worship) (N=108) 102
9. Means of the Individual Skills, Skill Categories, and Overall CSI for Group B (Members of Public Places of Businesses) (N=80) 103
10. Means and Standard Deviations of Malware and PII Skills Categories by Age Group (N=188) 106
11. Means and Standard Deviations of WIS Skills Category and Overall CSI by Age Group (N=188) 106
12. Means and Standard Deviations of Skill Categories and Overall CSI by Gender (N=188) 107
13. Means and Standard Deviations of Malware and PII Skills Categories by Job Function (N=188) 109
14. Means and Standard Deviations of WIS Skills Category and Overall CSI by Job Function (N=188) 109
15. Means and Standard Deviations of Malware and PII Skills Categories by Hours Online (N=188) 111

16. Means and Standard Deviations of WIS Skills Category and Overall CSI by Hours Online (N=188) 111
17. Means and Standard Deviations of Malware and PII Skills Categories by Primary Activity (N=188) 113
18. Means and Standard Deviations of WIS Skills Category and Overall CSI by Primary Activity (N=188) 113
19. Means and Standard Deviations of the Skill Categories and Overall CSI by Education (N=188) 115
20. Means and Standard Deviations of Malware and PII Skills Categories by Experience using Technology (N=188) 116
21. Means and Standard Deviations of WIS Skills Category and Overall CSI by Experience using Technology (N=188) 117

## Chapter 1

### Introduction

#### **Background**

The threats to organizational information systems (IS) due to vulnerabilities and breaches caused by employees continue to cause not only financial losses, but also information losses (Hovav & Gray, 2014; Jensen, Bailey, & Baar, 2014; Peha, 2013). The protection of IS lie in the most vulnerable spot; that vulnerability usually rests in individuals (Mitnick & Simon, 2002). Organizations and individuals rely on the embedded security features of the information technology (IT) products and services (Peha, 2013). Even with sophisticated intrusion detection systems, organizations are still at risk because employees make mistakes due to the convincing nature of social engineering incidents (i.e., phishing attacks, drive-by downloads, etc.). An employee, even with the best intentions, may work in an insecure manner or under stress and cause a threat (PricewaterhouseCoopers (PwC), 2013). This study addressed the need for additional empirical investigation and measures of cybersecurity skills, especially of non-IT professionals (Choi, 2013; Choi, Levy, & Hovav, 2013; Thomson & von Solms, 2005; Torkzadeh & Lee, 2003). The results of this study contribute to the IS body of knowledge by providing researchers and practitioners insight into the cybersecurity skills level of non-IT professionals. Participants asked to respond to a survey were found unwilling to report their actual behaviors related to cybersecurity issues in the workplace (Hu, Xu,

Dinev, & Ling, 2011). However, D'Arcy, Hovav, and Galletta (2009) found scenarios were a nonintrusive and unthreatening method to participants when attempting to collect computer misuse data. Moreover, participants preferred hands-on tasks when in an IS learning environment (Li & Liu, 2011). Thus, this study utilized scenarios with observable hands-on tasks to measure cybersecurity skills. Additionally, the results of this study promise to influence industry practices in mitigating the vulnerabilities and threats associated with cyber-attacks.

The remainder of this draft is organized in the following manner. First, a statement of the specific problem researched is presented. Next, the main dissertation goal and research questions as well as the relevance and significance of the research are discussed. A brief review of literature of related areas of research is presented within each of the relevant areas: malware, personally identifiable information (PII), and work information systems (WIS). Specific barriers and limitations are discussed. Finally, the approach section outlines the specific data analyses used to formulate a users' CSI, as well as a definition of terms.

### **Problem Statement**

The problem that this research addressed is the threats to organizational IS due to vulnerabilities and breaches caused by employees (Hovav & Gray, 2014; Jensen et al., 2014; Peha, 2013). According to Axelrod (2006), cybersecurity is “the prevention of damage to, unauthorized use of, exploitation of, and if needed, the restoration of electronic information and communications systems to ensure confidentiality, integrity, and availability” (p. 1). Skill is defined as “a combination of ability, knowledge, and

experience that enables a person to do something well” (Boyatzis & Kolb, 1991, p. 280). Therefore, cybersecurity skills (i.e., preventing malware, PII theft, WIS breaches) correspond to an individual’s technical knowledge, ability, and experience surrounding the hardware and software required to execute IS security to mitigate cyber-attacks (Choi et al., 2015). Improvements of IT tools (i.e., blacklists, whitelists, security pop-up messages, etc.) do not appear to solve the cybersecurity problem of a user without cybersecurity skills becoming prey to the deceptive nature of social engineering techniques (Algarni, Xu, Chan, & Tian, 2014). The protection of information lies in the most vulnerable spot and that vulnerability usually rests in individuals (Mitnick & Simon, 2002). It appears that a non-IT professional with limited cybersecurity skills presents opportunities for organizational information vulnerabilities and threats.

The importance of cybersecurity skills of non-IT professionals has not minimized over the years. Phish Tank (2009) and the Anti-Phishing Working Group (APWG) (2010) identified threats to frequently targeted markets (auction, financial, payment services, & retail). Five years later, Internet Service Providers (ISPs), classifieds, gaming, government, and social media were added to the list of targeted markets (APWG, 2014). Many approaches from artificial intelligence to security education, training, and awareness (SETA) programs attempt to mitigate the challenge of cyber threats. Phishing detection methods (i.e., blacklists, whitelists, heuristics, domain name server (DNS) analyzers, Classifier System, Lookup System, & hybrids) are usually invisible to the user; the detection occurs prior to the phished communication actually reaching the user (Hajgude & Ragha, 2012). User interfaces have seen updates to include security pop-up messages (Hong, 2012), inhibitive attractors (Bravo-Lillo et al., 2013), and domain-



highlighting (Lin, Greenberg, Trotter, Ma, & Aycock, 2011). Organizations and individuals rely on the embedded security features of the IT products and services sold on the Internet (Peha, 2013). Even with embedded IT security tools working well, the non-IT user may still receive a social engineering message that can hook them into making mistakes due to low cybersecurity skills (Winkler & Dealy, 1995).

In December 2013, Target Corporation announced its point-of-sale (POS) system experienced a data breach that began with a malware attack on a contractor (Yadron, Ziobro, & Devlin, 2014; Ziobro, 2014). Similarly, compromised login credentials of some employees were used by hackers to gain access to eBay's entire user database (Bensinger & Calia, 2014). The U.S. Department of Homeland Security (2012) recognized the great escalation of the nation's cyber threat in recent years. Recommendations were made to develop and advance technical cybersecurity skills as a way to encourage qualified candidates (U.S. Department of Homeland Security, 2012). Those users armed with the skills needed to quickly identify and report possible cyber-espionage occurrences "discovered more breaches than any other internal process or technology" (Verizon Enterprise Solutions, 2014, p. 42). "Yet we ignore the human factor in corporate security at our peril, since it's all too clear that technology alone can't guarantee security" (Kaspersky Lab, 2013, p. 15). Thus, it appears that additional empirical investigation on cybersecurity skills of non-IT professionals is warranted (Choi, 2013; Thomson & von Solms, 2005; Torkzadeh & Lee, 2003).

### **Dissertation Goal**

The main goal of this research study was to design, develop, and empirically test a

set of hands-on tasks set to measure the cybersecurity skills level of non-IT professionals. The need for this work was demonstrated by the work of Choi (2013), Furnell (2007), Whitman (2004), Havelka and Merhout (2009), as well as Rubin and Dierdorff (2009). Furnell (2007) found that individuals were not attuned to observe the visual, technical, and language cues involved with phishing e-mails. Whitman (2004) noted that human error or failures were the highest threat to information security. Furthermore, a user's habituated disregard of a security warning for a Website increases risk to IS security (Vance, Anderson, Kirwan, & Eargle, 2014). Havelka and Merhout (2009), as well as Rubin and Dierdorff (2009) focused on the need to include competencies, skills, knowledge, and abilities in the classroom so students had the tools (experience) necessary for future employment. The maturing of an individual's knowledge and skills develops user competency (Eschenbrenner & Nah, 2014). Choi (2013) recognized the lack of research involving cybersecurity skills, and the need for a better measure to assess cybersecurity skills. Furthermore, Choi (2013) identified self-reported surveys as a limitation of research due to a participant's reluctance to report actual misuse behavior or their inability to properly judge their accurate cybersecurity skill levels. Whereas, Torkzadeh and Lee (2003) cautioned self-reported perceived skills do not always correspond to the individual's actual skills. In the work of Gravill, Compeau, and Marcolin (2006), the use of paper versus computer self-reported evaluative measures varied more in accuracy than self-reported factual information, i.e., years of experience. Xu and Yeh (2012) adjusted for the varying individualities of the assessors that may create biases in the self-assessment process. Thus, this study was aligned to develop a set of scenarios that were used to assess the hands-on cybersecurity skills of non-IT

professionals based on demonstrated skills on cybersecurity tasks.

This work built on prior research by first identifying the difference between skills and competence. Burley, Eisenberg, and Goodman (2014) stated that cybersecurity was not a solitary occupational category and identified that knowledge, skills, and abilities were needed for more than cybersecurity work. According to Toth and Klein (2014), knowledge gathered by users and honed skills in a certain functional area developed competencies. Both Burley et al. (2014), as well as Toth and Klein (2014) appeared to exclude the very important factor of ‘experience’ or assumed it under another defined category. Toth and Klein (2014) excluded an additional factor, ‘ability’ altogether. According to Boyatzis and Kolb (1991), as well as Levy (2005), skill is a combination of knowledge, experience, and abilities that enables users to perform well. Over time, skills are honed and competencies are acquired (Eschenbrenner & Nah, 2014). A user’s computer competence is vital for an organization that relies on its employees to possess skills (i.e., combination of knowledge, experiences, & abilities) to complete technical tasks (Downey & Smith, 2011). More than any other internal process or technology, breaches were discovered by users armed with the skills needed to quickly identify and report possible cyber-espionage occurrences (Verizon Enterprise Solutions, 2014). Of the 16,000 responding to a phishing quiz, McAfee Labs (2014) found 80% had fallen for one out of seven phishing e-mails. Those in accounting, finance, and human resources, “which arguably hold some of the most sensitive corporate data, performed the worst” (McAfee Labs, 2014, p. 4). According to PwC (2013), most security incidents were attributed to everyday insiders like current or former employees. Verizon Communication’s chief security officer stated “it’s important to note that insider threats

are not necessarily a 'bad guy' with bad intentions; it could be a good employee doing righteous work in an insecure manner" (PwC, 2013, p. 8). Moreover, due to the lack of technological backgrounds and skills, non-IT professionals (including managers) reported finding themselves 'left behind' the IT staff (Guzman, Stam, & Stanton, 2008).

Furthermore, even with the best intentions, mistakes of non-IT users (i.e., office assistants, managers, executives), due to poor cybersecurity skills, represent the weakest link in an organization's IS security. Thus, this leads to the importance of a measure to assess the level of cybersecurity skills held by a non-IT professional.

This work secondly built on prior research by developing a measure that assessed the cybersecurity skills of non-IT professionals. Bronsberg (2011), as well as Morcke, Dorman, and Eika (2013) mentioned the importance of demonstrating the high-level of skills experienced in the medical and health profession academic programs. Hands-on skill assessment is a substantial part of the medical academic community (Berendonk, Stalmeijer, & Schuwirth, 2013). The importance of skills and hands-on skills assessment found in the health industry appears applicable to cybersecurity skills as well. Torzadeh and Lee (2003) used self-reported surveys to research the individual's perception of his or her IT skills and cautioned that perceived skills do not always correspond to actual observable skills. In the work of Gravill et al. (2006), users inaccurately assessed their knowledge of a specific software package. Prior literature such as Moskal (2010), Weigel and Hazen (2014), as well as Xu and Yeh (2012), addressed the flaws and consequences of erroneous self-assessment reporting. Thus, this research study established and validated a set of hands-on tasks that measured observable cybersecurity skills of non-IT professionals without the bias of or need for self-assessment.

The validity of observable hands-on tasks builds on the prior research of Katz (1974), Williamson (1975), Swanson (2004), as well as Vassiliou et al. (2014). Hands-on skills were developed by employee experimentation (trial & error) over time (Katz, 1974; Williamson, 1975). Swanson (2004) argued hands-on tasks were crucial for an employee's learning outcomes. Observable hands-on skills testing provided the unbiased evidence of competence required to perform a surgical endoscopy without the high-stakes risk to a patient (Vassiliou et al., 2014). Thus, this study established a measure that provides unbiased observable cybersecurity skills assessment without the high-stakes risk to IT by using expert-validated set of cybersecurity skills and scenario driven tasks.

The five specific goals of this research study were as follows. The first specific goal of this study identified a set of cybersecurity skills pinpointed by subject matter experts (SMEs) as those that can help mitigate critical vulnerabilities, which usually involve the compromise of devices, computers, and/or networks by non-IT professionals within their organizations. The second specific goal of this study developed a set of tasks that were categorized and linked to the SMEs identified set of cybersecurity skills. The third specific goal of this study developed a benchmarking index to hierarchically aggregate the set of SMEs identified cybersecurity skills using observable hands-on tasks. Such aggregated measure is called the Cybersecurity Skills Index (CSI) and integrated the set of measurable cybersecurity skills into a single benchmarking index ranging from zero to 100. According to Fenrich (2005), "hands-on skills can transfer to the real world" (p. 353). Chisholm et al. (2013) utilized a hands-on skills test to assess a group of emergency physicians' ability to work with medical technology equipment. Therefore, the fourth specific goal of this study empirically tested the CSI, which is based on real-

life scenarios, for cybersecurity skills on a group of 188 non-IT professionals. Prior IS research, e.g., Algarni, Xu, and Chan (2015), as well as Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010), found a correlation between demographic factors and victims of cybersecurity threats. Therefore, the last specific goal of this study empirically assessed the contribution of age, education level, gender, job function (e.g., administrative staff, managerial, executive, operations, physical security, information technology, technical services, & other), primary online activity, number of hours accessing the Internet, and experience using technology to the CSI.

### **Research Questions**

The main research question that this study addressed is: What tasks enable the validation of a hierarchical measure for observable cybersecurity skills of non-IT professionals? In addition, this study addressed five specific research questions as follows.

RQ1: What are the specific subject matter experts (SMEs) identified set of cybersecurity skills of non-IT professionals, which address the most common organizational cybersecurity threats?

RQ2: What are the specific SMEs identified tasks that can be categorized, linked, and validated to the set of the identified cybersecurity skills?

RQ3: What are the specific SMEs identified weights of the tasks and skills that enable a validated hierarchical aggregation to the Cybersecurity Skills Index (CSI) benchmarking index?

RQ4: What are the scores of the CSI benchmarking index for the aggregated set of SMEs identified cybersecurity skills of a group of 188 non-IT professionals?

RQ5: Are there any significant differences to CSI based on age, gender, educational level, job function, primary online activity, number of hours accessing the Internet, or experience using technology?

## **Relevance and Significance**

### *Relevance*

The purpose of this study was to seek mitigation of the threats to organizational IS due to vulnerabilities and breaches caused by non-IT professionals. Adversaries focus on gaining access to IS through employees (Kaspersky Lab, 2013). In a benchmark study, Ponemon Institute (2014a) found that human error or malicious attacks (i.e., criminal insiders, malware infections, or phishing/social engineering) were the root cause for 72% of organizational data breaches. There has been a variety of research studies focused on cybersecurity issues relating to embedded security features (Bravo-Lillo et al., 2013; Hong, 2012; Lin et al., 2011). However, a review of literature reveals that few studies have focused on cybersecurity as it relates to non-IT professionals (Choi et al., 2013; Jensen et al., 2014; Peha, 2013). Cybersecurity threats and vulnerabilities are causing substantial financial losses for individuals, organizations, and governments all over the world (Levy, Ramim, Furnell, & Clarke, 2011; Ramim & Levy, 2006). Cyberwar is another major concern that nations around the world are struggling to get ready to fight or maintain strong defense tactics. According to PwC (2013), an employee with the best

intentions working in an insecure manner may cause a threat. As organizations continue to rely on the Internet for conducting their daily operations, understanding an employee's cybersecurity skills levels is critical to securing information and the systems that stores it. Given the documented increase in importance of cybersecurity in everyday activity, the relevance of this study is substantial.

### *Significance*

This research advanced current research in cybersecurity and facilitated an increase in the body of knowledge regarding non-IT professionals as it relates to their cybersecurity skills in the context of malware, PII, and WIS. Prior research noted paper (Gravill et al., 2006) and self-reported (Torkzadeh & Lee, 2003) surveys did not accurately assess actual skills. According to Downey and Smith (2011), a user's computer competence is vital for an organization that relies on its employees to possess skills, (i.e., knowledge, experiences, & abilities) to complete technical tasks. The investigation of a good problem statement has practical significance (Terrell, 2012). Insight into an employee's cybersecurity skills levels can potentially help reduce the opportunities for organizational information vulnerabilities and threats. As seen in literature, organizations have an ongoing need for non-IT cybersecurity skilled professionals. Therefore, this study focused mainly on the non-IT professionals representing corporate organizations. Moreover, given the documented increase in individual, organizational, and governmental cybersecurity incidents, the significance of this study is substantial.

### **Barriers and Issues**



One potential barrier for this study was obtaining permission to measure the cybersecurity skills of non-IT professionals. Institutional Review Board (IRB) approval was needed in order to use non-IT professionals as participants. Approval to conduct the study was obtained prior to pursuing IRB approval.

Using the Delphi technique was a potential barrier. According to Gordon (1994), participant selection, following the Delphi technique, requires a great deal of attention and the researcher must meticulously prepare and test questionnaires to avoid ambiguity. Collecting an adequate number of responses from SMEs throughout the Delphi technique proved challenging as well (Gordon, 1994). In addition, identifying and locating the SMEs added to the challenge of the Delphi technique. Scheele (1975) recommended providing gifts or 'in kind' rewards as a way to encourage participation.

Appropriately implementing the development research within the accepted parameters is a potential barrier. The elements of development research focuses on complex, innovative solutions that have few, if any, accepted design and development principles; a comprehensive grounding in the literature and theory; empirical testing of product's practicality and effectiveness, as well as thorough documentation, analysis, and reflection on processes and outcomes (Ellis & Levy, 2009, p. 328).

With a foundation in literature (i.e., Ellis & Levy, 2010; Hevner & Chatterjee, 2010), this study progressed towards a successful research level design and development effort that incorporated the Delphi technique expert panel.

While developing and validating such a comprehensive set of scenarios-based, hands-on benchmarking index is valuable for organizations, the process of implementing

it in order to actually measure such skills was challenging. In order to overcome this issue, this study developed an iPad application (app) prototype that operationalized the previously developed and validated scenarios-based, hands-on tasks CSI into an actual app that was used to collect the cybersecurity skills data.

## **Limitations and Delimitations**

### *Limitations*

A limitation of this study was related to the expert opinions collected during the Delphi technique. Expert opinions are limited to those members recruited (Ellis & Levy, 2010). Therefore, combining the Delphi technique, review of literature, and a pilot-test mitigated this limitation. Furthermore, the recruitment of experts was not limited to one industry or government type. Thus, mitigating the limitation of bias.

Additionally, measuring the participant's responses to the scenarios-based, hands-on cybersecurity tasks was a limitation. Validity and reliability would be threatened if the MyCyberSkills™ iPad app incorrectly recorded or scored the participants' responses. In order to mitigate this limitation, an iterative development process was followed (Sheng, Magnien, Kumaraguru, Acquisti, & Cranor, 2007). Furthermore, an ongoing review of the data recorded and respective scoring was tested throughout the development process. A comprehensive review was conducted during the pilot-test to ensure the participants' responses were correctly recorded and scored prior to conducting the empirical study. Moreover, internal validity would be threatened if participants chose not to respond truthfully to the cybersecurity tasks presented during the data collection process (Ellis & Levy, 2010). Therefore, the vulnerability for respondents to desire to provide consistent

or socially-acceptable answers was mitigated by presenting four scenario-based, hands-on tasks to measure each respective cybersecurity skills (Verplanken & Orbell, 2003).

Furthermore, a participant completed each of the observable hands-on, scenario-based cybersecurity tasks while in the presence of an IS security expert. Each participant that completed all of the cybersecurity tasks were offered an honorarium (Scheele, 1975).

### *Delimitations*

A delimitation of this study was its limitation to a single mobile technology platform, an iPad app. Furthermore, this study was limited to the Southeastern United States. Participants' responsiveness to the iPad app was seen as a possible delimitation of the study as it may not be the same presented on a different platform and/or at other institutions.

### **Definitions of Terms**

The following represent terms and definitions.

**Cybersecurity Skills Index (CSI)** – The cybersecurity skills index is a logical and repeatable quantitative measure that indicate the level of cybersecurity skills of an individual.

**Cyber-attack** – illegal activities or a crime that takes place on an information system, i.e., theft of software, data, unauthorized access, or modification of information (Libicki, Senty, & Pollak, 2014; Ramim & Levy, 2006).

**Cybersecurity** – “the prevention of damage to, unauthorized use of, exploitation of, and if needed, the restoration of electronic information and communications systems to ensure confidentiality, integrity, and availability” (Axelrod, 2006, p. 1).

**Cybersecurity risk** – describes any disruption of daily operation and monetary loss caused by a malicious cyber event (Mukhopadhyay, Chatterjee, Saha, Mahanti, & Sadhukhan, 2013; National Institute of Standards and Technology (NIST), 2014).

**Cybersecurity skill** – correspond to an individual’s technical knowledge, ability, and experience surrounding the hardware and software required to execute IS security to mitigate cyber-attacks (Choi et al., 2013).

**Information System (IS)** – “A discrete set of information resources [i.e., personnel, equipment, funds, and information technology] organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Also includes specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems” (Kissel, 2013, p. 101).

**Information Technology (IT)** – “Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information” (Kissel, 2013, p. 104).

**Instrument** – “Any means used to measure or otherwise study subjects. In the language of social and behavioral research, an instrument can call to mind a mechanical device (as it does in ordinary language – a dentist’s drill, a saxophone), but it is used more broadly to include written instruments, such as attitude scales or interview schedules” (Vogt & Johnson, 2011, p. 181). “Therefore, indices, scales, and questionnaires are all measurement instruments” (Mendoza, 2014, p. 4).

**Personally identifiable information (PII)** – Any information about an individual that may be used to distinguish or trace an individual’s identity, i.e., name, social security number, date and place of birth, mother’s maiden name, or biometric records, either alone or when combined with other public information that is linkable to a specific individual, i.e., medical, educational, financial, and employment information (Krishnamurthy & Wills, 2009; McCallister, Grance, & Scarfone, 2010).

**Phishing** – A cyber-attack that mimics a legitimate or trusted Website to lure victims to disclose their user ids, passwords, or other personal information; it is being used in conjunction with social engineering attacks (McDowell, 2006; Ramim & Levy, 2006).

**Risk** – “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would rise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (NIST, 2006, p. 8).

**Risk mitigation** – “prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process” (Committee on National Security Systems (CNSS), 2010, p. 62).

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

**Social engineering** – the process of deceiving or influencing individuals to provide personal or corporate information in order to compromise the victim’s information system (computer) for the purpose of benefiting the attacker (Algarni et al., 2014; Mitnick & Simon, 2002; Winkler & Dealy, 1995)

**Vulnerability** – “A weakness in a system that can be exploited to violate the system’s intended behavior relative to safety, security, reliability, availability, and integrity or to obtain access to some asset” (Andrews & Whittaker, 2004, p. 70).

**Work Information System (WIS)** – An information system operating in an organization.

### **Summary**

This study addressed the threats to organizational IS due to vulnerabilities and breaches caused by employees by designing, developing, and empirically testing a hierarchical measure for observable cybersecurity skills of non-IT professionals (Hovav & Gray, 2014; Jensen et al., 2014, Peha, 2013). Non-IT professionals (i.e., office assistants, managers, executives) historically have access to sensitive data and represent 72% to 95% of cybersecurity threats to organizations. However, current measures of cybersecurity skills are based on perceived skills and self-reported surveys that do not always correspond to actual observable skills (Torkzadeh & Lee, 2003; Xu & Yeh, 2012). As seen in the medical and healthcare academic curriculum, assessing observable high-level hands-on skills allow for experience without harm to a system or individual (Chisholm et al., 2013; Fenrich, 2005). Thus, the importance of skills and hands-on assessment appears applicable to cybersecurity skills of non-IT professionals. Therefore, by using expert-validated set of cybersecurity skills and scenario driven tasks, this study established and validated a set of hands-on tasks that measures observable cybersecurity skills of non-IT professionals without bias or the high-stakes risk to IT.

## Chapter 2

### Review of the Literature

#### **Introduction**

In this chapter, a literature review is presented to provide a synopsis of the relevant literature pertaining to skills, data breaches, and cybersecurity as well as to lay the theoretical foundation for this study. The literature review was an important first step and “the theoretical foundation for the empirical study” (Paré, Trudel, Jaana, & Kitsiou, 2015, p. 183). Furthermore, a systematic search of quality peer-reviewed and secondary IS literature substantiates the existence of the research problem, vindicates a new contribution to the existing body of knowledge, and structures the study (Levy & Ellis, 2006; Paré et al., 2015). To ensure breadth, depth, rigor, consistency, clarity, brevity, as well as an effective analysis and synthesis, an extensive search of the IS literature domain was conducted using interdisciplinary fields including aviation, IS, medical, and transportation (Hart, 1998). From this literature review, existing knowledge, research questions, approach, and theoretical foundation for this study of designing, developing, and empirically testing a scenarios-based, hands-on hierarchical cybersecurity skills index were discovered. Moreover, information regarding cybersecurity skills shortage, risk mitigation, and tools are presented. Furthermore, in order to operationalize the CSI into an actual app, the scenarios and hands-on tasks were designed and developed utilizing literature from this review.

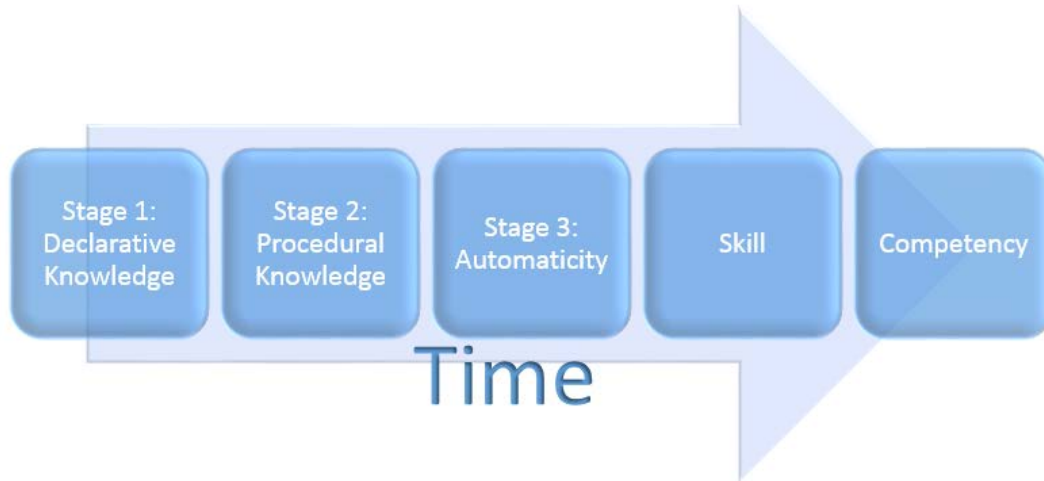
## **Skills and Competencies**

### *Skills Defined*

According to Boyatzis and Kolb (1991) as well as Levy (2005), skill is a combination of knowledge, experience, and abilities that enables users to perform well. The acquisition of a skill is a learning process and generally adopts three incremental stages (Anderson, 1982; Gravill et al., 2006). These stages begin with the initial acquisition of a skill known as declarative knowledge (Stage 1). At this stage, instruction and information about a skill are given to the user (Anderson, 1982; Fitts, 1964). Moreover, Stage 1 allows the user to establish the knowledge needed as a foundation for later learning stages (Gravill et al., 2006). The second stage of skill acquisition (Stage 2) allows the learner to practice declarative knowledge and convert it to procedural knowledge (Fitts, 1964; Neves & Anderson, 1981). Knowledge becomes better organized and users start to connect the actions needed to complete an activity (Gravill et al., 2006). Next, at the third stage, comes automaticity (Fitts, 1964; Marcolin, Compeau, Munro, & Huff, 2000). Users progress beyond the initial acquisition stage into an efficient and autonomous (Stage 3) by increasing their experience level (Anderson, 1982; Gravill et al., 2006; Kraiger, Ford, & Salas, 1993). Experience positively influences a user's computer usage, which helps establish the needed experience of the skill (Gravill et al., 2006). The ability to generalize procedures and increase performance occurs during the acquisition of knowledge phases (Marcolin et al., 2000). Over time, Eschenbrenner and Nah (2014) identified that skills are honed and competencies are acquired. The skill



development stages are shown in Figure 1. Whereas, Table 1 lists a summary of research studies defining skills and the skill development stages.



*Figure 1.* Skill development stages over time

Table 1

*Summary of Skills Defined*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Anderson, 1982	Theoretical		Acquisition of cognitive skill	Skill acquisition is a learning process that has three stages (e.g., declarative, procedural, & automaticity); each require time for honing
Boyatzis & Kolb, 1991	Development and empirical study via video/audio taped sessions	236 adults consisting of students, managers, and an assortment of manufacturing professionals	Personal and organizational skills based on the theory of learning	Developed and validated the learning skills profile, which assesses learning skills through a typology of 12 skill scales

Table 1

*Summary of Skills Defined (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Eschenbrenner & Nah, 2014	Literature review and synthesis		IS user competency, social cognitive theory	Developed a conceptual foundation of IS user competency and proposed an IS user competency framework
Fitts, 1964	Theoretical		Perceptual-motor skill learning	Skill learning is a continuously evolving hierarchical process that with practice over time leads to peak performance (i.e., competency)
Gravill et al., 2006	Empirical study via paper survey and controlled experiment	67 volunteers from four large financial, retail, consulting, and distribution organizations	Self-assessed user competence	End-users did accurately self-assess their software knowledge, but did improve as experience and understanding of IT increased
Kraiger et al., 1993	Theoretical		Cognitive, skills-based, and affective outcomes theories	Identified framework for evaluating learning outcomes using an organized classification scheme
Levy, 2005	Empirical study via longitudinal study	2 MBA programs (one online and one on-campus)	Learning skills profile	Skills were positively enhanced in both the online and on-campus MBA programs

Table 1

*Summary of Skills Defined (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Marcolin et al., 2000	Empirical study via survey and flash-card self-efficacy assessment	66 university administrators and students	End-user competency	End-users ranked higher their perceived ability to use a software package than their demonstrated competence level of the same software package

*Competence vs. Skills*

Bronsborg (2011) as well as Morcke et al. (2013), demonstrated the importance of the high-level of skills experienced in the medical and health profession academic programs. The need to include competencies, skills, knowledge, and abilities in the classroom so students have the tools (experience) necessary for future employment were the focus of the research by Havelka and Merhout (2009), as well as Rubin and Dierdorff (2009). Havelka and Merhout (2009) found that knowledge is obtained through coursework. Whereas, Rubin and Dierdorff (2009) found the courses offered by colleges and universities are relevant to the competency level of a student. It was discovered that the maturing of an individual's knowledge improves skills, which then develops user competency (Eschenbrenner & Nah, 2014). Moreover, it was previously noted in literature that knowledge gathered by users and honed skills in a certain functional area developed competencies (Toth & Klein, 2014). A misalignment between course offerings and required corporate competencies reduces the individual's exposure to important knowledge that is needed to do a task well (Rubin & Dierdorff, 2009). Additionally, it

was noted that a reasonable degree of competency at a skill “requires at least 100 hours of learning and practice” (Anderson, 1982, p. 369). An individual’s competency level of a particular skill is valuable; it may influence or even determine an individual’s level of professional success and satisfaction (Havelka & Merhout, 2009; Levy & Ramim, 2015). Moreover, IT feature use was found to positively influence an increase in an end-user’s skills (Benilian, 2015). A user’s computer competence is vital for an organization that relies on its employees to possess skills, (i.e., knowledge, experiences, & abilities) to complete technical tasks (Downey & Smith, 2011). Thus, it appears competency is acquired after a skill is practiced over time (Levy & Ramim, 2015). A summary of research studies regarding skill, competence, and the development of competence are listed in Table 2.

Table 2

*Summary of Competence vs. Skills*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Bronsborg, 2011	Empirical study via survey	102 medical students at a private non-profit university in the Southeastern U.S.	Learning skills profile to measure IT skill competency	To better prepare a medical student for the workforce, opportunities to learn IT skills are needed
Downey & Smith, 2011	Empirical study via survey	610 midshipmen in the U.S. Navy’s commissioning program	Competence and its relationship with attitudes	Competence and attitudes were improved with skills training

Table 2

*Summary of Competence vs. Skills (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Eschenbrenner & Nah, 2014	Literature review and synthesis		IS user competency, social cognitive theory	Developed a conceptual foundation of IS user competency and proposed an IS user competency framework
Havelka & Merhout, 2009	Theoretical		IT professional competence	Developed a theoretical model of skills (i.e., knowledge, experiences, and abilities) desired for IT specialists
Levy & Ramim, 2015	Empirical study via quasi-experiment	253 business management students	Skills and competence assessment	Students with hands-on experience (i.e., computer simulation) performed better than those without
Morcke et al., 2013	Literature review and analysis		Outcome (competency) based education	Undergraduate medical education programs for nearly 60 years have utilized outcome (competency) based education
Rubin & Dierdorff, 2009	Empirical assessment	373 U.S. colleges and universities	MBA curricula and managerial competencies	Competencies in the classroom were found necessary to prepare students for future employment

Table 2

*Summary of Competence vs. Skills (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Toth & Klein, 2014	Standard		Role-based model for Federal IT/cyber-security training	Specific IT/cybersecurity training for an individual based on job function and responsibilities

### *Information Technology Skills*

One of the main challenges in the study of IT skills is the fact that IT skills have been measured, predominantly in research, based on self-reported survey instruments (Levy, 2005; Torkzadeh & Lee, 2003). Adomßent and Hoffman (2013), as well as Beaudoin, Kurtz, and Eden (2009), identified that competencies are important to accomplish something successfully and responsibly. Lerouge, Newton, and Blanton (2005) defined IT skills as those skills that correspond to the technical knowledge regarding the hardware, software, and programming features of IS. Marakas, Yi, and Johnson (1998) concluded the increase of technology skills across users is important as IT becomes a mainstay in the daily lives of individuals. New technologies are adopted by organizations regularly (Weigel & Hazen, 2014). According to Marcolin et al. (2000), competence with IT not only empowers users, it has an effect on their workplace productivity. In order to effectively use IT for the benefit of the organization, a user needs to acquire skills working with new IS and technologies (Eargle, Taylor, Sawyer, & Gaskin, 2014). IT skills are essential for an organization to gain competitive equality, but the management of those IT skills sustain an organization's competitive advantage (Mata,

Fuerst, & Barney, 1995). Thus, the importance of assessing those skills warrants additional research (Levy & Ramim, 2015; Weigel & Hazen, 2014). Table 3 lists a summary of research studies regarding the importance of IT skills.

Table 3

*Summary of Information Technology Skills*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Adomßent & Hoffman, 2013	Concept paper		Competencies in the context of education for sustainable development	Competency is important to accomplish an educational sustainable development.
Beaudoin et al., 2009	Empirical study via survey	318 online learners from Western, Japanese, Mexican, and Israeli countries	System of knowledge, experience, and abilities	Derived a set of competencies useful for successful online learning
Eargle et al., 2014	Empirical study via self-reporting survey	377 users of Microsoft Excel	Skill acquisition and habituation	A person's skill acquisition through multi-purposing is improved by comprehensiveness of use and atypical use
Lerouge et al., 2005	Empirical study via mailed surveys	124 IS professionals	IS skill set	A systems analyst position requires a multi-faceted skill set, but the skills were not ranked equally in terms of job importance and preferred use

Table 3

*Summary of Information Technology Skills (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Levy, 2005	Empirical study via longitudinal study	2 MBA programs (one online and one on-campus)	Learning skills profile	Skills were positively enhanced in both the online and on-campus MBA programs
Levy & Ramim, 2015	Empirical study via quasi-experiment	253 business management students	Skills and competence assessment	Students with hands-on experience (i.e., computer simulation) performed better than those that did not
Marakas et al., 1998	Literature review and synthesis	40 papers focused on the CSE construct as a developed measure or evaluated as a variable	Computer self-efficacy	Negative impacts associated with personnel introduced to IT may be tempered with increase computer self-efficacy through experience and knowledge
Marcolin et al., 2000	Empirical study via survey and flash-card self-efficacy assessment	66 university administrators and students	End-user competency	End-users ranked higher in their perceived ability to use a software package than their demonstrated competence level of the same software
Mata et al., 1995	Literature review and analysis	5 IT-based sources of competitive advantage	Strategic management theory	Managerial IT skills were a source of sustained competitive edge.



Table 3

*Summary of Information Technology Skills (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Torkzadeh & Lee, 2003	Empirical study via developed instrument	282 end-users from variety of industries and management levels	Perceived end-user computing skills	Identified 12 items for measuring perceived end user computing skills, but cautioned perceptions do not always correspond to actual skills
Weigel & Hazen, 2014	Empirical study	22 IS graduate students employed in an IT position	Technology proficiency assessment	Addressed the flaws and consequences of erroneous self-assessment reporting by presenting technology proficiency assessment constructs

**Data Breaches**

From 2005 to 2012, Privacy Rights Clearinghouse (2014) reported over 607 million records lost from nearly 3,500 data breaches. According to Boritz and No (2011), in the past government agencies were only involved in egregious privacy breaches. One and one-half years later, President Barack Obama signed Executive Order No. 13,681 (2014) requiring “the use of multiple factors of authentication and an effective identity proofing process” (p. 63492) when a U.S. citizen’s personal data is made available through digital applications. Nearly 1.6 billion records were reported lost from 453 data breaches during the period of January 2013 to December 2014 and an additional 454 breaches occurred with an unknown number of lost records (Privacy Rights

Clearinghouse, 2014). According to Identity Theft Resource Center (ITRC) (2015), 25% of the 64 data breaches reported in January 2015 resulted in the exposure of 455,337 individual records. Of the remaining 75%, an unknown number of records were exposed (ITRC, 2015). Industries affected included banking, business, education, medical and healthcare, as well as government and military sectors (ITRC, 2015). During 2015, 1,670 data breaches occurred with nearly 50% reporting an unknown number of compromised data records (Gemalto, 2016). By the end of May 2016, 42% of data breach incidents resulted in 12 million records compromised (ITRC, 2016). In addition, nearly 400 million email addresses and passwords of customers associated with LinkedIn and multiple email providers (i.e., Hotmail, Gmail, Mail.ru, etc.) were found available for sale online (Identity Force, 2016; Scott, 2016).

Prior research identified the need for research to address the threats to organizational IS due to vulnerabilities and breaches caused by employees (Choi et al., 2013; Jensen et al., 2014; Peha, 2013). More than any other internal process or technology, breaches were discovered by users armed with the skills needed to quickly identify and report possible cyber-espionage occurrences (Verizon Enterprise Solutions, 2014). Technology alone cannot guarantee security. A security risk is often accepted by a user when the countermeasure interferes with work productivity (Choi et al., 2013). Therefore, the human factor cannot be ignored in corporate security without peril (Kaspersky Lab, 2013). Most security incidents were attributed to everyday insiders like current or former employees (PwC, 2013). Since 2003, four of the top nine security incident patterns (e.g., miscellaneous errors, crimeware, insider misuse, & physical theft/loss) involved human error or misuse (Verizon Enterprise Solutions, 2015).

According to Symantec Corporation (2015), not all insider threats are intentional; 84% of insider related data breaches reported were due to an unintentional act or failure to secure a computer or drive. Of the 1,670 data breaches reported in 2015, 38% were due to an accidental loss or malicious insider (Gemalto, 2016). Moreover, it was noted that “unfortunately, even the best security mechanisms can be bypassed through social engineering” (Winkler & Dealy, 1995, p. 1), which “is now considered the great security threat to people and organizations” (Algarni et al., 2014, p. 1). Even amid those who classified themselves as being aware of social engineering techniques, Kvedar, Nettis, and Fulton (2010)’s findings suggested an implemented social engineering plot could succeed. A user with technology knowledge does not automatically become skilled in cybersecurity (Choi et al., 2013). In the work of Qin and Burgoon (2007), users had an 18% accuracy in detecting deception. According to Enterprise Risk Management (ERM) (2014), not protecting an organization’s information puts “the reputation, success, and survival of the organization at risk” (p. 2). An example of this occurred in November 2014 when Sony Pictures suffered a data breach that shut down all e-mail communications and computer usage due to a hacker posting a threatening message on company owned computers and obtaining unsecured data files (Privacy Rights Clearinghouse, 2014). Another data breach reported by Anthem identified hackers compromised work information system credentials of a system administrator, possibly through email phishing (Mathews & Yadron, 2015). Moreover, malware, use of stolen credentials, and phishing were identified as the top three cyber threats by Verizon Enterprise Solutions (2016). However, the skills needed to mitigate such cybersecurity threats and to protect corporate IT systems from such data breach attacks can be the

difference between experiencing a breach or not. It appears no one is immune from a cyber-attack (Verizon Enterprise Solutions, 2016). Thus, the importance of a measure to assess the level of cybersecurity skills held by a non-IT professional is significant. Table 4 lists a summary of research studies regarding data breaches.

Table 4

*Summary of Data Breaches*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Algarni et al., 2014	Empirical study via qualitative survey	78 social networking site (SNS) account holders	Social engineering	Social engineering is a threat to SNS account holders
Boritz & No, 2011	Literature review and synthesis		Framework to identify key stakeholders and their interactions to structure e-commerce privacy settings	Previous studies on privacy settings in e-commerce have relied on opinions not actual behaviors and privacy of accumulated PII is an important growing issue
Choi et al., 2013	Empirical study via expert reviewed survey	185 respondents from a large government transportation agency	Cybersecurity threats and vulnerabilities	End user awareness of monitoring and cybersecurity initiative skill reduced misuse intentions
Jensen et al., 2014	Empirical study via laboratory experiment	111 subjects	Effect of color on key business information retention	The use of color to highlight critical information (i.e., corporate security policies) does increase the end-user's retention of that information

Table 4

*Summary of Data Breaches (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Kvedar et al., 2010	Empirical study via vulnerability assessment simulation	Graduate, undergraduate, and high school students attending simulation	Social engineering	Over 40% did not perceive social engineering as a threat and 85% gave the attackers network information
Qin & Burgoon, 2007	Experimental study via interviews	122 community members and undergraduate students	Social engineering in a deception related setting	Human judgment on deception is biased and inaccurate
Winkler & Dealy, 1995	Case study	Compilation of large financial institutions	Social engineering	Social engineering attacks were successful due to low cybersecurity skills

*Social Engineering*

Social engineering tends to be widely employed and very effective due to human nature's frailties and lack of awareness of such dangers at various levels (Siponen, 2001). Social engineering is a method used by a hacker to navigate around technical security controls (Jenkins, 2013). A successful social engineering attack is defined as an art of manipulation, deception, or intrusion (Mitnick & Simon, 2002, 2005; Podhradsky, D'Ovidio, Engebretson, & Casey, 2013). Every organization has at least one individual susceptible to a social engineering attack (Mouton, Leenen, Malan, & Venter, 2014). An attack may be as easy as asking for the sensitive information and newer technologies are making it even easier (Podhradsky et al., 2013). The number of individuals that can be

targets of a social engineering attack increases as electronic computing devices prevail (Mouton et al., 2014). Moreover, social engineering threats are increasing due to new trends (e.g., Bring Your Own Device) and the use of mobile devices accessing WIS in insecure environments (i.e., cafés) (Krombholz, Hobel, Huber, & Weippl, 2015). Thus, examples of social engineering disconfirm the belief that technical security controls completely secure a system and the user must not be security conscious (Jenkins, 2013).

Vulnerabilities must be identified, assessed, and prioritized by IT management and individuals (Algarni et al., 2014; Goodman & Lin, 2007). Social engineering scams do not discriminate against an individual's age, gender, or education level (Algarni et al., 2015; Podhradsky et al., 2013). An individual's knowledge and ability to identify a social engineering attack lowers a corporation's access vulnerability (Goodman & Lin, 2007). However, most individuals in an organization have a willingness to be helpful and that creates opportunities for a successful social engineering attack (Goodman & Lin, 2007). Many social engineering techniques (e.g., phishing, identity theft, spamming, etc.) exist and are used to compromise IT, while attacking individuals or organizations (Algarni et al., 2014). Furthermore, susceptibility to fall victim to a social engineering attack was found higher for women and young adults (Algarni et al., 2015). Moreover, all education levels of non-IT professionals were found susceptible to social engineering victimization (Algarni et al., 2015). Successful social engineering attacks often involve human emotions of trust, fear of getting disciplined, compliance, and personal gain (Mitnick & Simon, 2002; Podhradsky et al., 2013). Thus, this study addressed the development of a social engineering countermeasure that does not extinguish the individual's tendency to help (Goodman & Lin, 2007). Moreover, this study identified the cybersecurity skills

level of an individual without harm to any existing IT. Table 5 lists a summary of research studies regarding social engineering and the range of social engineering threats.

Table 5

*Summary of Social Engineering*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Jenkins, 2013	Empirical study via experiments	2108 participants from three studies	Insider threats	Demonstrated the importance understanding the risks of weak security behavior
Podhradsky et al., 2013	Empirical study via Xbox 360 Elite	3 user profiles on 1 Xbox 360 Elite	Social engineering, PII disclosure in virtual societies	PII was exposed even though user profiles were deleted.
Siponen, 2001	Theoretical		Information security awareness	Dimensions of information security awareness and the respective target groups were identified

*Malware*

According to International Business Machines (IBM) Global Technology Services (2014), ‘human error’ was identified as a contributing factor in over 95% of all security incidents investigated. Furthermore, an infected attachment or selecting an unsafe Uniform Resource Locator (URL) was the most prevalent contributing ‘human error’ when it comes to inflicting malware on computing systems (IBM Global Technology Services, 2014). Reported cases of malware attacks were not limited to one particular operating system (i.e., Windows, Mac, iOS, Android) (Chin, Felt, Sekar, & Wagner,

2012) or type of device (i.e., Automatic Teller Machine (ATM), computer, Point-of-Sale (POS) terminal, smartphone) (Choo, 2011). Chen, Gu, Zhuge, Nazario, and Han (2011) identified Web-based malicious software (malware) as an exploiter of client-side vulnerabilities, pervasive, and hard to block. Malware may also arrive via an e-mail attachment, which can lead to damaged computers, stolen personal information, and mount attacks on computers (Comesongsri, 2010). Provos, Rajab, and Mavrommatis (2009) discussed how an adversary sends a spam e-mail to a user, which then directs the user to a Webpage with malicious content. Malware infections occur mostly due to users lured to complete an action that leads to infecting their computer (Lévesque, Nsiempba, Fernandez, Chiasson, & Somayaji, 2013). A survey of 400 business executives and technology professionals identified that malware and hacking were top concerns within their organizations (CompTIA, 2015). Moreover, in the third quarter of 2014, an estimated 20 million new strands of malware were created (CompTIA, 2015). However, in the work of Harris, Furnell, and Patten (2014), approximately 6% of the non-IT participants surveyed were concerned with malware infections appearing on their mobile devices. This is alarming since both IT and non-IT participants failed to protect their mobile devices with anti-virus or firewall software (Harris et al., 2014). Min, Varadharajan, Tupakula, and Hitchens (2014) recommended at least one anti-virus software installation per device. However, Lévesque et al. (2013) found that 20% of the participants were infected with some type of malicious software that went undetected by the installed anti-virus software. Moreover, cyber criminals are focusing malicious software to attack mobile devices, which then weakens the corporate perimeter-based defenses as mobile devices are brought in and out of the work environment (He, 2013).



Malware delivery occurs in the form of an email attachment that included various file formats (Bere, Bhunu-Shava, Gamundani, & Nhamu, 2015). The flexibility for an end user to check email via a mobile device increases the risk of malware exposure. Thus, it appears that users with skills to prevent malware via e-mail or Webpages would reduce the number of infections. However, a tool to measure such skills does not appear to be reported in literature, especially of non-IT professionals. A summary of malware and the vastness of the threats associated with malware is shown in Table 6.

Table 6

*Summary of Malware*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Chen et al., 2011	Empirical study via prototype system	26,498 malicious scenarios from 1,248 distinct sites	Malware	Developed and tested a prototype that allows review of malware trails
Chin et al., 2012	Empirical study via structured interview and survey	60 mobile device owners	Privacy and security	Smartphone owners were hesitant to complete sensitive tasks on their phones
Comesongsri, 2010	Empirical study via pen and paper survey	376 college students	Theory of planned behavior, protection model theory, and discord	Phishing protection intention
He, 2013	Literature and blog mining review	327 mobile social media security blogs	Mobile social media risks and mitigation	Mitigation techniques are needed to thwart cyber-attacks and threats via mobile social media

Table 6

*Summary of Malware (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
IBM, 2014	Empirical study via cyber-attack event data	Nearly 1,000 clients in 133 countries	Data breaches	Human error contributed to over 95% of the security events
Lévesque et al., 2013	Empirical study via real-world computer usage and diagnostics	50 participants recruited on a university campus	Malware and anti-virus detection	Anti-virus software does not detect all infections or threats to an IS
Min et al., 2014	Empirical study via vulnerability testing	10 antivirus software programs	Malware detection	After an antivirus update, a malware infection could occur due to a design vulnerability

*Personally Identifiable Information*

PII is defined as information that 1) distinguishes or traces an individual's identity, e.g., social security number, biometric records, date and place of birth, and 2) any data or information associated with an individual, including but not limited to medical, educational, financial, and employment (Krishnamurthy & Wills, 2009; U.S. Government Accountability Office (GAO), 2008). An exploitation of PII may occur with a user merely opening a file. Thus, organizations should be aware and isolate all PII available within their environment, including contractor sites and backup tapes (McCallister et al., 2010). Individuals participating online via social media are vulnerable to having their PII leaked to third parties (Krishnamurthy & Wills, 2009). Furthermore, the leaked PII may be collected and linked to other personal information, which may

result in PII theft (Malin, 2005; McCallister et al., 2010). Mitigation for protecting PII theft is heightened when corporations, e.g., Anthem, Target, Home Depot, etc., experience a data breach. Anthem experienced such a data breach in February 2015 and announced that names, social security numbers, birthdates, and addresses were stolen (Mathews & Yadron, 2015). South Koreans with higher education degrees were thought to fall victim to identity theft more often than those without degrees due to work related duties that involved online activities (Paek & Nalla, 2015). Identity theft was the cause of more than half (53.2%) of the 888 data breaches that occurred globally in the first half of 2015 (Gemalto, 2015). Furthermore, the United States reported the highest number of incidents; a total of 671 data breaches (Gemalto, 2015). An example of this occurred in June 2015 when the Office of Personnel Management announced that PII of 21 million applicants and 1.1 million non-applicants (e.g., spouses and co-habitants) were part of two separate data breaches (U.S. Office of Personnel Management, 2015). This is alarming when prior research has found that as few as three pieces of personal information (date of birth, gender, & zip code) uniquely identify 87% of the United States population (Malin, 2005).

In a study of Facebook profiles, over time individuals shared less PII publicly and more privately to ‘friends’ (Stutzman, Gross, & Acquisti, 2012). In doing so, Facebook users shared more PII, sometimes unknowingly, to silent listeners (e.g., third party apps, advertisers) on the network (Malin, 2005; Stutzman et al., 2012). PII disclosure or theft may also occur from a trail of PII breadcrumbs collected from Web browsing and later reconstructed (Airoldi, Bai, & Malin, 2011). Even with the best security mechanisms, social engineering is a great security threat to PII (Algarni et al., 2014; Winkler & Dealy,

1995). A user with poor information sharing habits and practices increases risk of PII exposure (Ball, Ramim, & Levy, 2015). According to Heartfield and Loukas (2013), 90% of participants were deceived into executing malware that used their computer for collecting personal information. Thus, a measure to determine the participant's skill level of detecting malware will assist in reducing not only an individual's, but a corporation's, vulnerability to PII theft via malware. Table 7 lists a summary of research studies regarding PII.

Table 7

*Summary of Personally Identifiable Information*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Airoldi et al., 2011	Empirical observations and controlled simulated study	1226 patients from 231 hospitals, 144 individuals from 86 households, 1000 subjects for simulations	Entropy metric for assessing disclosure risk of distributed databases	Risk of trail disclosure and PII re-identification is driven by the quantity of PII distributed across databases.
Algarni et al., 2014	Empirical study via qualitative survey	78 social networking site (SNS) account holders	Social engineering	Social engineering is a threat to SNS account holders due to SNSs lack of mitigation techniques
Ball et al., 2015	Empirical study via quantitative survey	390 students and faculty members	Personal information sharing awareness, habits, and practices	Habits significantly influence practices, which may expose PII through social media and e-learning systems

Table 7

*Summary of Personally Identifiable Information (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Heartfield & Loukas, 2013	Empirical study via experimental evaluation	20 technically trained university students	Phishing and file masquerading	Technical end-to-end security solutions in the cloud do not take the human element into consideration
Krishnamurthy & Wills, 2009	Empirical study via online social networks	12 online social networks	PII	Online social networks directly and indirectly released PII to third parties
Malin, 2005	Empirical study via URL access data	86 households and 144 individuals accessing 66,000 distinct Web pages	Re-identification	Data trails from multiple Website visits, re-identification was possible and revealed relationships between PII and unidentifiable data
Paek & Nalla, 2015	Empirical study	10,671 South Korean individuals aged 14 and older	Korea Crime Victim Survey (KVCS) 2008	Education level was positively correlated to identity theft victimizations
Stutzman et al., 2012	Empirical study via longitudinal panel	5,076 Facebook users	Social network privacy and disclosure	Although personal data shared publicly reduced, the quantity and score of personal data revealed privately increased

Table 7

*Summary of Personally Identifiable Information (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Winkler & Dealy, 1995	Case study	Compilation of large financial institutions	Social engineering	Social engineering attacks were successful due to low cybersecurity skills

*Phishing*

The term phishing was created by hackers describing the activity of stealing AOL account information in 1995 (James, 2005; Ryan, 1997). A typical phishing attack occurs when a victim receives a fraudulent e-mail disguised as a genuine e-mail asking the recipient to confirm pieces of personal information by clicking on a hyperlink. The hyperlink leads to the spoofed Website with matching images and logos that appears as genuine as the legitimate site. A successful phisher may steal valuable financial information, such as a social security number, bank account details, and credit card numbers (Huang, Ma, & Chen, 2011) by harvesting the information from the spoofed site and illegally using it (Davinson & Sillence, 2010).

With detection occurring prior to the phished communication actually reaching the user, phishing detection methods (i.e., blacklists, whitelists, heuristics, DNS analyzers, Classifier System, Lookup System, or hybrids) are usually invisible to the user (Hajgude & Ragha, 2012). Furnell (2007) found that individuals were not attuned to observe the visual, technical, and language cues involved with phishing e-mails. According to Paek and Nalla (2015), each additional phishing attempt increased the odds of identity theft victimization by 2 percent. APWG (2010) and Phish Tank (2009)

identified threats to frequently targeted markets (auction, financial, payment services, & retail). APWG (2014) reported the same targeted markets plus the addition of ISPs, classifieds, gaming, government, and social media. Many approaches from artificial intelligence to SETA programs attempt to mitigate the challenge of cyber threats.

Phishing may be compared to purse snatching. The threat of purse snatching has existed for as long as purses have existed, and yet, it occurs every day (Weber, 2012). Numerous attempts to solve the phishing threat exist and despite those efforts the user continues to fall victim to attacks. Thus, users with the skill to identify phishing attempts would reduce the loss of PII along with confidential corporate information. A summary of research studies regarding phishing and end user vulnerabilities are listed in Table 8.

Table 8

*Summary of Phishing*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Davinson & Sillence, 2010	Empirical study via experimental groups	64 staff and students	Health belief model	Providing information about the risk involved improved security behavior
Furnell, 2007	Empirical study	415 Internet users	Phishing	End users cannot rely solely on technical, visual, and language cues of phishing messages
Hajgude & Raha, 2012	Literature review and synthesis		Phishing detection	Proposed a phishing detection algorithm that combined blacklist, white list, and heuristic analysis

Table 8

*Summary of Phishing (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Huang et al., 2011	Conceptual paper		Phishing mitigation and one-time passwords	Proposed authentication system to reduce phished login credentials
Paek & Nalla, 2015	Empirical study	10,671 South Korean individuals aged 14 and older	Korea Crime Victim Survey (KVCS) 2008	Identity theft victimization was correlated to number of phishing attempts received

*Social Media*

Social media networks have four essential features: “1) a digital profile, 2) search and privacy, 3) relational ties, and 4) network transparency” (Kane, Alavi, Labianca, & Borgatti, 2014, p. 284). Because users of e-mail or electronic discussion boards do not establish a profile, nor is searching or viewing a list of connections allowed by others, Kane et al. (2014)’s definition does not include e-mail or electronic discussion boards. Although social media networks provide many benefits, users suffer harm when their personal information is lost, stolen, or wrongly accessed (Romanosky, Hoffman, & Acquisti, 2013). According to Chhabra, Aggarwal, Benevenuto, and Kumaraguru (2011), the accessibility to a large group of gullible users on an open platform attracted adversaries to lure victims with shortened URLs within social media networks (i.e., Orkut, Habbo, & Facebook). Geographically, the USA was found among the targeted countries, while Facebook, Orkut, and Twitter combined accounted for two-thirds of phishing URLs from social media networks (Chhabra et al., 2011). A threat to social



media network users may be a vulnerable friend or other community attributes (Gundecha, Barbier, & Liu, 2011). Furthermore, Gundecha et al. (2011) identified that a user's privacy was impacted by each new friend. Users were either not cautious or not aware of their friends' security and privacy concerns (Gundecha et al., 2011). Protection for/from social media networks (i.e., Facebook & Twitter) was identified as an organization's IT security weak spot by 763 IT security decision makers and practitioners representing 11 countries in North America and Europe (Cyberedge Group, 2014). Moreover, social engineering victimization may be predicted by a non-IT professional's age, gender, security knowledge, and elapsed time in joining Facebook (Algarni et al., 2015). Without social engineering skills (i.e., knowledge, experience, & abilities), 62.5% were victimized by a social engineering attack (Bullée, Montoya, Pieters, Junger, & Hartel, 2015). Thus, it appears skill in protecting PII via social media networks would assist in not only strengthening an individual's identity, but also an organization's IT security. A summary of research studies regarding social media and how it was introduced follows in Table 9.

Table 9

*Summary of Social Media*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Algarni et al., 2015	Empirical study	7,540 Facebook profile observations	Social engineering	Susceptibility to cybersecurity threat victimization predicted by demographics

Table 9

*Summary of Social Media (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Bullée et al., 2015	Empirical study	118 University building occupants	Social engineering training	Social engineering knowledge, experience, and abilities reduced the number of victims
Chhabra et al., 2011	Empirical study via social media	6,474 shortened URLs directed to phished sites	PII theft via social media and shortened URL services	Phishers presented shortened URLs on social media to lure victims
Cyberedge Group, 2014	Empirical study via Web-based survey	763 IT security decision makers and practitioners	Cyber threats	Potential insider threats and having the necessary tools to investigate security breaches were a higher concern than any external threat source
Gundecha et al., 2011	Empirical study via Facebook profiles	100,000 Facebook users	Social media networks	Introduced an approach to vulnerabilities that exist due to a friend's security settings on social media site
Kane et al., 2014	Theoretical		Social media networks	Identified a framework for evaluating and discussing the use of social media in empirical research

Table 9

*Summary of Social Media (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Romanosky et al., 2013	Empirical analysis	1,772 U.S. data breach observations	Data breach litigation and settlement	Lawsuits involving PII theft were settled more often than litigated

*Work Information Systems Security*

Information systems are expected by society to “do what is required and expected of them despite environmental disruption, human user and operator errors, and attacks by hostile parties” (Goodman & Lin, 2007, p. 1). To address these expectations, user interfaces have seen updates to include security pop-up windows (Hong, 2012), inhibitive attractors (Bravo-Lillo et al., 2013), and domain-highlighting (Lin et al., 2011). Current or prior employees present the greatest security threat to WIS as accidental harm or exposure to external threats may occur due to lack of cybersecurity skills (Jacob & Antony, 2014). Organizations and individuals rely on the embedded security features of the IT products and services sold on the open market (Peha, 2013). The use of mobile devices has increased exploits in the workplace by 52% (PwC, 2016). Whitman (2004) noted that human error or failures were the highest threat to information security. Even with the best security mechanisms, a well-planned and executed social engineering attack could succeed (Kvedar et al., 2010; Winkler & Dealy, 1995). Information security incidents globally increased 38% in 2015 (PwC, 2016). Without a cybersecurity skilled workforce to combat cyber-attacks, a work information system’s vulnerability increases as the aggressive cybercriminals continue to escalate the frequency, severity, and impact

of cyber-attacks (PwC, 2016). Table 10 lists a summary of research studies regarding work information systems security and threat mitigation methods.

Table 10

*Summary of Work Information Systems Security*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Bravo-Lillo et al., 2013	Empirical study via online hands-on tasks	A total of 3,722 Amazon's Mechanical Turk workers over three experiments	Security warning dialogue design	Inhibitive attractors reduced the threat of end users installing illegitimate software, granting dangerously excessive permissions to PII online, and habitual ignoring of a familiar security warning
Goodman & Lin, 2007	Literature review and synthesis		Cybersecurity research	Cybersecurity threats, vulnerabilities, and future research opportunities in the U.S.
Hong, 2012	Literature review		Phishing	History of phishing attacks and identified the importance of including the human element in researching solutions

Table 10

*Summary of Work Information Systems Security (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Kvedar et al., 2010	Empirical study via vulnerability assessment simulation	Graduate, undergraduate, and high school students attending simulation	Social engineering	At a network vulnerability focused event, over 40% did not perceive social engineering as a threat and 85% gave the attackers network information
Lin et al., 2011	Empirical study via controlled experiment	22 university students and staff	Domain-highlighting, phishing mitigation	Phishing mitigation tools were not used at all times by end-users
Whitman, 2004	Empirical study via online survey	192 top computing executives	IS security threats	Human error was among the dominant costs of unintentional IS security threats
Winkler & Dealy, 1995	Case study	Compilation of large financial institutions	Social engineering	Social engineering was successful due to low cybersecurity skills

*Confidential Information Exposure*

One successful deployment of a social engineering technique is all it takes to compromise corporate information (McAfee Labs, 2014). The departments holding the most sensitive data were the least successful at detecting legitimate or illegitimate e-mail messages (McAfee Labs, 2014). In the work of Qin and Burgoon (2007), users detected deception with an 18% accuracy rate. Even among those who classified themselves as being aware of social engineering techniques, Kvedar et al. (2010)'s findings suggested

that an implemented social engineering plot could succeed. Social engineering can bypass even the best security mechanisms (Winkler & Dealy, 1995). The exposure of confidential information through social engineering is a great security threat to people and organizations (Algarni et al., 2014).

Social engineering is not the only threat to the exposure of confidential information. Confidential information disclosure may occur by an employee conducting unsecure activities, while at work or at home. One such example involves an investment specialist at Morgan Stanley that admitted to illegally downloading confidential information of about 350,000 clients; the details of how that information was uploaded to an open file sharing site is unknown (Baer, 2015). According to the Federal Bureau of Investigation (FBI)'s investigation of the Central Intelligence Agency (CIA)'s director, General David Petraeus, an employee in a classified position was performing unsecure Internet activities which heightened national security concerns (Barrett, Perez, & Gorman, 2012). The U.S. Department of State and the Broadcasting Board of Governors' Office of Inspector General (OIG) (2012) reported the Ambassador of Kenya ordered a commercial Internet connection be installed in the bathroom of his embassy office in lieu of the secure Internet connection provided by the Department of State. Furthermore, the Ambassador demanded the information management staff use a commercial email system in lieu of the department email system (U.S. Department of State & the Broadcasting Board of Governors, 2012). Former Secretary of State, Hillary Clinton's cybersecurity skill level was questioned while she explained the convenience of using a personal email address to conduct official government operations instead of a government issued email address (Clinton, 2015). Furthermore, an individual volunteering information on a social

networking Website (e.g., Facebook or MySpace) creates a social engineering vulnerability not only to the individual, but to their workplace and co-workers (Mills, 2009). Each of these incidents were a breeding ground for potential confidential information exposure (Kozak, Iefremova, Szkola, & Sas, 2014; Spirin, 2014). Thus, it appears a measure to evaluate the user's skill level at protecting confidential information will help to mitigate exposure and strengthen IT security. Moreover, reports of such a measure appears absent in literature, especially of non-IT professionals. Table 11 lists a summary of research studies regarding confidential information exposure.

Table 11

*Summary of Confidential Information Exposure*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Algarni et al., 2014	Empirical study via qualitative survey	78 social networking site (SNS) account holders	Social engineering	Social engineering is a threat to SNS account holders due to SNSs lack of mitigation techniques
Kozak et al., 2014	Empirical study	26,937 email addresses from 2,000 published articles	Sharing of email addresses	Use of institutional email address may link an end-user to other PII, but the effect of using a non-institutional email account for scholarly communications is unknown

Table 11

*Summary of Confidential Information Exposure (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Kvedar et al., 2010	Empirical study via vulnerability assessment simulation	Graduate, undergraduate, and high school students attending simulation	Social engineering	At a network vulnerability focused event, over 40% did not perceive social engineering as a threat and 85% gave the attackers network information
Qin & Burgoon, 2007	Experimental study via interviews	122 community members and undergraduate students	Social engineering in a deception related setting	Human judgment on deception is biased and inaccurate
Winkler & Dealy, 1995	Case study	Compilation of large financial institutions	Social engineering	Social engineering attacks were successful due to low cybersecurity skills

*Password Exploitations*

Since the 1960s, a common method of authentication is text-based passwords (Wilkes, 1968). In an evaluation of the Multics system, passwords were singled out as a weak point (Saltzer, 1974). Of the 621 confirmed data breaches and thousands of security incidents reported in 2013, 76% were due to weak or stolen credentials (Verizon Enterprise Solutions, 2013). According to Gaw and Felten (2006), a new password was not created for each new account; password reuse was increasing. In addition, online password management tools and accounts were found to contribute to poor password practices (Gaw & Felten, 2006). The creation of a digital identity ecosystem became a



national security priority for the U.S. Government in 2011 due to users accumulating online identities and having difficulty in managing their respective credentials (Bauer, Bravo-Lillo, Fragkaki, & Melicher, 2013). Moreover, the threat of a password exploitation was found with 61% of the IT and non-IT students surveyed as they allowed applications to store their authentication credentials (Harris et al., 2014). Furthermore, password exploitation threat was heightened with authentication credentials absent on nearly 72% of IT and non-IT student-owned smartphones, tablets, and laptops/PCs (Harris et al., 2014).

Ives, Walsh, and Schneider (2004) identified when users frequently re-use passwords, “a domino effect can result as one site’s password file falls prey to a hacker who then uses it to infiltrate other systems, potentially revealing additional password files that could lead to the failure of other systems” (p. 76). An end-user’s disregard of instructions to create a unique password for a Website increases the risk of password exploitations (Grimes, Marquardson, & Nunamaker, 2014). In October 2014, Dropbox clarified that a hacker attack may have stolen login credentials from other sites and attempted to use them to access Dropbox accounts (MacMillan & Yadron, 2014). Even though reusing login credentials makes it easier to remember account details, it places individuals and organizations at a greater security risk (MacMillan & Yadron, 2014). Verizon Enterprise Solutions (2014) reported a stolen password from a POS vendor was the same for each organization managed by the vendor. Armed with information of the vendor’s customer base, the attacker was then able to use the stolen password for gaining access and installing malicious code to capture transmitted data (Verizon Enterprise Solution, 2014). In October 2014, J. P. Morgan Chase & Company disclosed in a

regulatory filing that data related to 76 million households and 7 million small businesses were compromised (J. P. Morgan Chase & Company, 2014). It is suspected an employee's personal computer infected with malware was the culprit that allowed intruders access to J. P. Morgan Chase & Company's network via the employee's virtual private network password (Glazer & Yadron, 2014). Of the financial malware gang incidents reported, 24% were due to the Dyre Wolf harvesting employee and customer credentials for access to "business banking, corporate banking, treasury management, and high-value accounts" (Kessem, 2016, p. 12). Thus, it appears skill in password usage would assist in protecting an organization's information and enhance IT security. Table 12 lists a summary of research studies regarding password exploitations. Table 12 lists a summary of research studies regarding password exploitations.

Table 12

*Summary of Password Exploitations*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Bauer et al., 2013	Empirical study via survey	424 Amazon Mechanical Turk participants in three separate Human Intelligence Tasks	PII and single sign-on	Consent dialogs were ineffective as participants were unable to identify the PII data types passed to service providers
Gaw & Felten, 2006	Empirical study via laboratory exercise and online survey	58 completed online survey, 49 completed laboratory exercise	Management strategies of passwords for online accounts	Poor password practices were identified as a result of the nature of online accounts and password management tool

Table 12

*Summary of Password Exploitations (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Harris et al., 2014	Empirical study via two surveys	227 IT and non-IT college students	Security of mobile devices	Lack of use and improper storing of authentication credentials heightened the risk of password exploitations
Ives et al., 2004	Literature review and synthesis		Password reuse	End-users reuse of passwords is a security threat and increases the vulnerability of each IS accessed with the same password
Saltzer, 1974	Case study		Multics system	Protected information was at risk of exposure due to nine identified design flaws

**Cybersecurity**

Cybersecurity is “the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation” (National Initiative for Cybersecurity Careers and Studies (NICCS), 2014, Cybersecurity section, para. 1). Cybersecurity also includes the restoration of digital information and communications (Axelrod, 2006, p. 1). The International Organization

for Standardization (ISO) / International Electrotechnical Commission (IEC) established ISO/IEC 27002 (2013) as the code of practice for organizations to apply information security controls. These information security controls include that employee education is conducted on a regular basis to ensure the appropriate information security skills and qualifications are maintained (ISO/IEC, 2013; Spruit & Röling, 2014). An end-user without the skill to use a cybersecurity tool or an unusable cybersecurity tool translates into a potential information security breach (Nurse, Creese, Goldsmith, & Lamberts, 2011). Therefore, including the human and social aspects in the cybersecurity system development processes encourages cybersecurity tool usage (Nurse et al., 2011).

The protection of information remains in the most vulnerable spot (Mitnick & Simon, 2002). Humans, despite their intellect, are the most severe threat to an individual's security (Mitnick & Simon, 2002). Information is valuable and knowledge protects information from progressively sophisticated cybersecurity threats (ERM, 2014). Therefore, cybersecurity skills correspond to an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS security (Choi et al., 2013). Limited cybersecurity skills contribute to the behavior of users that causes human errors, often times unintentional (Choi, 2013). Furthermore, the need for users to demonstrate cybersecurity skills is not limited to a single occupation or profession (Burley et al., 2014). Likewise, a technology savvy user does not automatically make a cybersecurity savvy user (Choi et al., 2013). Thus, it appears that a non-IT professional with limited cybersecurity skills presents opportunities for organizational information vulnerabilities and threats (Thomson & von Solms, 2005). Table 13 lists a summary of research studies regarding cybersecurity.

Table 13

*Summary of Cybersecurity*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Axelrod, 2006	Literature review and synthesis		Cybersecurity and critical infrastructure	Defines cybersecurity and provides recommendations for protecting the critical infrastructure
Burley et al., 2014	Literature review and synthesis		Cybersecurity professionalism	All employees, IT and non-IT, need cybersecurity skills
Choi, 2013	Empirical study via Web-based survey	185 working professionals at a U.S. government agency	Cybersecurity threats and vulnerabilities	Cybersecurity skills reduce an end user's computer misuse intention
Choi et al., 2013	Empirical study via expert reviewed survey	185 respondents from a large government transportation agency in a Northeastern U.S. metropolitan	Cybersecurity threats and vulnerabilities	End user awareness of policies increased cybersecurity action skills
Nurse et al., 2011	Literature review and synthesis		Cybersecurity usability and human-computer interaction and security	Guidelines for extending ISO/IEC 27002 into measuring the usability of a cybersecurity tool
Spruit & Röling, 2014	Development research		Information Security Focus Area Maturity Model (ISFAM)	ISFAM enables an organization to set up and measure its current information security maturity

### *Cybersecurity Skills Shortage*

A strong security posture cannot exist without a team of security professionals to combat the organization's "complex and serious internal and external threats" (Ponemon Institute, 2014b, p. 2). And yet, Ponemon Institute (2014b) found the IT security function understaffed at 70% of organizations surveyed. People that want to use their cybersecurity skills for good and not evil are difficult to locate (Rastello & Smialek, 2013). Furnell and Moore (2014) found that 57% of digital leaders surveyed indicated enhanced IT skills are needed in the existing workforce. Thus, suggesting that there is a notable gap between actual IT skills within organizations and those IT skills believed to be needed (Furnell & Moore, 2014). IS security positions are predicted to grow 37% from 2012 to 2022 (U.S. Department of Labor, 2014). According to the commissioner for the Air Force Association's CyberPatriot contest, feeding the technical workforce starts with getting teenagers excited about science, technology, engineering, and math (STEM) in middle school; waiting until high school was too late (Rastello & Smialek, 2013). Nearly 3,900 young adults, ages 18 to 26, from 12 different countries want jobs using cyber skills, but 58% were not taught cybersecurity skills in the classroom (Raytheon - National Cyber Security Alliance (NCSA), 2015). An average of 22 staff members were reported in an IT security function in 2013 with an expected growth to an average of 29 members in 2014 (Ponemon Institute, 2014b). The increase need of workers with cybersecurity skills is likely to persist at least until education and training catch up (Burning Glass Technologies, 2015).

The demand for employees with skills to protect computer networks and the information contained within those systems will continue to rise as cyber-attacks increase

(U.S. Department of Labor, 2014). Furthermore, hackers have the skills and tactics to exploit the vulnerabilities of individuals, industries, or governments conducting transactions online (Cox, 2015). “As long as the threat exists, there would seem to be sufficient demand for cybersecurity services” (Libicki et al., 2014, p. 76). In addition to the persistent threat, the government’s interest in cybersecurity is a major driver in the demand for those with cybersecurity skills (Libicki et al., 2014). In an attempt to recruit and retain professionals with cybersecurity skills, the U.S. Senate unanimously passed Senate Bill 1691 (2014) to grant the Department of Homeland Security (DHS) the authority to hire qualified experts in an expedited manner at a competitive salary, as well as more benefits and incentives (Chabrow, 2014). People with good cybersecurity skills may be used in many related specialties; all do not obtain a computer science degree (Libicki et al., 2014). Cybersecurity is not exclusively a technical undertaking; an effective national cybersecurity workforce requires a vast range of backgrounds and skills (National Research Council (NRC), 2013). Furthermore, information security practitioners were resistant of attempts to isolate cybersecurity into a single profession in the United Kingdom (Reece & Stahl, 2015). Cybersecurity is a people problem, which requires a people solution (Spidalieri & Kern, 2014). One of the main initiatives of The Comprehensive National Cybersecurity Initiative (CNCI) is to encourage the expansion of cyber education by developing a cyber-skilled workforce, while establishing an effective pipeline for future employees (U.S. National Security Council, 2011). Interviews with self-proclaimed hackers identified the importance of the public in defending against cyber terrorism (Cox, 2015). There is a “demand for skilled workers to secure critical infrastructure and cyberspace” (Spidalieri & Kern, 2014, p. 1).

Furthermore, identifying an individual's poor security practices will assist in strengthening the United States' collective defense against cyber terror (Cox, 2015).

Thus, this study assisted in the identification and measurement of cyber-skilled individuals. A summary of research studies regarding cybersecurity skills shortage follows in Table 14.

Table 14

*Summary of Cybersecurity Skills Shortage*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Cox, 2015	Website reviews and interviews	Several hundred terrorism Websites and 43 self-proclaimed hacker interviews	Cyber terrorism	Cybersecurity skilled individuals assist in strengthening the U.S.' defense against cyber terror
Furnell & Moore, 2014	Empirical study via survey	419 respondents from a UK science and technology showcase event	Security literacy	Initiatives are needed to improve security literacy (i.e., cybersecurity skills)
Libicki et al., 2014	Literature review and analysis		Cybersecurity manpower	There is a high demand for cybersecurity experts in industry as well as the government
Reece & Stahl, 2015	Empirical study via interviews	18 UK information security practitioners	Professionalization of information security	Practitioners are resistant of attempts to the professionalization of information security.



### *Cybersecurity Risk Mitigation and Tools*

Cybersecurity involves both technical and human ability “to protect or defend against cyber-attacks” (CNSS, 2010, p. 22). Risk is defined as “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would rise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (NIST, 2006). Therefore, cybersecurity risk describes any disruption of operations and monetary loss caused by a malicious cyber event (Mukhopadhyay et al., 2013; NIST, 2014). An organization or individual “prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process” (CNSS, 2010, p. 62) is defined as risk mitigation. According to Maxion and Reeder (2005), risk mitigation is necessary to protect IS systems as humans making mistakes compromise IS security. These mistakes include unprotected sensitive files, erroneously configured systems, and mistakenly sending clear text to correspondents (Maxion & Reeder, 2005). Malware as an attack tool appears in many forms, i.e., trojans, virus, worms, rogeware, and is delivered through spam, phishing, and drive-by downloads; each of which involves human interaction (Jang-Jaccard & Nepal, 2014). Moreover, according to Jang-Jaccard and Nepal (2014), common hardware attacks involved hardware trojans, illegal clones, and side channel attacks, i.e., snooping hardware signals. Whereas, common software attacks included software programming bugs (e.g., memory management, user input validation, race conditions, user access privileges, etc.). Likewise, networking protocol attacks and network monitoring and sniffing were the most common network attacks (Jang-Jaccard & Nepal, 2014). As technologies (e.g., social media, cloud computing,

critical infrastructure, embedded systems & sensors, etc.) emerge, the need to mitigate cybersecurity threats and vulnerabilities increases (Jang-Jaccard & Nepal, 2014; Ransbotham, Mitra, & Ramsey, 2012). In response to the cybersecurity threats “placing the Nation’s security, economy, and public safety and health at risk” (NIST, 2014, p. 1), President Obama issued an Executive Order No. 13,636 (2013) to address the need for improving the critical infrastructure systems. Executive Order No. 13,636 (2013) established that “the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties” (p. 11739). Furthermore, the Executive Order 13,636 (2013) summons for the making of the ‘Cybersecurity Framework’ that includes “a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks” (p. 11741).

Through government and private sector collaboration, NIST (2014) created a common language, cost effective, non-regulatory ‘Cybersecurity Framework’ that addresses and manages cybersecurity risk. According to NIST (2014), the ‘Framework’ is to complement, not replace, an organization’s risk mitigation and cybersecurity program. Based on the existing standards, guidelines, and practices, the ‘Framework’ is scalable and evolving as technology advances and business requires (NIST, 2014). It is technology neutral to provide a flexible and risk-based implementation that may be used with a broad array of cybersecurity risk management processes (NIST, 2014). The ‘*Framework Core*’ consists of five functions identified by industry as helpful in

managing cybersecurity risk (NIST, 2014). These functions (Identify, Protect, Detect, Respond, & Recover) assist management of cybersecurity activities at their highest level (NIST, 2014). As described in NIST (2014), the functions may be performed simultaneously and continuously to build an operational culture that tackles the dynamic cybersecurity risk. To grant discussion on how this research fits within the Cybersecurity Framework, each function definition follows.

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities, i.e., asset management, business environment, governance, risk assessment, and risk management strategy;
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services, i.e., access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology;
- **Detect** – Development and implement the appropriate activities to identify the occurrence of a cybersecurity event, i.e., anomalies and events, security continuous monitoring, and detection processes;
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event, i.e., response planning, communications, analysis, mitigation, and improvements;
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event, i.e., recovery planning, improvements, and communications. (NIST, 2014, pp. 8-9)

The five core functions' concurrent and continual cyclical nature are represented in Figure 2.



Figure 2. NIST's cybersecurity framework functions

A human element exists in each function. Thus, the CSI benchmarking index assists in *identifying* cybersecurity skills of non-IT professionals by providing scenarios-based, hands-on tasks to measure those skills. This identification assists in *protecting* the cybersecurity risk areas. Individuals not scoring at an acceptable competency threshold level may be restricted access until the necessary skills are identified above the acceptable competency threshold level measured by the CSI. An individual with cybersecurity skills demonstrates through the CSI benchmarking index the skills necessary in *detecting* anomalies and malicious cybersecurity events in a timely manner. Furthermore, the CSI benchmarking index documents the individual's existing skills and competencies levels in *responding* to a set of cybersecurity tasks. Over time as an individual obtains additional knowledge, experience, and ability, the individual's skills levels increase, and ultimately their competency is achieved (Eschenbrenner & Nah, 2014; Marcolin et al., 2000). Therefore, the CSI assists in the continuous monitoring of cybersecurity skills needed to mitigate and *recover* from cybersecurity risks, which

encourages a strong critical infrastructure. Moreover, the CSI benchmarking index promotes the adoption of the ‘Cybersecurity Framework’ (PwC, 2014). Table 15 lists a summary of cybersecurity risk mitigation and tools.

Table 15

*Summary of Cybersecurity Risk Mitigation and Tools*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Eschenbrenner & Nah, 2014	Literature review and synthesis		IS user competency, social cognitive theory	Developed a conceptual foundation of IS user competency and proposed an IS user competency framework
Jang-Jaccard & Nepal, 2014	Literature review and synthesis		Cybersecurity vulnerabilities and emerging threats	Mitigation of cybersecurity threats should include all levels (e.g., IT & non-IT professionals) of end-users
Marcolin et al., 2000	Empirical study via survey and flash-card self-efficacy assessment	66 university administrators and students	End-user competency	End-users demonstrated less competence than their perceived ability to use a software package
Maxion & Reeder, 2005	Empirical study via laboratory study	24 university students and research staff	Human error, file-permission settings	Human error in file-permission settings were mitigated with an user-interface designed with the external sub-goal support design principle

Table 15

*Summary of Cybersecurity Risk Mitigation and Tools (Cont.)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Ransbotham et al., 2012	Empirical analysis	333 exploited vulnerabilities from three databases	Exploitations of vulnerabilities by attackers	Vulnerabilities disclosed through markets reduces attack penetration, risk, and volume

### **Summary of What is Known and Unknown**

A review of various aspects of skills, cybersecurity, and data breaches was conducted to provide the foundation for this research study. A description of what is known and unknown is provided with this literature review. Through this review of the literature, various data breaches and skills were identified as they relate to cybersecurity. Moreover, it was found that cybersecurity skills are fundamental as a risk mitigation tool and yet there is a cybersecurity skills shortage among non-IT professionals.

Skills are acquired in a three stage incremental learning process (Anderson, 1982; Gravill et al., 2006). The maturing of knowledge also improves an individual's skills, which develops user competency (Toth & Klein, 2014; Rubin & Dierdorff, 2009). When measuring an individual's skills, Gravill et al. (2006) as well as Torkzadeh and Lee (2003) cautioned that individuals did not accurately self-report or perceive their actual skill levels. Prior literature (i.e., Katz, 1974; Swanson, 2004) identified the effectiveness of hands-on tasks for increasing employee's skills. Levy and Ramim (2015) found students with hands-on experience (i.e., computer simulation) performed better than those without. In the work of Vassiliou et al. (2014), observable hands-on skills were found to

provide an unbiased evidence of competence required in the medical and health profession. The use of scenario-based, hands-on skill assessments found in the aviation, medical, and transportation appears applicable to cybersecurity skills of non-IT professionals. A benchmarking index to hierarchically aggregate the set of SMEs identified cybersecurity skills using observable hands-on tasks appears to be absent from literature. Thus, this research study designed, developed, and empirically tested a benchmarking index to hierarchically aggregate the set of SMEs identified cybersecurity skills using observable hands-on tasks. Furthermore, the benchmarking index operationalized into an iPad app that assesses the cybersecurity skills level of non-IT professionals.

## Chapter 3

### Methodology

#### **Overview of Research Design**

This research study was classified as a developmental research. Developmental research tries to answer how the construction of a ‘thing’ addresses a problem (Ellis & Levy, 2009). Richey and Klein (2014) defined developmental research as a way to “create knowledge grounded in data systematically derived from practice” (p. 1). According to Ellis and Levy (2009), developmental research is comprised of three major elements: 1) product criteria is established and validated; 2) process for product development is accepted and formalized; as well as 3) determination of the product’s criteria is met through a formalized, accepted process. In the work of Tracey and Richey (2007), a systematic process was used to develop and then validate their model using the Delphi technique where an expert panel analyzed along with offering feedback on the proposed design. After suggested revisions were analyzed and incorporated, their model was validated by the Delphi technique (Tracey, 2009). Figure 3 illustrates the research design this study followed. To begin Phase One, the site approval letter and Institutional Review Board (IRB) approval were obtained as seen in Appendices A and B, respectively. Thus, Phase One of this developmental research study utilized an expert-review process following the Delphi technique to design and validate the scenarios-based, hands-on benchmarking index for measuring cybersecurity skills (Ramim & Lichvar,



2014). Therefore, Phase Two of this study operationalized the previously developed and validated scenarios-based, hands-on benchmarking index into an iPad app that was used to assess the cybersecurity skills of non-IT professionals. Furthermore, Phase Three of this research study used the previously developed and validated iPad app to conduct a quantitative empirical study by collecting data from 188 non-IT professionals and documenting the results of the measure. The main research question that this study addressed is: What tasks enable the validation of a hierarchical measure for observable cybersecurity skills of non-IT professionals? A group of 188 non-IT professionals were contacted to empirically test the developed CSI.

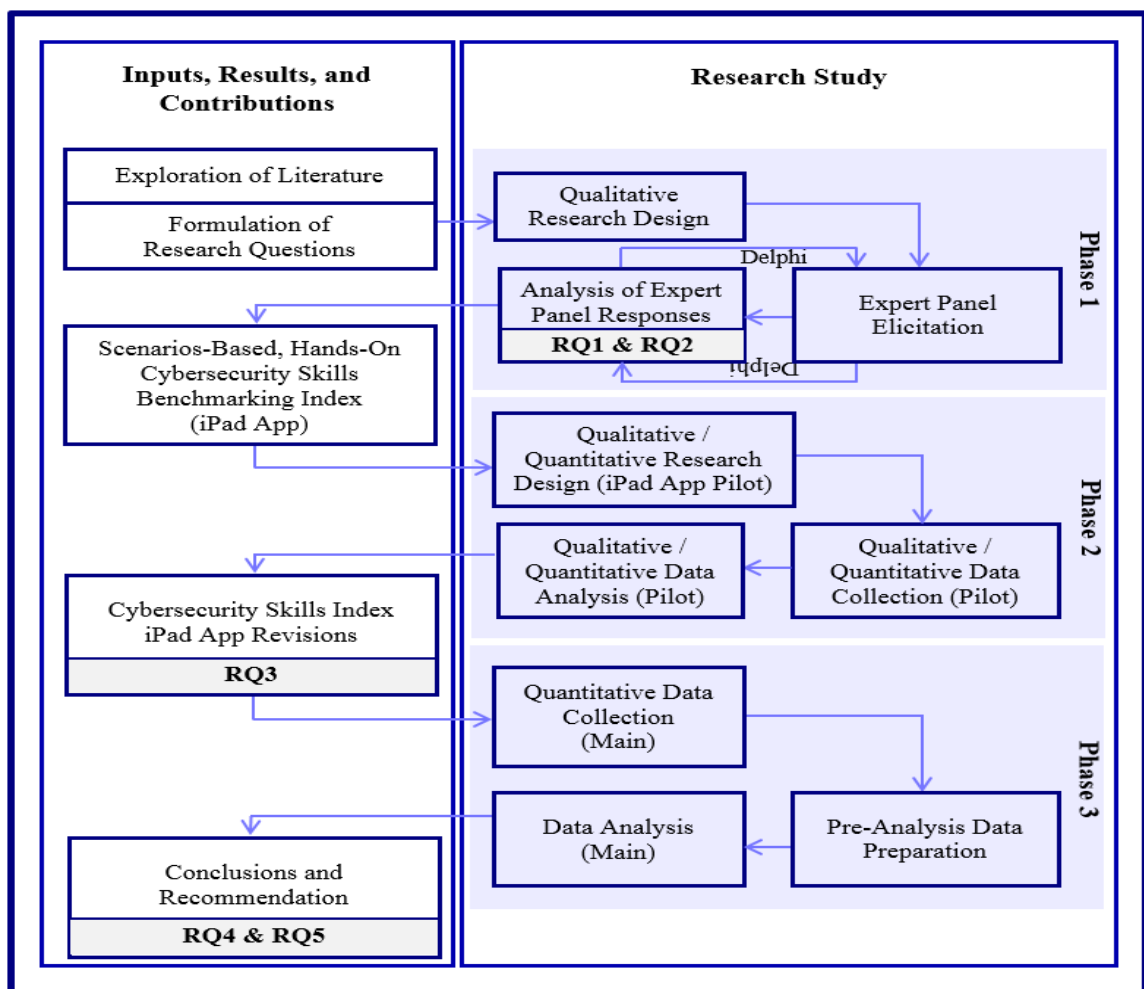


Figure 3. Overview of the Research Design Process

## **Instrument Development**

Choi (2013) recognized the lack of research involving cybersecurity skills, and the need for a measure to assess cybersecurity skills. Furthermore, Choi (2013) identified self-reported surveys as a limitation of research due to a participant's reluctance to report actual misuse behavior. Whereas, Torkzadeh and Lee (2003) cautioned self-reported perceived skills do not always correspond to the individual's actual skills. In the work of Gravill et al. (2006), the use of paper versus computer self-reported evaluative measures varied more in accuracy than self-reported factual information, i.e., years of experience. Xu and Yeh (2012) adjusted for the varying individualities of the assessors that may create biases in the self-assessment process. Weigel and Hazen (2014) argued that practitioners needed an instrument that would measure both perceived and actual technical skills of employees. Senior executives are a critical element to promoting safe computing practices to employees (Tarafdar, D'Arcy, Turel, & Gupta, 2015). The U.S. National Security Council has developed CNCI, and one of its main initiatives is to:

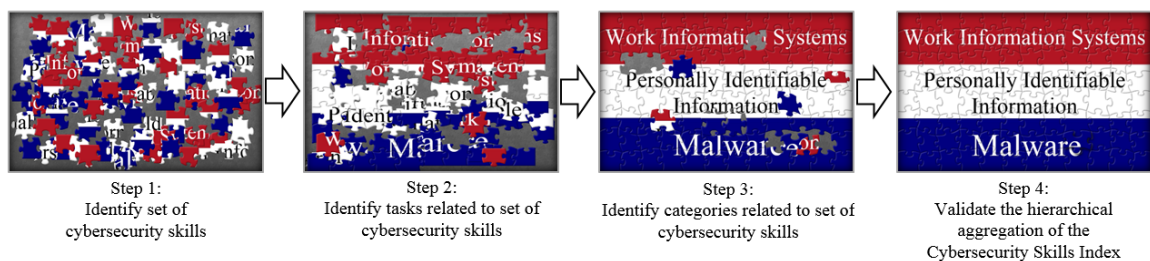
**Initiative #8: Expand cyber education.** While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However, there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are

limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge. (U.S. National Security Council, 2011, para. 17)

Yet, the existing measures of cybersecurity skills are dated and limited. Additional work is needed to develop a measure based on scenarios that emulate real-life cases of cybersecurity attacks. Moreover, with the shift from desktop to laptop computers, and in the past decade to mobile devices, there is a need to ensure such measures are not tied to specific platform and/or operating system. Therefore, this study began by developing a list of the top platform independent skills that form a basis for the set of scenarios that capture potential cybersecurity threats.

With the vast shift into mobile computing and the seamless move between devices that the majority of current employees are engaged in, a critical need emerges to ensure that prior to uncovering the list of the skills, a set of platform independent threats were identified. A list of matching skills needed by non-IT professionals were then developed that formed the foundation for the development of the specific scenarios. For example, the threat of malware via e-mail attachment can be evaluated via an activity within an e-mail attack scenario that provides participants with a list of e-mails in an inbox asking them to identify potential harmful messages and measure how many of these they identify. Another example of an activity within the e-mail attack scenario is to present participants with two e-mail messages from a bank, asking them to identify the one that is

a hoax and the one that is real, while asking them to identify all the indicators that triggered the suspicion of the hoax e-mail. As such, this study was set to develop a tool to assess the observable hands-on, scenarios-based cybersecurity skills of non-IT professionals. Figure 4 illustrates the four step development process of the CSI. Whereas, additional information about the process of using the developed tool to collect and score the performances on the cybersecurity skills of non-IT professionals is provided in succeeding sections.



*Figure 4.* CSI development process

### *Expert Panel*

Content validity is established with literature reviews, pre-testing, and expert panels (Straub, 1989). An expert possesses skills, (i.e., knowledge, experiences, & abilities) in a particular field or domain (Lichvar, 2011). Furthermore, an expert panel can attest to how well “the measure includes an adequate and representative set of items that tap the concept” (Sekaran & Bougie, 2013, p. 226). When judgmental information is essential, prior research has employed the Delphi technique (Okoli & Pawlowski, 2004; Ramim & Lichvar, 2014). Using the Delphi technique provides a method for consensus-building without direct confrontation among the experts (Dalkey & Helmer, 1963). Characterized as an iterative group communication process, the Delphi technique allows for experts to address complex problems in an effective manner (Okoli & Pawlowski,

2004; Ramim & Lichvar, 2014; Scheele, 1975). Prior research, e.g., Brancheau and Wetherbe (1987), as well as Schmidt, Lyytinen, Keil, and Cule (2001), utilized the Delphi technique for forecasting, issue identification, and concept/framework development. In addition, the Delphi technique ensures both reliability and validity as it exposes the study to a panel of differing, and often contradictory, opinions while seeking convergence through SMEs' feedback (McFadzean, Ezingard, & Birchall, 2011; Schmidt et al., 2001). Thus, this study followed the Delphi technique for the purpose of identifying the indispensable expert opinion of cybersecurity threats and related skills (Ramim & Lichvar, 2014).

Key features that are regarded as the Delphi technique include anonymity, iteration, controlled feedback, and statistically clustering the responses (Rowe & Wright, 1999; Skinner, Nelson, Chin, & Land, 2015). Anonymity was maintained in this study with the use of Web-based questionnaires. Between each iteration, feedback was controlled by incorporating the SMEs' responses into the next iteration of the Delphi technique data collection. Therefore, once this study identified the top platform independent threats and related cybersecurity skills for mitigating those threats, scenarios-based, hands-on tasks were developed for establishing the CSI. Prior to data collection, the tasks utilized to measure each respective skill of the CSI were presented to a panel of eight experts in the cybersecurity field for review and validation. These experts were recruited from industry and government agencies specializing in cybersecurity. The expert recruitment email may be seen in Appendix C. All suggested changes received from the panel's review were addressed and incorporated into the iPad app. The tasks

were then presented to the panel as an iteration of the Delphi technique. Appendix D provides the expert qualitative and quantitative questionnaire.

### *Scenario Method*

A hypothetical scenario method is “also known as a vignette or policy capturing method” (Siponen & Vance, 2010, p. 492). With this method, each participant is presented with “written descriptions of realistic situations and then requested responses on a number of rating scales” (Trevino, 1992, p. 127-128). According to Hu et al. (2011), individuals are naturally unwilling to report their actual criminal or deviant behavior. But, participants view scenarios as unthreatening and nonintrusive (D’Arcy et al., 2009). Therefore, business, criminology, IS, and medical scholars have resorted to the use of scenarios to elicit input from participants (Hovav & D’Arcy, 2012; Hu et al., 2011; Kushniruk, Triola, Borycki, Stein, & Kannry, 2005). A scenario method was the most used methodology in 55% of the 174 ethical decision-making articles reviewed by O’Fallon and Butterfield (2005). Certification or specialist exams utilize a scenario-based and/or hands-on tasks to test the candidate’s skills (Furnell, 2004). Moreover, scenario-based assessments are utilized throughout industry and the military to measure skills (Thomas & Lee, 2015; Wesolek, 2009). Antisocial and ethical/unethical behavior assessment is commonly assessed with scenario-based methods (Siponen & Vance, 2010). A scenario method was utilized to simulate two real cases of compromised critical information systems in part of measuring the participant’s abuse intent (Kim, Park, & Baskerville, 2016). Therefore, consistent with prior IS research (i.e., D’Arcy et al., 2009; Hovav & D’Arcy, 2012; Vance, Siponen, & Pahlila, 2012), the designed scenarios presented in this study represent realistic and commonplace situations to the participants.

### *Hands-on Tasks and Skill Assessments*

Hands-on skill assessments are a substantial part of the medical academic community (Berendonk et al., 2013). Skill assessments are completed through the observation of demonstrated hands-on tasks (Vassiliou et al., 2014). Scenario-based, hands-on tasks are used to measure a driver's skills without causing harm to individuals, damage to vehicles, or inaccurate self-perceived responses (Sahami & Sayed, 2013; Sundström, 2011). Moreover, aviation academic curriculum utilizes scenario-based, hands-on assessments to measure pilots' skills as mandated by the Federal Aviation Administration (FAA) (Thomas & Lee, 2015). The importance of skills and hands-on skills assessment found in the aviation, healthcare, and transportation industries appear applicable to cybersecurity skills as well. Torkzadeh and Lee (2003) used self-reported surveys to research the individual's perception of his or her skills and cautioned that perceived skills do not always correspond to actual skills. In the work of Gravill et al. (2006), users inaccurately assessed their knowledge of a specific software package. Prior literature addressed the flaws and consequences of erroneous self-assessment reporting (Mann, 2010; Weigel & Hazen, 2014; Xu & Yeh, 2012). Thus, this study established a validated set of observable hands-on, scenarios-based tasks that measure cybersecurity skills of non-IT professionals without the bias of or need for self-assessment.

### *MyCyberSkills™ iPad App Development*

The CSI includes a set of hands-on tasks that measure the actual cybersecurity skills level of non-IT professionals. With the use of literature, (i.e., Mathews & Yadron, 2015; Yadron et al., 2014), a scenario starts each task. Each skill included a group of four cybersecurity related hands-on tasks for the non-IT professional to identify and

demonstrate their skill level as if in a real-life situation (Hovav & D'Arcy, 2012; Vance et al., 2012). The MyCyberSkills™ prototype operationalized the previously developed and validated scenarios-based, hands-on benchmarking index into an iPad app that was used to assess the cybersecurity skills of non-IT professionals. The conceptual design of the CSI as it is presented within the MyCyberSkills™ iPad app is exhibited in Figure 5.



Figure 5. Conceptual design of the CSI operationalized within the MyCyberSkills™ iPad App Prototype

Each of the cybersecurity related tasks were presented individually in the MyCyberSkills™ iPad app. Once task one of a skill was completed, scenario two was presented. Task two then incremented in difficulty and presents the non-IT professional again with four response options. As the non-IT professional responds to each hands-on observable task, the MyCyberSkills™ iPad app recorded the non-IT professional's performance level using a scale of 0 to 10 and then presented the next cybersecurity related task. According to Schwartz and Fischer (2004), an individual cannot solve a problem that exceeds the individual's highest developed skill level. Therefore, the level of difficulty increased as each task was presented within the respective skill. This presentation continued measuring the non-IT professionals' skills with an easy, somewhat difficult, difficult, and very difficult task within each skill. Figure 6 illustrates the process of each skill (n) as it was presented to the non-IT professional. Each skill



began with a scenario (e.g., n.1) and then presented the hands-on task with four response options (e.g., n.1.1). For some skills, the individual's response warranted an alternate scenario for maintaining the incremental level of difficulty. When this occurs, scenarios were identified as A and B as seen in the somewhat difficult category of Figure 6.

Once the set of tasks for a specific skill was completed by the non-IT professional, the next set of tasks began with a relevant scenario followed with the easiest cybersecurity related task and incrementing to the very difficult cybersecurity related task. This process continued until a response was received for each task. A total weighted score interval of zero to 40 was possible for each cybersecurity skill. During an iteration of a Delphi technique, the SMEs were asked to assign each cybersecurity skill ( $CS_i$ ) a weight,  $W_{CS_i}$ , ranging from zero to one. A coefficient was identified after the set number of cybersecurity skills were established in order to display the overall CSI score range of zero to 100. After completing all tasks, the MyCyberSkills™ iPad app displayed the achieved overall CSI score interval of zero to 100 and the score interval of zero to 100 for each individual cybersecurity skill.

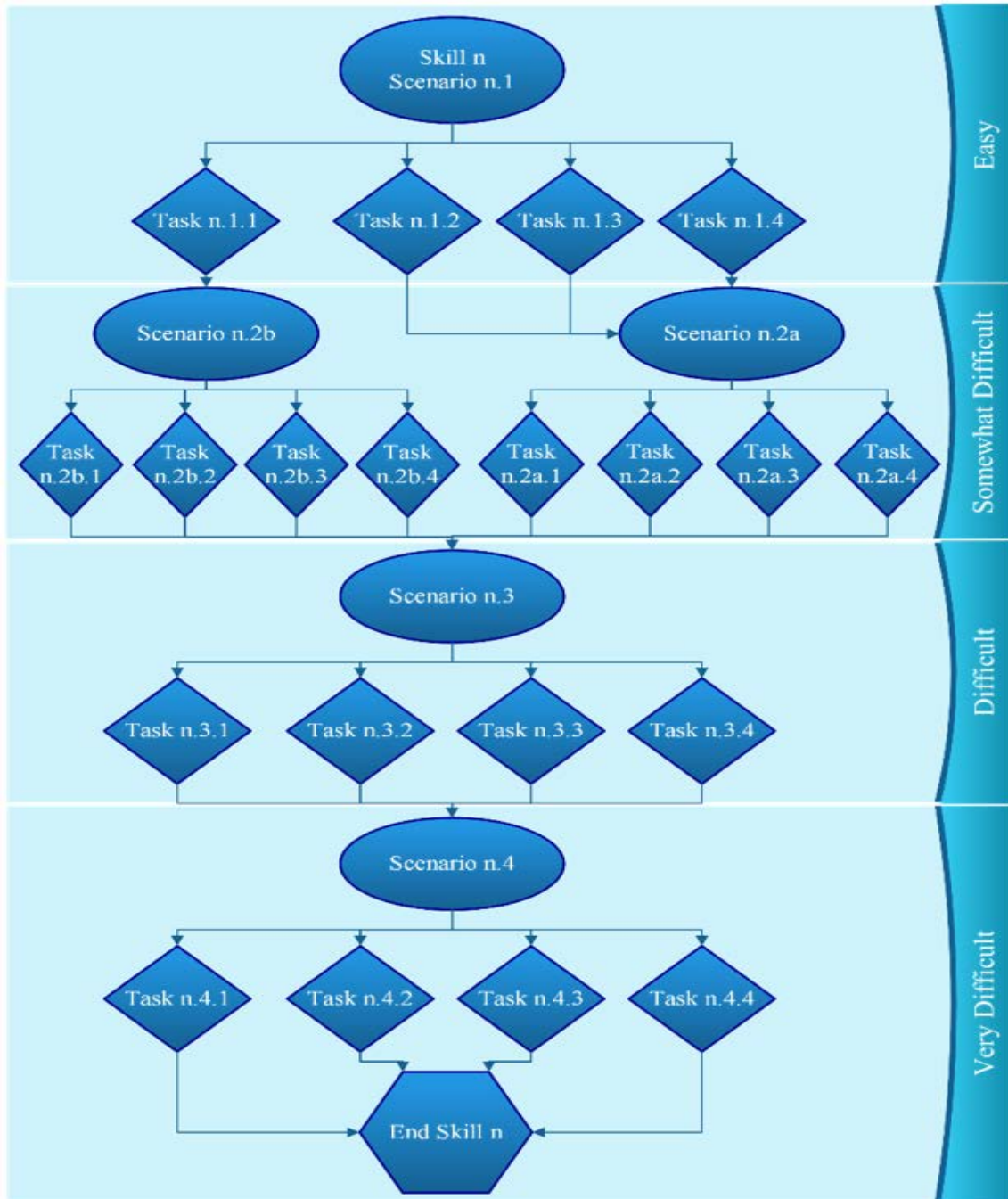


Figure 6. Scenario-based, hands-on task skill levels

### Reliability and Validity

Reliability may exist without validity, but validity cannot exist without reliability (Mendoza, 2014; Reinard, 2006). Moreover, validity and reliability influence the amount

a researcher may learn about the phenomenon under investigation (Leedy & Ormrod, 2013). Within this development research, the use of the sequential-exploratory method allowed for the capitalization of the benefits from each qualitative and quantitative research approach to collect data (Greene, Caracelli, & Graham, 1989; Terrell, 2011). Reliability ensures consistent or error-free results are produced (Rogers, 1995), as well as makes “a statement about measurement accuracy” (Boudreau, Gefen, & Straub, 2001, p. 5). Thus, this study evaluated the MyCyberSkills™ iPad app in an iterative development process, in addition to analyzing the data captured (Onwuegbuzie, Bustamante, & Nelson, 2010; Sheng et al., 2007).

### *Reliability*

The CSI was developed to measure the cybersecurity skills level of non-IT professionals incorporated into the MyCyberSkills™ iPad app. An index’s reliability is determined by reproducibility and consistency (Helminen, Halonen, Rankinen, Nissinen, & Rauramaa, 1995). Without stability and internal consistency, the measurement precision of an index is viewed as weak (Helminen et al., 1995; Chakhssi, de Rulter, & Bernstein, 2010). Therefore, the MyCyberSkills™ iPad app assessment was validated with rigorous testing. As the scenarios-based, hands-on tasks were developed, each response received a score. To ensure the correct score was recorded and the participant received an accurate CSI score by the MyCyberSkills™ iPad app, 21 non-IT professionals were observed while demonstrating their hands-on tasks during the pilot-test of the initial app. As the participants demonstrated each task, the action taken was manually recorded and scored. The overall CSI score and individual skills scores were then manually calculated. If the manual calculations compared to those calculated by the

MyCyberSkills™ iPad app matched, reliability and validity was established. Thus, the individual task scores, the overall score for each skill, and the CSI score was validated using this manual process. Moreover, to ensure a higher reliability of this study, a balance was found among factors (i.e., data collection environment, length of the test) which were identified to effect reliability and validity (Reinard, 2006).

### *Validity*

An index is considered valid based on its relevance and provision of an accurate assessment of what it is measuring (Alias, 2015). Incorporating the validation of a measure can help substantiate research findings, as well as “move the IS field forward toward meaningful replicated studies” (Straub, 1989, p. 162). Striving for validation, a panel of 8 experts were asked how relevant each task was in accessing the respective skill and to describe in their own words revisions (if any) needed to the skill or task (Boudreau et al., 2001; Nelson, Bustamante, Wilson, & Onwuegbuzie, 2008). Moreover, asking for IS and cybersecurity experts’ comments and suggestions ensured the MyCyberSkills™ iPad app maintained consistency, ‘state-of-the-art’ knowledge, and industry practicality (Ball et al., 2015; Wang, Nieveen, & van den Akker, 2007). Therefore, this study reduced the threat to validity by using scenarios-based, hands-on tasks that were validated through an expert panel following the Delphi technique (Ramim & Lichvar, 2014). Furthermore, eliciting the feedback from the SMEs ensured both validity and reliability that the criteria used to develop the CSI measure was appropriate (Brown, Levy, Ramim, & Parrish, 2015).

### *Pilot-Test Initial App*

Once the MyCyberSkills™ iPad app was developed, it was subjected to a pilot-test (Creswell, Plano Clark, Gutmann, & Hanson, 2003). As part of the pilot-test of the initial app, 21 non-IT professionals were observed while demonstrating their skills with the presented hands-on, cybersecurity tasks. Appendix E provides the pilot study recruitment email. Prior to beginning the pilot test, all participants were asked to acknowledge and sign an informed consent form as seen in Appendix F. The main focus of this pilot-test was on instrument (i.e., indices, scales) fidelity (Collins, Onwuegbuzie, & Sutton, 2006; Vogt & Johnson, 2011). Regardless of research paradigm, instrument fidelity is defined as the goal in every study “to obtain data that has one or more of the following characteristics: trustworthiness, credibility, dependability, objectivity, confirmability, and/or transferability” (Collins et al., 2006, p. 77). Moreover, this pilot-test ensured the appropriateness of each item (Onwuegbuzie et al., 2010). Furthermore, it assessed 1) the extent to which the scenarios and tasks of the MyCyberSkills™ iPad app appeared relevant and interesting to the respondent; 2) the specific tasks measured the intended content area; and 3) the tasks sampled the respective skill (Onwuegbuzie et al., 2010). At this phase, outcome validity and generalizability were important in order to assess the consequences of using the MyCyberSkills™ iPad app and the extent the meaning of scores may be generalized to other populations (Collins et al., 2006; Onwuegbuzie et al., 2010).

Rigorous testing and an expert-panel as discussed at length in earlier sections were fundamental in establishing fidelity of the CSI benchmarking index and the MyCyberSkills™ iPad app. Furthermore, open-ended questions were available for participants to provide feedback on the MyCyberSkills™ iPad app. Sequentially

collecting qualitative and quantitative data allowed for the identification of themes in the SMEs' validated skills, which were integrated into the design and development of the MyCyberSkills™ iPad app (Creswell et al., 2003). Moreover, collecting both qualitative and quantitative data at this phase not only enhanced the MyCyberSkills™ iPad app, but also validated the CSI (Nelson et al., 2008; Onwuegbuzie et al., 2010). Thus, the feedback and results from this pilot-test were analyzed and all adjustments to the CSI and/or MyCyberSkills™ iPad app were completed. At the conclusion of the pilot test, each participant was given the opportunity to attend a cybersecurity workshop offered by the researcher as a token of appreciation for their time.

#### *Design and Empirical Study: Revised App*

Problematic items identified during the initial pilot-test were revised or discarded (Onwuegbuzie et al, 2010; Sheng et al., 2007). After the initial app was revised, an empirical study was conducted using the previously developed and validated iPad app. This quantitative phase of the developmental research study collected data from 188 non-IT professionals and documented the results of the measure. Furthermore, recommendations for the administration as a result from the data analysis are presented in Chapter Five. Additional information regarding the sample, data collection, and analysis follows.

#### **Population and Sample**

This study evaluated the cybersecurity skills level of 188 non-IT professionals using the developed CSI. These non-IT professionals were recruited at multiple public places located within the Southeastern United States. Appendix G was utilized to recruit

participants for the empirical research study. With the assistance of demographic data, the sample characteristics in the research were used to test the representation of the data collected to the generalized study population (Sekaran & Bougie, 2013). Although inferential statistics were not performed on categorical data, (i.e., age, gender) collecting the data assists in identifying the characteristics of the participants (Terrell, 2012). Therefore, demographic data, such as age, gender, as well as job function, were collected as part of this research study.

### *Data Collection*

Prior to beginning the empirical research study, participants were asked to complete an informed consent form as seen in Appendix H. With the use of the validated MyCyberSkills™ iPad app, 188 non-IT professionals were presented a set of cybersecurity skills related tasks. Each task contained four possible responses. As the participants responded to each task, the score associated with that response was recorded on a spreadsheet stored as a password protected Google document. After all participants completed the MyCyberSkills™ app, a cybersecurity workshop was provided to assist the participants in furthering their cybersecurity knowledge, experience, and abilities.

Pre-analysis data screening involved the process of detecting and dealing with irregularities or problems with the collected data (Levy, 2006). It may also indicate that the developed tool is not performing as expected. According to Mertler and Vannatta (2010), data must be checked for accuracy and consistency. Furthermore, rigorous data examination must be completed prior to final analysis of data as missing data may create substantial effects (Alias, 2015; Hair, Black, Babin, & Anderson, 2010). Thus, missing

data were evaluated during and prior to the final analysis of data to ensure a consistent, valid, and reliable tool (Levy, 2006; Onwuegbuzie et al., 2010).

### *Data Analysis*

Findings of the data collected from the literature review, the expert panel, and the MyCyberSkills™ iPad app initial pilot-test was used to develop a valid and reliable assessment of cybersecurity skills levels. Furthermore, an empirical study using the validated MyCyberSkills™ iPad app was conducted with a group of 21 non-IT professionals. The iterative processes lead to increased instrument fidelity as well as reliability and validity (Alias, 2015; Onwuegbuzie et al., 2010). By using literature and an expert panel, the identification of the most common cybersecurity organizational threats addressed RQ1. This study addressed RQ2 by using the literature review and expert panel for establishing the four tasks for each of the skills needed to thwart the most common cybersecurity organizational threats. This research study addressed RQ3 by validating the CSI benchmarking index with the expert panel and pilot-test. Testing the level of cybersecurity skills of 188 non-IT professionals using the same CSI developed in RQ3 addressed RQ4. To assess the fifth research question, descriptive and one-way Analysis of Variance (ANOVA) was conducted on age, educational level, gender, job function, primary online activity, number of hours accessing the Internet, and experience using technology to identify any significant differences to CSI scores.

### **Resources**

In order to complete this study the following resources were used:



- Access to a pool of non-IT professionals in the U.S.: The sample was collected from a population of non-IT professionals recruited from multiple public places located in the Southeastern United States. This sample was accessible and approved through the IRB process.
- App developers: App developers were required to assist with programming the MyCyberSkills™ tool. These developers were recruited from a population of students at two institutions of higher education located in the state of Florida. The developers assisted in programming the MyCyberSkills™ prototype used in collecting data for this research study.
- Articulate Storyline 2: This software package was used by the app developers to transform the written scenarios-based, hands-on tasks into a Web-based prototype. The prototype was published using HTML5, Flash, and JavaScript.
- Expert panel: Many phases of this research relied on an expert panel of industry, academic, and government professionals in the cybersecurity field. Feedback from the expert panel was used to identify the top nine cybersecurity skills as well as the validity of the scenarios, tasks, and scores presented in the MyCyberSkills™ iPad app.
- Google forms: This web-based tool was used to develop the expert survey instrument as well as record the data collected upon the participant completing the iPad app. An account was activated for use and the survey was designed to ensure successful implementation of the tool.

- Statistical analysis tool: Statistical Package for the Social Sciences (SPSS) was used to complete descriptive statistics, frequency distributions, and ANOVA. Lists and graphs were created using the SPSS tool to compile and analyze the results.
- Technology: Each step of the dissertation process required the use of hardware, software, networking, and library resources. Communications with advisor and committee, researching the literature, and writing the dissertation report was completed using this technology. All necessary technology components were acquired.

### **Summary**

Chapter Three included a description of the research design, methodology, an explanation of the MyCyberSkills™ iPad app, and measures that were used in this research study. This study was classified as developmental in nature and used a sequential-exploratory approach to validate the reliability of the CSI benchmarking index and MyCyberSkills™ iPad app. A discussion of methods was presented that answered the five research questions. The cybersecurity skills benchmarking index was developed using a literature review, in addition to feedback by an expert panel. The assessment criteria was based on literature and initiated the process. Next, SMEs evaluated the cybersecurity threats, related skills, and their respective weights used in the CSI. Feedback from the SMEs were then used to revise the CSI until a consensus was reached using the Delphi technique. According to McFadzean et al. (2011) as well as Skinner et al. (2015), this methodology is acceptable to assess the reliability and validity of the CSI.

Issues pertaining to reliability and validity of the CSI and MyCyberSkills™ iPad app were discussed along with how they were mitigated.

Next, the population and sample for this research study was presented, which included the selection criteria of the non-IT professionals. Furthermore, the pre-analysis data screening, as well as the data analysis addressed the research questions. Pre-analysis data screening was used to “detect irregularities or problems with the collected data” (Levy, 2006, p. 150). It assisted in identifying when the developed tool was not performing as intended. Chapter Three concludes with the resources that were used to conduct this research study.

## Chapter 4

### Results

#### **Overview**

Outlined within this chapter are the results of the data analysis for this research investigation. The results for this study were completed in three phases. Details of each phase are presented in the order conducted. Phase One details the data collection for the expert panel using the Delphi technique, which was then used to develop a novel scenarios-based, hands-on cybersecurity skills benchmarking index. The results of Phase One address RQ1 and RQ2.

Phase Two details the development of a the MyCyberSkills™ iPad app prototype using gathered expert panel feedback with the Delphi technique as well as a pilot study to ensure the prototype accurately recorded scores. The results of Phase Two address RQ3. The conclusion of the chapter includes Phase Three, the results summary using the MyCyberSkills™ iPad app prototype, and the data analysis processes used. The results of Phase Three address RQ4 and RQ5.

#### **Qualitative Research and Expert Panel (Phase One)**

This study employed the Delphi technique for the purpose of identifying the expert opinion of cybersecurity threats and related skills (Ramim & Lichvar, 2014). The Delphi technique is an iterative group communication process that allows for experts to

address complex problems in an effective manner and without direct confrontation (Dalkey & Helmer, 1963; Okoli & Pawlowski, 2004; Ramim & Lichvar, 2014).

Anonymity was maintained in this phase of this research study with the use of Web-based questionnaires (Rowe & Wright, 1999). Between each questionnaire, the SMEs' responses were incorporated into the next questionnaire to control the feedback.

The first round of the Delphi technique consisted of 12 platform independent cybersecurity threats. After a survey of the existing body of knowledge, these threats were identified and presented to SMEs from the Florida chapter of the InfraGard, a public-private partnership between the United States Federal Bureau of Investigation (FBI)'s cyber division and private sector that focus on cybersecurity, along with SMEs from other federal agencies such as the United States Secret Services' (USSS) Electronic Crimes Task Force team and industry. The SMEs were asked to rank in order of importance the threats that non-IT professionals poses for organizational cybersecurity posture. Based on the SMEs' feedback, the list of 12 platform independent cybersecurity threats were narrowed to 10 platform independent cybersecurity threats. In the second Delphi technique round, the 10 cybersecurity threats identified as the most significant were then presented to the panel of SMEs in a Web-based survey using a seven-point Likert scale. Based on a score of '1' for strongly disagree and '7' for strongly agree, each of the cybersecurity threats were evaluated to determine 1) if it was valid to be included in the core fundamental cybersecurity threat set, 2) if a proposed platform independent skill is valid or not; and 3) if each proposed skill is independent from other proposed cybersecurity skills. Moreover, the SME panel were asked to provide a ranking of '1', representing the highest threat, to '10', representing a lessor threat. The skill importance

weight for each skill was calculated so the lesser threat received a weight closer to 0.0, while the highest ranked threat received a weight closer to 1.0. The threats are based on their skill importance weight in causing harm to organizations and individuals, while forming the foundations for the development of the hierarchical-based indexing to measure an overall measure of cybersecurity skills. The survey instruments were designed electronically using Google forms.

A consensus of SMEs' opinion emerged with the top nine cybersecurity skills needed for non-IT professionals. Malware, PII, and WIS related threats were the distinct categories identified among the cybersecurity threats and identified matching skills. At the end of the second Delphi round, the difference between the lowest ranked cybersecurity threat/skill and the highest was nearly 2.28. Cybersecurity threat and corresponding skill number 10, preventing unauthorized information system access via workstation lock or log out, was identified as an outlier and the SMEs highly recommended discarding it. Table 16 displays the collective results of both Delphi rounds identifying the top nine platform independent cybersecurity skills, their respective category, SME rankings, number of SME responses, ranked weighted total, ranked average, and skill importance weight. These results were used to address the first and second research questions of this study. Moreover, the top nine platform independent cybersecurity skills, their respective category, SME rankings, and skill importance weight was the foundation for the start of Phase Two.

Table 16

*Rankings of the Top Nine Cybersecurity Skills*

Skills	Category	Individual SME Rankings										SME Response	Weighted Total	Weighted Average	Skill Importance Weight
		1	2	3	4	5	6	7	8	9	10				
1 - Preventing the leaking of confidential digital information to unauthorized individuals	Work Information Systems (WIS)	8	2	0	0	3	0	1	2	0	2	18	128	7.111	0.136
2 - Preventing malware via non-secure Websites	Malware	1	4	4	3	0	4	1	0	0	1	18	124	6.889	0.132
3 - Preventing personally identifiable information (PII) theft via access to non-secure networks	PII	4	1	2	3	2	2	2	0	2	0	18	120	6.667	0.127
4 - Preventing PII theft via e-mail phishing	PII	1	3	1	2	2	3	2	3	1	0	18	105	5.833	0.112
5 - Preventing malware via e-mail	Malware	2	0	6	1	2	0	2	0	3	2	18	103	5.722	0.109
6 - Preventing credit card information theft by purchasing from non-secured Websites	Malware	1	1	1	3	2	2	1	6	1	0	18	94	5.222	0.100
7 - Preventing information system compromise via USB or storage drive/device exploitations	WIS	0	3	1	2	1	2	3	3	2	1	18	91	5.056	0.097
8 - Preventing unauthorized information system access via password exploitations	WIS	1	0	1	4	3	2	1	1	3	2	18	89	4.944	0.095
9 - Preventing PII theft via social networks	PII	0	2	2	0	3	2	3	2	3	1	18	87	4.833	0.092
<b>Totals --&gt;</b>												<b>941</b>	<b>52.278</b>	<b>1.000</b>	

**Qualitative and Quantitative Research (Phase Two)**

The development and validation of a comprehensive set of scenarios-based, hands-on benchmarking index was a good step in the right direction. At the beginning of Phase Two and using the results of Phase One as a foundation, the designed set of observable scenarios-based, hands-on tasks that measure cybersecurity skills of non-IT professionals without the bias of or need for self-assessment were operationalized into a MyCyberSkills™ iPad app prototype. Each skill was designed in this study to include a group of four cybersecurity related hands-on tasks for the non-IT professional to identify and demonstrate their skill level as if in a real-life situation (Hovav & D'Arcy, 2012; Vance et al., 2012). The sum of all nine skills multiplied times their respective weight ( $w_i$ ) was then multiplied times the coefficient of 2.5. This resulted in the non-IT professionals' CSI score of zero to 100. With the use of literature, (e.g., Glazer and Yadron 2014), a scenario began each task. The written scenarios-based, hands-on tasks were transformed into a digital presentation with the use of Articulate Storyline 2. Table

17 displays the CSI, the SMEs ranked cybersecurity skills ( $SK_i$ ), their respective hands-on tasks ( $T_{ij}$ ), description, range, and weight. These results were incorporated into the design and development of the MyCyberSkills™ iPad app prototype.

Table 17

*Cybersecurity Skills Index and SMEs Ranked Cybersecurity Skills*

Variable	Components	Description	Range	Weight
$SK_1$	$T_{1_1} + T_{1_2} + T_{1_3} + T_{1_4}$	Preventing the leaking of confidential digital information to unauthorized individuals	0 – 40	.136
$SK_2$	$T_{2_1} + T_{2_2} + T_{2_3} + T_{2_4}$	Preventing malware via non-secure Websites	0 – 40	.132
$SK_3$	$T_{3_1} + T_{3_2} + T_{3_3} + T_{3_4}$	Preventing personally identifiable information (PII) theft via access to non-secure networks	0 – 40	.127
$SK_4$	$T_{4_1} + T_{4_2} + T_{4_3} + T_{4_4}$	Preventing PII theft via e-mail phishing	0 – 40	.112
$SK_5$	$T_{5_1} + T_{5_2} + T_{5_3} + T_{5_4}$	Preventing malware via e-mail	0 – 40	.109
$SK_6$	$T_{6_1} + T_{6_2} + T_{6_3} + T_{6_4}$	Preventing credit card information theft by purchasing from non-secured Websites	0 – 40	.100
$SK_7$	$T_{7_1} + T_{7_2} + T_{7_3} + T_{7_4}$	Preventing information system compromise via USB or storage drive/device exploitations	0 – 40	.097
$SK_8$	$T_{8_1} + T_{8_2} + T_{8_3} + T_{8_4}$	Preventing unauthorized information system access via password exploitations	0 – 40	.095
$SK_9$	$T_{9_1} + T_{9_2} + T_{9_3} + T_{9_4}$	Preventing PII theft via social networks	0 – 40	.092
CSI	$\left(\frac{5}{2}\right) \sum_{i=1}^9 [(SK_i) \cdot w_i]$	Coefficient * (Sum of all 9 skills * respective weights)	0 – 100	

After transforming each of the skills into a digital presentation, a panel of eight SMEs was presented a questionnaire in a portable document format (PDF) soliciting qualitative and quantitative feedback on the scenarios, tasks, and scoring of the prototype. Table 18 lists the collective feedback from all experts and the adjustments made to the initial MyCyberSkills™ prototype. Recommendations of the SMEs' were incorporated into the prototype before the second round of the Delphi technique began. The expert panel was asked to repeat the review process again on the revised MyCyberSkills™ iPad app prototype at which time the interpretation of the original feedback and adjustments was validated. At the conclusion of round two of the Delphi technique, a consensus of



SMEs' opinion was reached regarding the digital presentation of the scenarios, tasks, and scoring within the MyCyberSkills™ iPad app prototype. Thus, no additional iterations with the expert panel were required. The Delphi technique reinforced the validity of the MyCyberSkills™ iPad app prototype.

Table 18

*Delphi Expert Panel Suggested Adjustments to Initial Prototype*

<b>Change #</b>	<b>Feedback</b>	<b>Adjustments</b>
1.	The “I don’t know” button for aborting a task was confusing and values scored too high.	All “I don’t know” options were changed to a different action or “no change” option and values assigned according to possible threat mitigation.
2.	Scenario associated with question 2.2a and 2.2b does not address preventing malware via non-secure Websites.	The scenario was changed to request a driver update to simulate a malware infection threat.
3.	Question 6.2 needs to ask for credit card information not MoneyPak.	Image for question 6.2 revised to ask for credit card information.
4.	Question 7.1 should have an option to “do nothing” or “leave in parking garage”.	“I don’t know” option was changed to “leave USB on the ground”.

Furthermore, throughout the development process rigorous testing was completed to ensure the validity and reliability of the MyCyberSkills™ iPad app prototype. To ensure the correct score was recorded by the prototype, the business administrator sent a participation email to the non-IT professionals on staff at a public place of worship in the Southeastern United States for completing the MyCyberSkills™ iPad app prototype. Out of the 40 invitations to participate, 21 non-IT professionals were observed while

demonstrating their hands-on tasks during the pilot-test, generating a 52.5% response rate. When comparing the manually recorded scores to the automatically recorded scores, a scoring anomaly was noted early in the pilot-test. The anomaly was corrected prior to the conclusion of Phase Two. Any revisions to the MyCyberSkills™ iPad app prototype were made prior to the empirical study (Sheng et al., 2007; Terrell, 2012). Thus, the third research question and goal of this study was addressed with the novel CSI operationalized with the MyCyberSkills™ prototype. Furthermore, to address the fourth and fifth research questions and goals in Phase Three, the validated and reliable MyCyberSkills™ iPad app prototype was the tool used for collecting data from non-IT professionals and documenting the results of the measure.

### **Quantitative Research (Phase Three)**

#### *Pre-Analysis Data Screening*

In Phase Three, participants were recruited by 1) a participation flyer posted throughout a public place of worship located in the Southeastern United States as well as 2) flyers and emails shared with multiple public places of business (i.e., restaurants, medical offices, etc.). Participants were invited to attend a cybersecurity workshop or receive a \$5 Starbucks gift card as a token of appreciation for completing the MyCyberSkills™ iPad app prototype. Out of 975 individuals invited, 245 responses were collected, generating a 25.1% response rate.

Prior to completing the MyCyberSkills™ prototype, participants were asked demographic and technology usage questions. These responses were recorded prior to the participant beginning the MyCyberSkills™ iPad app prototype. Elimination of cases with

response-set, verification of missing data, and addressing extreme cases or outliers was performed in the pre-analysis data screening to ensure the accuracy of the data collected (Levy, 2006). Pre-analysis data screening revealed 57 participants that began the study, but did not complete the MyCyberSkills™ iPad app prototype tool.

Data accuracy was not a matter of concern as the prototype was designed to allow only a single valid answer for each task. Additionally, completed responses were downloaded into a Google form and imported into Statistical Package for the Social Sciences (SPSS) for further pre-analysis data screening. The data set was analyzed for any response-set issues, where participants selected the same scale value for all the technology usage questions. After a visual inspection, no response-set cases appeared. Respondents were forced to select from a fixed set of answers and were unable to leave any items unanswered. However, to ensure the accuracy of the data, descriptive statistics were used to identify the minimum and maximum value for each skill score to determine if responses were within the expected value range and were not accidentally corrupted during the transfer of data between Google forms and SPSS. All responses were within the expected ranges and none were removed. Thus, generating 188 or 19.3% non-IT professional responses for analysis.

The means and standard deviations for the individual skills one to nine, skill categories, and overall CSI for the population were calculated. A review of the calculated means of the individual skills, skill categories, and overall CSI was used to address the fourth research question and goal of this study. Table 19 presents the means and standard deviations for the population. With a mean of 81.4%, the participants appeared most skilled in the preventing the leaking of confidential information (SK<sub>1</sub>). Moreover, the

participants appeared least skilled in the preventing malware via Email (SK<sub>5</sub>) with a mean of 47.4%. Figure 7 presents a visualization of the means of the individual skills (e.g., SK<sub>1</sub>, SK<sub>2</sub>, SK<sub>3</sub>, SK<sub>4</sub>, SK<sub>5</sub>, SK<sub>6</sub>, SK<sub>7</sub>, SK<sub>8</sub>, & SK<sub>9</sub>) and the malware, PII, and WIS categories sorted from highest to lowest along with the overall CSI for the population.

Table 19

*Means and Standard Deviations for the Population (N=188)*

	Item	Mean	Standard Deviation
Individual Skills	SK <sub>1</sub> Leak Confidential Info	0.814	0.142
	SK <sub>2</sub> Malware via Non-Secure Web	0.493	0.190
	SK <sub>3</sub> PII Theft via Non-Secure Web	0.484	0.298
	SK <sub>4</sub> PII Theft via email	0.598	0.198
	SK <sub>5</sub> Malware via email	0.474	0.185
	SK <sub>6</sub> Credit Card Theft via Non-Secure Web	0.581	0.159
	SK <sub>7</sub> USB Exploits	0.652	0.191
	SK <sub>8</sub> Password Exploits	0.725	0.175
	SK <sub>9</sub> PII Theft via Social Network	0.636	0.215
Categories	WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	0.730	0.119
	Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	0.516	0.116
	PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	0.573	0.161
	Overall CSI	0.605	0.099

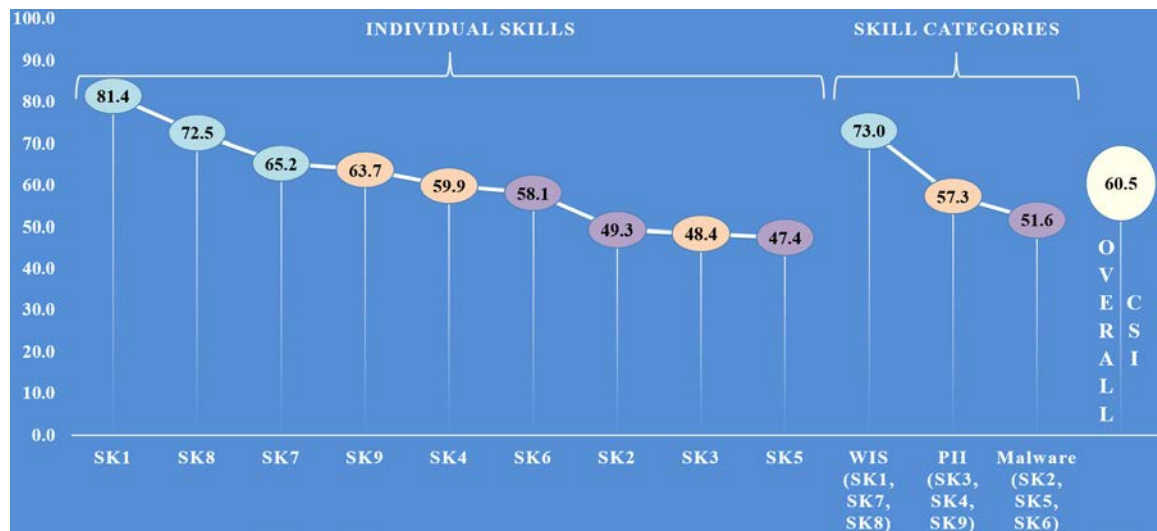


Figure 7. Means of the Individual Skills, Skill Categories, and Overall CSI

### *Demographic Analysis*

After completing the pre-analysis data screening, 188 responses remained for analysis, with demographics that represents a likeness to that of the general sample targeted. Of which, 107 or 56.9% were females and 81 or 43.1% were completed by males. An analysis of the participants' ages revealed that 122 or 64.9% were 20 to 54 years of age. Overall, 151 or 80.3% had a primary activity of work related tasks, social network (Facebook, Twitter, Instagram, etc.), or search engine (Google, Yahoo, Bing, etc.) and 124 or 66.0% accessed the Internet 6 to 30 hours per week. While nearly 35% of the participants were in administrative staff, managerial, or executive job functions, over 50% of participants responded with the job function of 'other'. Given a community approach was used to recruit participants, a response of 'other' could include occupations such as nurses, teachers, dental assistants, cashiers, and wait staff. Moreover, an analysis of the participants' education revealed 120 or 63.8% had completed a college or graduate degree, 56 or 29.8% had earned a high school diploma, as well as 12 or 6.4% responded with 'other' education. After further review, a participants' response of 'other' education indicated an industry certification or license obtained outside of the secondary or higher education institutions (i.e., nursing or teaching certification, etc.). Moreover, 159 or 84.6% of the participants indicated having neutral to absolutely expert level of experience using technology. Appendix I displays the details of the demographics of the population.

Table 20

*Descriptive Statistics of the Population (N=188)*

<b>Item</b>	<b>Frequency</b>	<b>Percentage (%)</b>
<b>Gender</b>		
Male	81	43.1%
Female	107	56.9%
<b>Age</b>		
18 or 19 years	11	5.8%
20 to 24 years	21	11.2%
25 to 34 years	41	21.8%
35 to 44 years	27	14.4%
45 to 54 years	33	17.5%
55 to 64 years	36	19.2%
65 or older	19	10.1%
<b>Academic Level</b>		
High school diploma	56	29.8%
College degree	90	47.9%
Graduate degree	30	15.9%
Other	12	6.4%
<b>Job Function</b>		
Administrative staff	38	20.2%
Managerial	18	9.6%
Executive	8	4.3%
Operations	9	4.8%
Physical security	2	1.0%
Information Technology	10	5.3%
Technical Services	5	2.7%
Other	98	52.1%
<b>Accessing the Internet</b>		
0 to 5 hours	10	5.3%
6 to 10 hours	42	22.4%
11 to 15 hours	19	10.1%
16 to 20 hours	19	10.1%
21 to 25 hours	23	12.2%
26 to 30 hours	21	11.2%
31 or more hours	54	28.7%

Table 20

*Descriptive Statistics of the Population (N=188) (Cont.)*

<b>Item</b>	<b>Frequency</b>	<b>Percentage (%)</b>
<b>Primary Internet Activity</b>		
Work related tasks	76	40.4%
Social network (Facebook, Twitter, Instagram, etc.)	31	16.5%
Search engine (Google, Yahoo, Bing, etc.)	44	23.4%
Personal finances (banking, bill paying, etc.)	5	2.7%
Entertainment (music, movies, video games, etc.)	10	5.3%
Shopping or auctions (eBay, Amazon, etc.)	17	9.0%
Personal communication (email, voice over IP, etc.)	5	2.7%
<b>Experience with Technology</b>		
Absolutely no experience	2	1.1%
Somewhat no experience	9	4.8%
Slightly no experience	18	9.6%
Neutral experience	46	24.4%
Slightly expert experience	67	35.6%
Somewhat expert experience	34	18.1%
Absolutely expert experience	12	6.4%

Two types of analyses were conducted to assess for any difference between the two recruitment locations: frequencies and percentages as well as a one-way analysis of variance (ANOVA). The population was divided into two groups. This research study compared the two groups: Group A and Group B. Group A included individuals from a public place of worship within the Southeastern United States. Group B included individuals from multiple public places of business (i.e., restaurants, medical offices, etc.). Group A included 108 or 57.4% individuals of a public place of worship. Group B included 80 or 42.6% individuals from public places of business. Details of the demographics of the population of each group are presented in Table 21.

Table 21

*Descriptive Statistics for Each Group in the Population*

Item	Group A (N=108)		Group B (N=80)	
	Frequency	Percentage (%)	Frequency	Percentage (%)
<b>Gender</b>				
Male	48	44.4%	33	41.2%
Female	60	55.6%	47	58.8%
<b>Age</b>				
18 or 19 years	3	2.8%	8	10.0%
20 to 24 years	9	8.3%	12	15.0%
25 to 34 years	20	18.5%	21	26.3%
35 to 44 years	12	11.1%	15	18.8%
45 to 54 years	19	17.6%	14	17.5%
55 to 64 years	29	26.9%	7	8.7%
65 or older	16	14.8%	3	3.7%
<b>Academic Level</b>				
High school diploma	34	31.5%	22	27.5%
College degree	49	45.4%	41	51.2%
Graduate degree	17	15.7%	13	16.3%
Other	8	7.4%	4	5.0%
<b>Job Function</b>				
Administrative staff	23	21.3%	15	18.8%
Managerial	11	10.2%	7	8.7%
Executive	4	3.7%	4	5.0%
Operations	2	1.9%	7	8.7%
Physical security	1	0.9%	1	1.3%
Information Technology	5	4.6%	5	6.3%
Technical Services	5	4.6%	0	0.0%
Other	57	52.8%	41	51.2%
<b>Accessing the Internet</b>				
0 to 5 hours	6	5.6%	4	5.0%
6 to 10 hours	29	26.9%	13	16.3%
11 to 15 hours	13	12.0%	6	7.5%
16 to 20 hours	12	11.1%	7	8.7%
21 to 25 hours	13	12.0%	10	12.5%
26 to 30 hours	7	6.5%	14	17.5%
31 or more hours	28	25.9%	26	32.5%



Table 21

*Descriptive Statistics for Each Group in the Population (Cont.)*

Item	Group A (N=108)		Group B (N=80)	
	Frequency	Percentage (%)	Frequency	Percentage (%)
<b>Primary Internet Activity</b>				
Work related tasks	41	38.0%	35	43.8%
Social network (Facebook, Twitter, etc.)	28	25.9%	16	20.0%
Search engine (Google, Yahoo, Bing, etc.)	18	16.7%	13	16.3%
Personal finances (banking, bill paying, etc.)	7	6.5%	3	3.7%
Entertainment (music, movies, video games, etc.)	7	6.5%	10	12.5%
Shopping or auctions (eBay, Amazon, etc.)	5	4.6%	0	0.0%
Personal communication (email, voice over IP, etc.)	2	1.8%	3	3.7%
<b>Experience with Technology</b>				
Absolutely no experience	2	1.8%	0	0.0%
Somewhat no experience	6	5.6%	3	3.7%
Slightly no experience	13	12.0%	5	6.3%
Neutral experience	29	26.9%	17	21.3%
Slightly expert experience	33	30.6%	34	42.5%
Somewhat expert experience	16	14.8%	18	22.5%
Absolutely expert experience	9	8.3%	3	3.7%

In addition, a one-way ANOVA was conducted to assess the statistical significant mean differences for each individual skill, skill categories, and overall CSI between those completing the MyCyberSkills™ iPad app prototype at a public place of worship and those that completed the prototype at a public place of business. The groups were analyzed by using descriptive statistics to calculate the means and standard deviations.

Table 22 provides the means and standard deviations for each group.

With a mean of 80.6%, Group A (members of a public place of worship) participants appeared most skilled in the preventing the leaking of confidential information (SK<sub>1</sub>). Moreover, the participants appeared least skilled in the preventing malware via email (SK<sub>5</sub>) with a mean of 46.3%. When comparing the means of the three categories, the mean of the malware category was the lowest at 51.5%. The mean of the PII category was 57.3% and the WIS category appeared with the highest mean of 73.2%. Thus, presenting a mean difference of 21.7% between the malware and WIS categories. Furthermore, the overall CSI mean was 60.4%. Figure 8 presents a visualization of the means of the individual skills and the skill categories sorted from highest to lowest along with the overall CSI for Group A.

Table 22

*Means and Standard Deviations for Each Group of the Population*

Item	Group A (N=108)		Group B (N=80)	
	Mean	Standard Deviation	Mean	Standard Deviation
SK <sub>1</sub> Leak Confidential Info	0.806	0.132	0.823	0.154
SK <sub>2</sub> Malware via Non-Secure Web	0.491	0.193	0.495	0.187
SK <sub>3</sub> PII Theft via Non-Secure Web	0.467	0.292	0.506	0.307
SK <sub>4</sub> PII Theft via email	0.600	0.192	0.596	0.209
SK <sub>5</sub> Malware via email	0.463	0.188	0.487	0.181
SK <sub>6</sub> Credit Card Theft via Non-Secure Web	0.592	0.152	0.565	0.169
SK <sub>7</sub> USB Exploits	0.685	0.180	0.606	0.198
SK <sub>8</sub> Password Exploits	0.703	0.174	0.754	0.174
SK <sub>9</sub> PII Theft via Social Network	0.652	0.217	0.615	0.213
WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	0.732	0.110	0.728	0.131
Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	0.515	0.114	0.516	0.120
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	0.573	0.152	0.572	0.173
Overall CSI	0.604	0.091	0.605	0.111

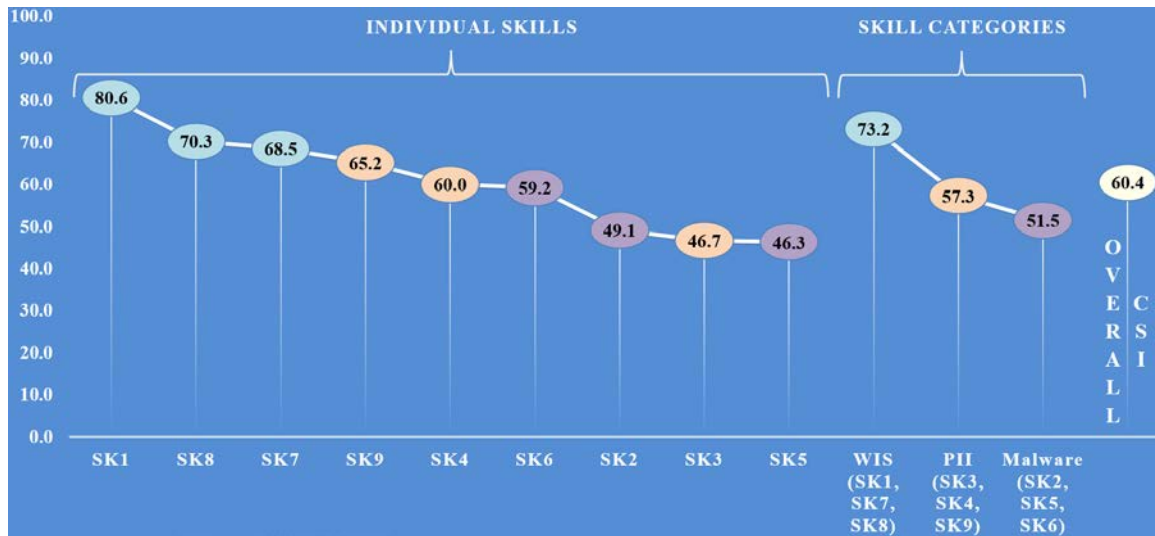


Figure 8. Means of the Individual Skills, Skill Categories, and Overall CSI for Group A (Members of Public Place of Worship) (N=108)

Group B (members of public places of business) participants also appeared most skilled in the preventing the leaking of confidential information (SK<sub>1</sub>) with a mean of 82.3%. Moreover, the participants appeared least skilled in the preventing malware via email (SK<sub>5</sub>) with a mean of 48.8%. When comparing the means of the three categories, the mean of the malware category was the lowest at 51.6%. The mean of the PII category was 57.3% and the WIS category appeared with the highest mean of 72.8%. Thus, presenting a mean difference of 21.2% between the malware and WIS categories. Furthermore, the overall CSI mean was 60.5%. Figure 9 presents a visualization of the means of the individual skills and the skill categories sorted from highest to lowest along with the overall CSI for Group B.



Figure 9. Means of the Individual Skills, Skill Categories, and Overall CSI for Group B (Members of Public Places of Businesses) (N=80)

Using SPSS to calculate the ANOVAs for each individual skill, skill category, and overall CSI by recruitment location, a significance difference,  $F(1, 186) = 8.038, p = 0.005$ , was demonstrated on SK<sub>7</sub>: Preventing information system compromise via USB or storage drive/device exploitations between Group A and Group B participants. Although no significant difference,  $F(1, 186) = 3.867, p = 0.050$ , was demonstrated on SK<sub>8</sub>: Preventing unauthorized information system access via password exploitations, additional research involving this skill is needed. Skills one, two, three, four, five, six, and nine had no significant difference between groups with each a  $p > 0.25$ . No significant differences were demonstrated on the malware,  $F(1, 186) = 0.000, p = 0.987$ , PII,  $F(1, 186) = 0.000, p = 0.989$ , and WIS,  $F(1, 186) = 0.046, p = 0.830$ . Furthermore, no significant difference,  $F(1, 186) = 0.005, p = 0.942$ , was demonstrated on overall CSI between each recruitment location. Table 23 provides an overview of the mean square scores and ANOVA results.

Table 23

*ANOVA Results for Each Recruitment Location (N=188)*

Item	df	Mean Square between Groups	ANOVA			
			F	Sig.		
SK <sub>1</sub> Leak Confidential Info	1	0.012	0.635	0.426		
SK <sub>2</sub> Malware via Non-Secure Web	1	0.000	0.014	0.906		
Individual Skills	SK <sub>3</sub> PII Theft via Non-Secure Web	1	0.070	0.786	0.376	
	SK <sub>4</sub> PII Theft via email	1	0.000	0.014	0.903	
	SK <sub>5</sub> Malware via email	1	0.026	0.778	0.378	
	SK <sub>6</sub> Credit Card Theft via Non-Secure Web	1	0.032	1.281	0.259	
	SK <sub>7</sub> USB Exploits	1	<b>0.285</b>	<b>8.038</b>	<b>0.005</b>	**
	SK <sub>8</sub> Password Exploits	1	0.118	3.867	0.050	
	SK <sub>9</sub> PII Theft via Social Network	1	0.061	1.312	0.253	
	Categories	WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	1	0.000	0.046	0.830
		Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	1	0.000	0.000	0.987
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )		1	0.000	0.000	0.989	
Overall CSI	1	0.000	0.005	0.942		

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

Reviewing the individual skills, skill categories, and overall CSI, this study determines that preventing information system compromise via USB or storage drive/device exploitations (SK<sub>7</sub>) has the most significant difference by recruitment location compared to the other skills. However, when SK<sub>7</sub> was combined with SK<sub>1</sub> and SK<sub>8</sub> to form the WIS category, there was no significant difference between recruitment locations. Furthermore, the overall CSI has no significant difference between groups.

#### *Data Analysis*

After the pre-analysis data screening was performed, the descriptive analysis for the population (N=188) was conducted. To answer RQ5, the useful responses were analyzed using descriptive statistics to calculate the skill categories (e.g., malware, PII, &

WIS) as well as overall CSI means and standard deviations by age, gender, educational level, job function, primary activity, hours accessing the Internet, and experience using technology. It was noted the minimum CSI score was 28.5%, maximum score was 85.5%, and the overall CSI mean was 60.5%. A review of the means for the malware, PII, and WIS categories as well as overall CSI by age group revealed that higher means were achieved by those in the 45 to 54 years of age group. Furthermore, those 25 to 34 years of age had the second highest means in PII, WIS and overall CSI. Figure 10 presents the means and standard deviations of the malware and PII skills categories for each age group. Whereas, Figure 11 presents the means and standard deviations of the WIS skill category and overall CSI for each age group. Next ANOVAs were conducted to assess if there were differences between the skill categories of malware, PII, and WIS, as well as overall CSI by age groups. Results of the ANOVA by the WIS category were significant,  $F(6, 181) = 2.218, p = 0.043$ , suggesting there were differences in age groups by WIS. The ANOVA conducted for the malware category was not significant,  $F(6, 181) = 1.422, p = 0.208$ . Results were similar for the PII category,  $F(6, 181) = 0.972, p = 0.445$ . The ANOVA conducted for overall CSI was also not significant,  $F(6, 181) = 1.478, p = 0.187$ , suggesting there were no differences in overall CSI by age group. Table 24 presents the ANOVA results of the three categories as well as overall CSI by age group.

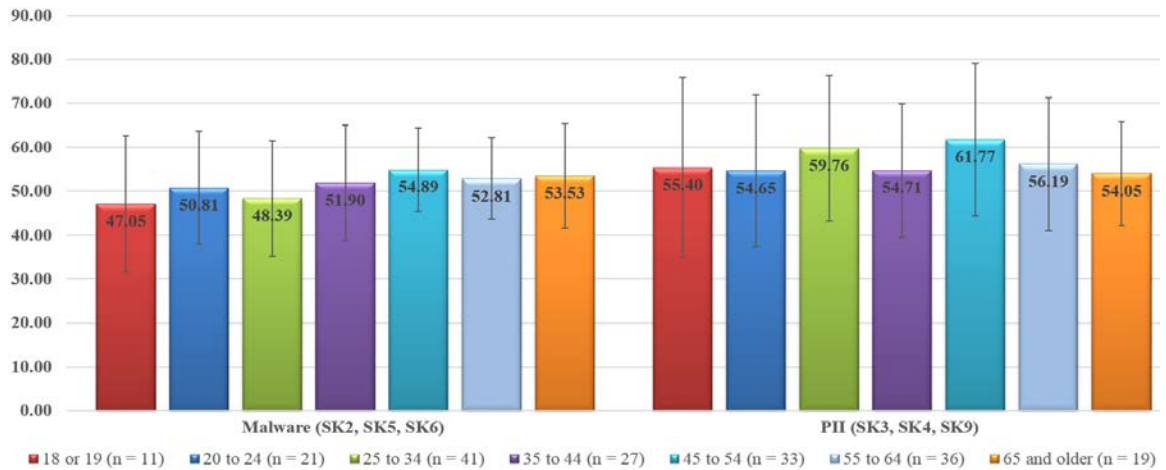


Figure 10. Means and Standard Deviations of Malware and PII Skills Categories by Age Group (N=188)

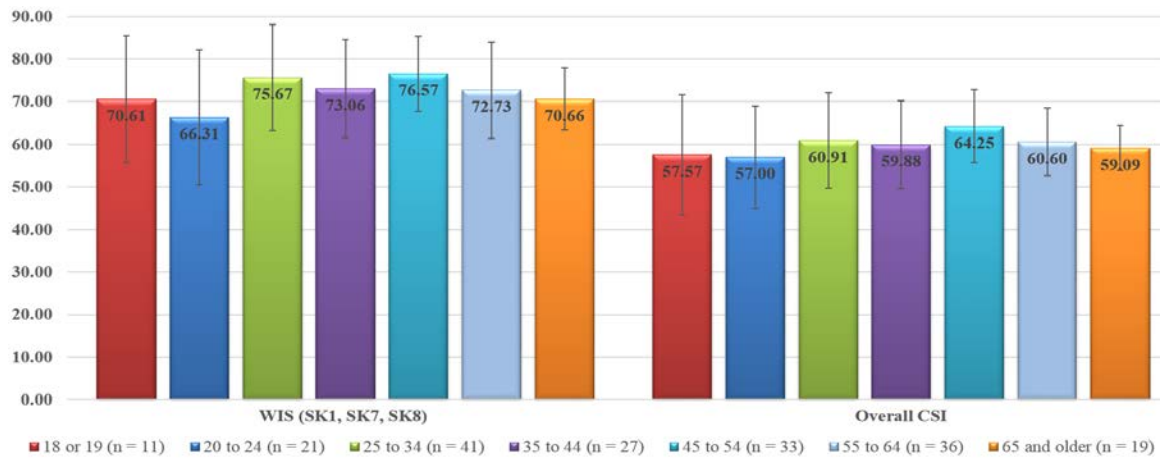


Figure 11. Means and Standard Deviations of WIS Skills Category and Overall CSI by Age Group (N=188)

Table 24

ANOVA Results for Age Group (N=188)

Item	df	ANOVA		
		Mean Square between Groups	F	Sig.
Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	6	0.019	1.422	0.208
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	6	0.025	0.972	0.445
WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	<b>6</b>	<b>0.030</b>	<b>2.218</b>	<b>0.043</b> *
Overall CSI	6	0.014	1.478	0.187

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

The means of malware, PII, and WIS categories as well as overall CSI were lower for females than males. Figure 12 presents the means and standard deviations of the malware, PII, and WIS skills categories as well as overall CSI by gender. One-way ANOVAs were conducted to assess if there were differences between the skill categories and overall CSI by gender. Results of the ANOVA for the WIS category was significant,  $F(1, 186) = 5.872, p = 0.016$ , suggesting there were differences in WIS by gender. The ANOVA conducted for the malware category was not significant,  $F(1, 186) = 0.224, p = 0.636$ . Results were similar for the PII category,  $F(1, 186) = 1.442, p = 0.231$ . The ANOVA conducted for overall CSI was also not significant,  $F(1, 186) = 3.158, p = 0.077$ , suggesting there were no differences in overall CSI by gender. Table 25 presents the ANOVA results for the malware, PII, and WIS categories as well as overall CSI by gender.

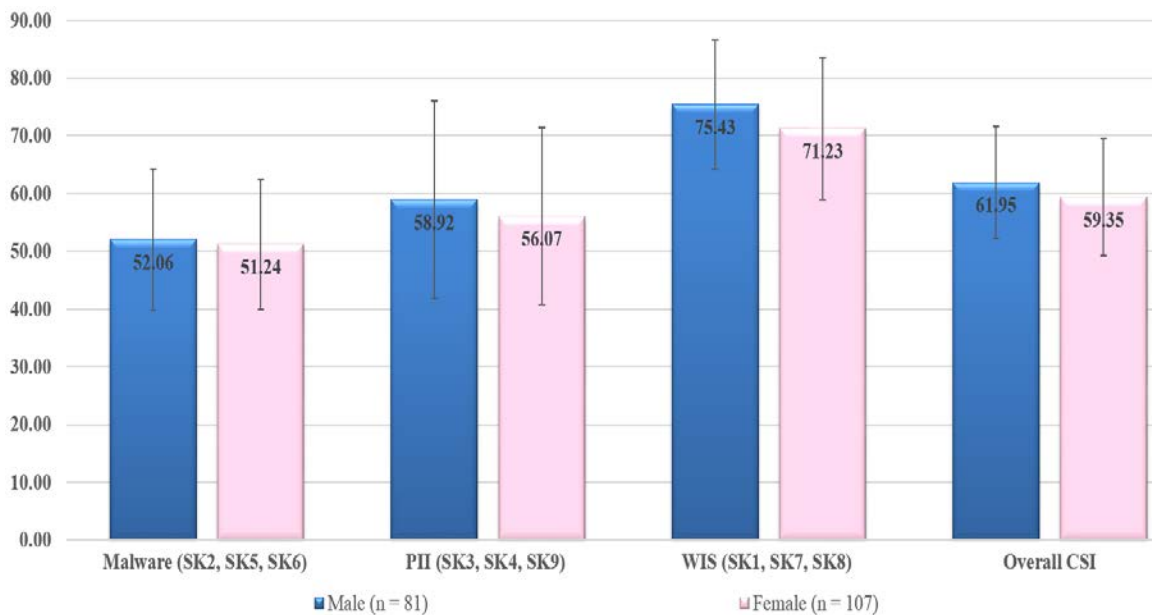


Figure 12. Means and Standard Deviations of Skill Categories and Overall CSI by Gender (N=188)



Table 25

*ANOVA Results for Gender (N=188)*

<b>Item</b>	<b>df</b>	<b>Mean Square between Groups</b>	<b>ANOVA</b>	
			<b>F</b>	<b>Sig.</b>
Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	1	0.003	0.224	0.636
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	1	0.037	1.442	0.231
WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	<b>1</b>	<b>0.081</b>	<b>5.872</b>	<b>0.016</b> *
Overall CSI	1	0.031	3.158	0.077

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

A review of the calculated means for administrative staff revealed malware, PII, WIS and overall CSI percentages attained were higher than those in managerial job functions. Figure 13 presents the means and standard deviations of the malware and PII skills categories by job function. Furthermore, Figure 14 presents the means and standard deviations of the WIS skills category and overall CSI by job function. One-way ANOVAs were conducted to assess if there were differences between the skill categories and overall CSI by job function. Results of the ANOVA for the overall CSI was not significant,  $F(7, 180) = 1.690$ ,  $p = 0.113$ , suggesting there were no significant difference in overall CSI by job function. The ANOVA conducted for the malware category was also not significant,  $F(7, 180) = 1.262$ ,  $p = 0.271$ . Results were similar for the PII category,  $F(7, 180) = 1.683$ ,  $p = 0.115$ . The ANOVA conducted for WIS was also not significant,  $F(7, 180) = 1.128$ ,  $p = 0.347$ , suggesting there were no differences in WIS by job function. Table 26 presents the ANOVA results of the malware, PII, WIS, and overall CSI by job function.

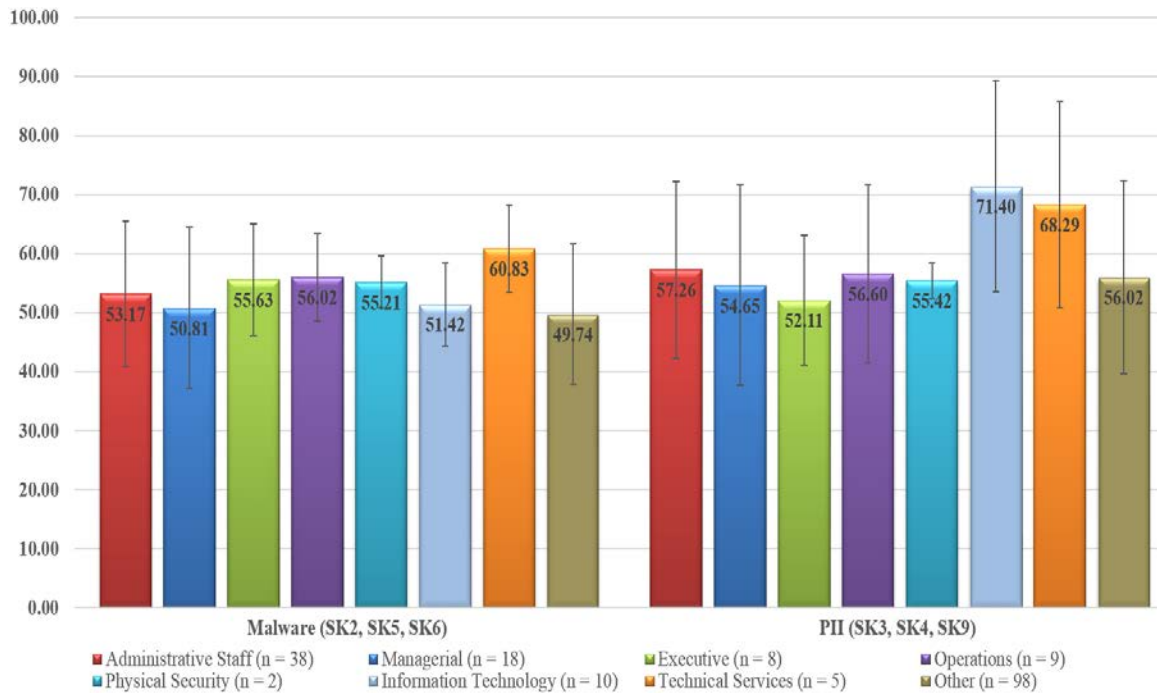


Figure 13. Means and Standard Deviations of Malware and PII Skills Categories by Job Function (N=188)

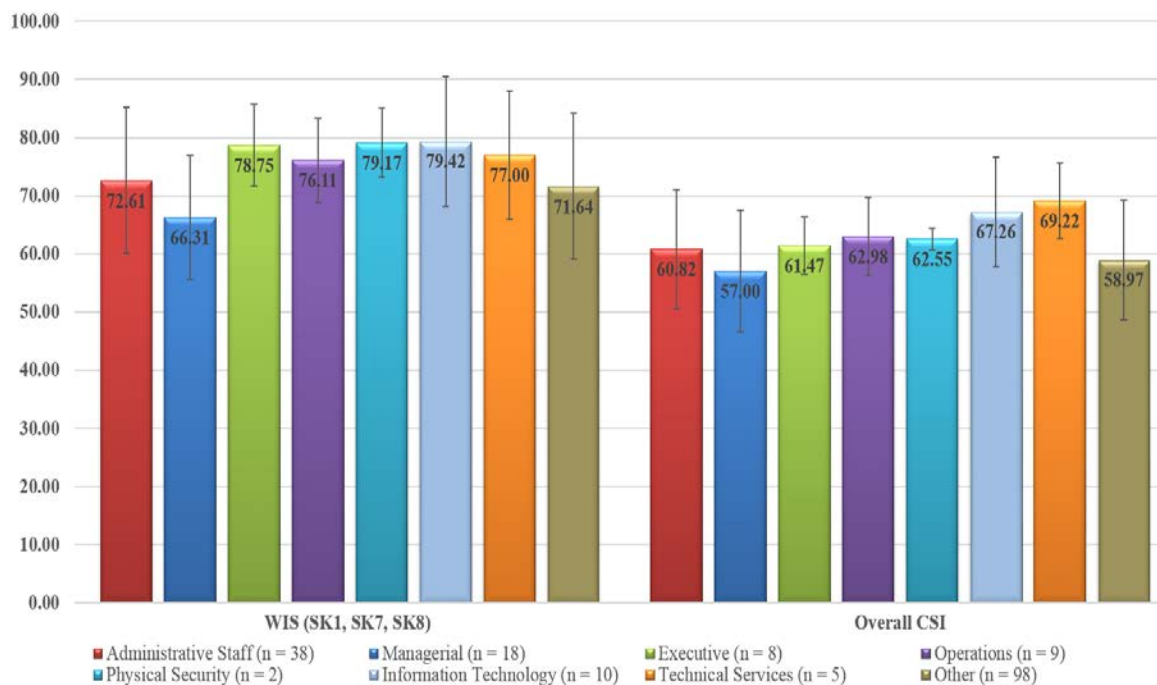


Figure 14. Means and Standard Deviations of WIS Skills Category and Overall CSI by Job Function (N=188)

Table 26

*ANOVA Results for Job Function (N=188)*

Item	df	Mean Square between Groups	ANOVA	
			F	Sig.
Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	7	0.017	1.262	0.271
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	7	0.042	1.683	0.115
WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	7	0.016	1.128	0.347
Overall CSI	7	0.016	1.690	0.113

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

The PII and WIS skills categories as well as the overall CSI means of those accessing the Internet six to 10 hours weekly were nearly 4.5% to 12.2% higher than those accessing the Internet any other times. Moreover, those participants accessing the Internet 11 to 15 hours weekly scored nearly 7.0% higher than the other groups. Figure 15 presents the means and standard deviations of the malware and PII skills categories by the number of hours participants accessed the Internet. Furthermore, Figure 16 presents the means and standard deviations of the WIS skills category and overall CSI by the number of hours the participants accessed the Internet. One-way ANOVAs were conducted to assess if there were differences between the malware, PII, WIS categories and overall CSI by the number of hours participants accessed the Internet. Results of the ANOVA for the overall CSI was not significant,  $F(6, 181) = 1.663$ ,  $p = 0.132$ , suggesting there were no significant difference in overall CSI by the number of hours accessing the Internet. The ANOVA conducted for the malware category was also not significant,  $F(6, 181) = 1.099$ ,  $p = 0.364$ . Results were similar for the PII category,  $F(6, 181) = 1.939$ ,  $p = 0.076$ . The ANOVA conducted for WIS was also not significant,  $F(6, 181) = 0.648$ ,  $p = 0.691$ , suggesting there were no differences in WIS by the number of hours a participant

accessed the Internet. Table 27 presents the ANOVA results of the skill categories as well as overall CSI by the number of hours participants accessed the Internet.

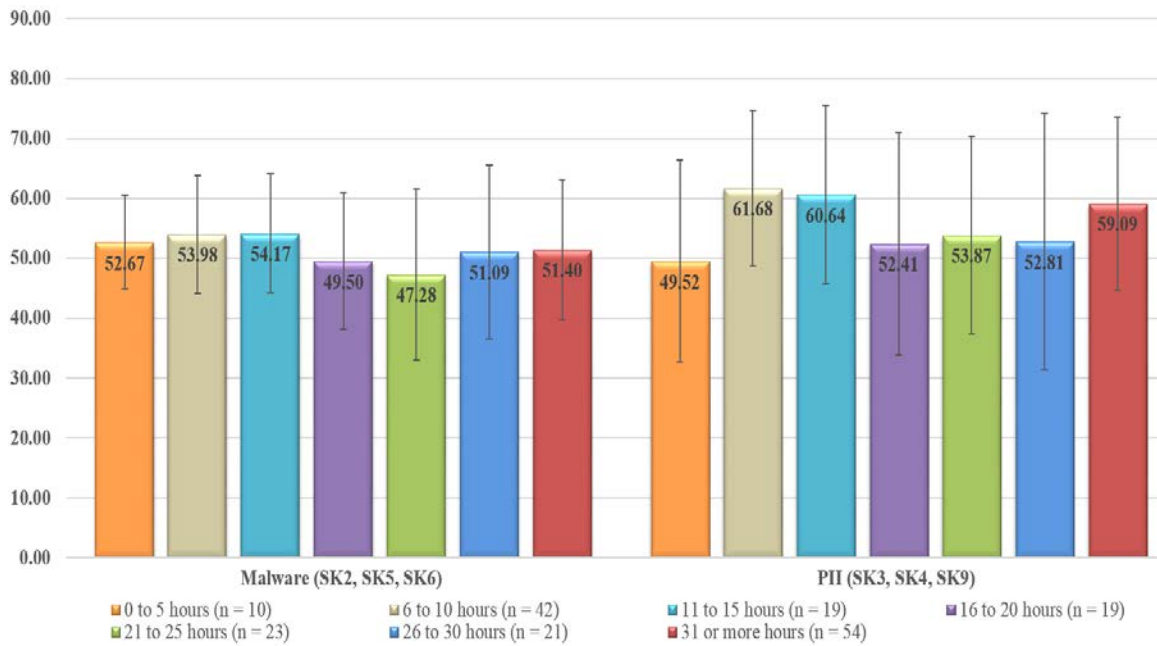


Figure 15. Means and Standard Deviations of Malware and PII Skills Categories by Hours Online (N=188)

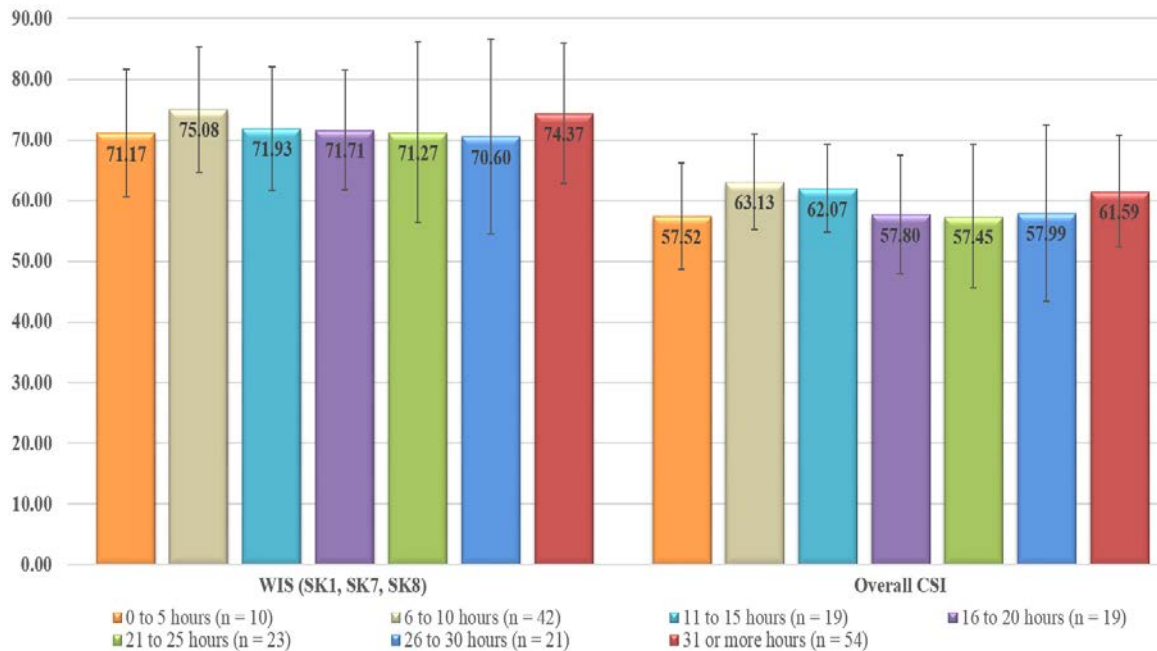


Figure 16. Means and Standard Deviations of WIS Skills Category and Overall CSI by Hours Online (N=188)

Table 27

*ANOVA Results for Hours Accessing the Internet (N=188)*

Item	df	Mean Square between Groups	ANOVA	
			F	Sig.
Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	6	0.014	1.099	0.364
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	6	0.049	1.939	0.076
WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	6	0.009	0.648	0.691
Overall CSI	6	0.016	1.663	0.132

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

Review of the means for the malware, PII, and WIS categories as well as overall CSI by primary activity revealed approximately 8.0% between the highest and lowest for each category. The means for overall CSI by primary activity varied from highest to lowest nearly 2.5 percentage points. Figure 17 presents the means and standard deviations of the malware and PII skills categories by primary activity. Whereas, Figure 18 presents the means and standard deviations of the WIS skills category and overall CSI by primary activity. One-way ANOVAs were conducted to assess if there were differences between the malware, PII, WIS skills categories, and overall CSI by primary activity. Results of the ANOVA for the overall CSI was not significant,  $F(6, 181) = 0.304, p = 0.934$ , suggesting there were no significant difference in overall CSI by primary activity. The ANOVA conducted for the malware category was also not significant,  $F(6, 181) = 0.969, p = 0.447$ . Results were similar for the PII category,  $F(6, 181) = 0.537, p = 0.779$ . The ANOVA conducted for WIS was also not significant,  $F(6, 181) = 0.678, p = 0.667$ , suggesting there were no significant differences in WIS by primary activity. Table 28 presents the ANOVA results of the malware, PII, WIS, and overall CSI by primary activity.

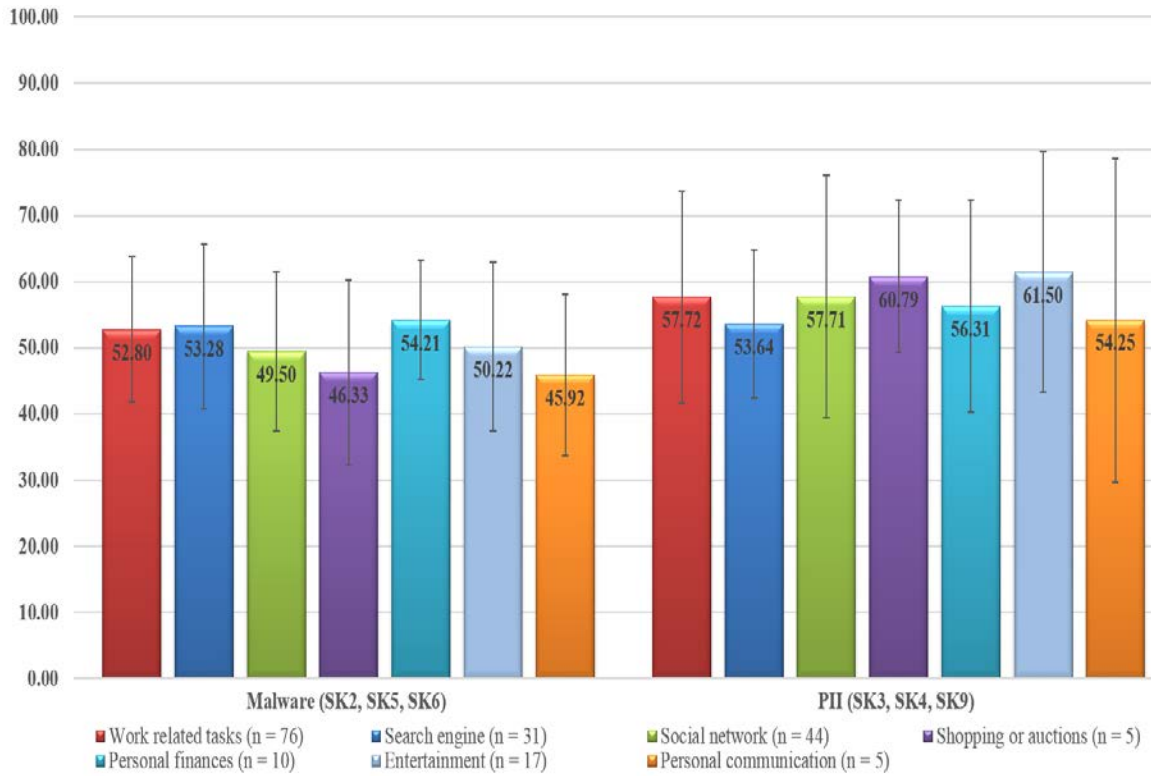


Figure 17. Means and Standard Deviations of Malware and PII Skills Categories by Primary Activity (N=188)

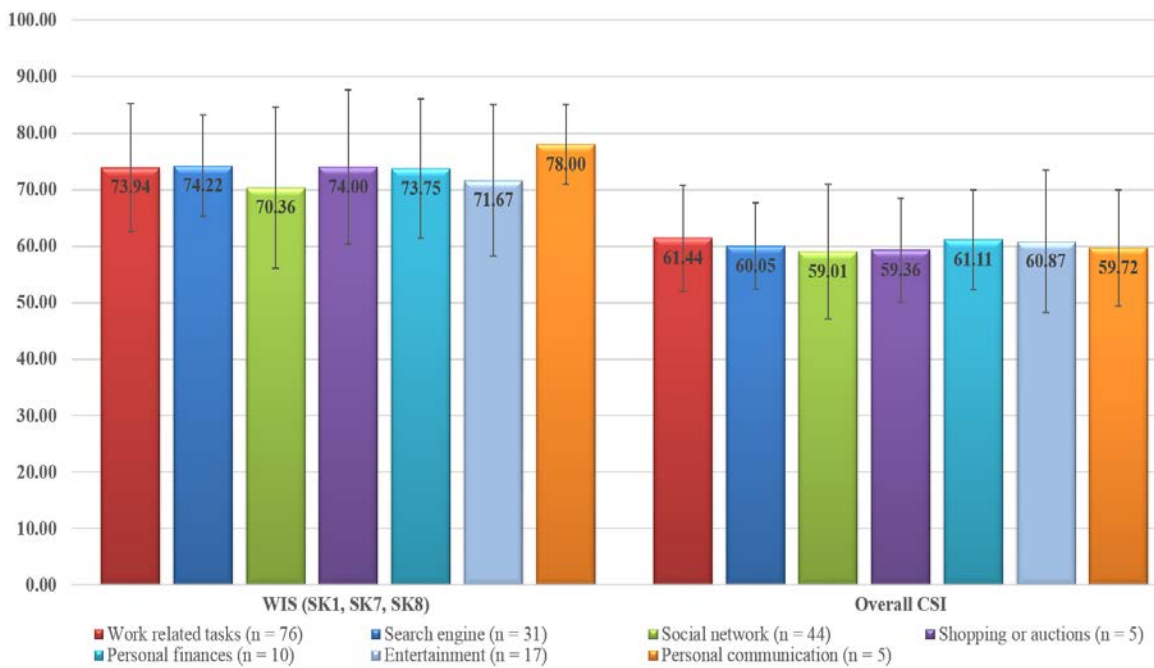


Figure 18. Means and Standard Deviations of WIS Skills Category and Overall CSI by Primary Activity (N=188)

Table 28

*ANOVA Results for Primary Activity (N=188)*

Item	df	Mean Square between Groups	ANOVA	
			F	Sig.
Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	6	0.013	0.969	0.447
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	6	0.014	0.537	0.779
WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	6	0.009	0.678	0.667
Overall CSI	6	0.003	0.304	0.934

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

A review of the means for the malware and WIS categories as well as overall CSI incremented with education. Furthermore, those with ‘other’ education had the highest means for malware, WIS, and overall CSI. The PII category means revealed those with college educations had higher percentages than the remaining educational groups. Figure 19 presents the means and standard deviations of the malware, PII, and WIS skills categories as well as and overall CSI by education. To assess if there were differences between the malware, PII, and WIS skills categories as well as the overall CSI by primary activity, ANOVAs were conducted. Results of the ANOVA revealed the overall CSI by education was significant,  $F(3, 184) = 2.670$ ,  $p = 0.048$ , suggesting there were significant differences in overall CSI by education. The ANOVA conducted for the malware category was not significant,  $F(3, 184) = 2.461$ ,  $p = 0.064$ . Results were similar for the PII category,  $F(3, 184) = 0.937$ ,  $p = 0.423$ . The ANOVA conducted for WIS was also not significant,  $F(3, 184) = 2.000$ ,  $p = 0.115$ , suggesting there were no significant differences in WIS by education. Table 29 presents the ANOVA results of the malware, PII, WIS, and overall CSI by education.

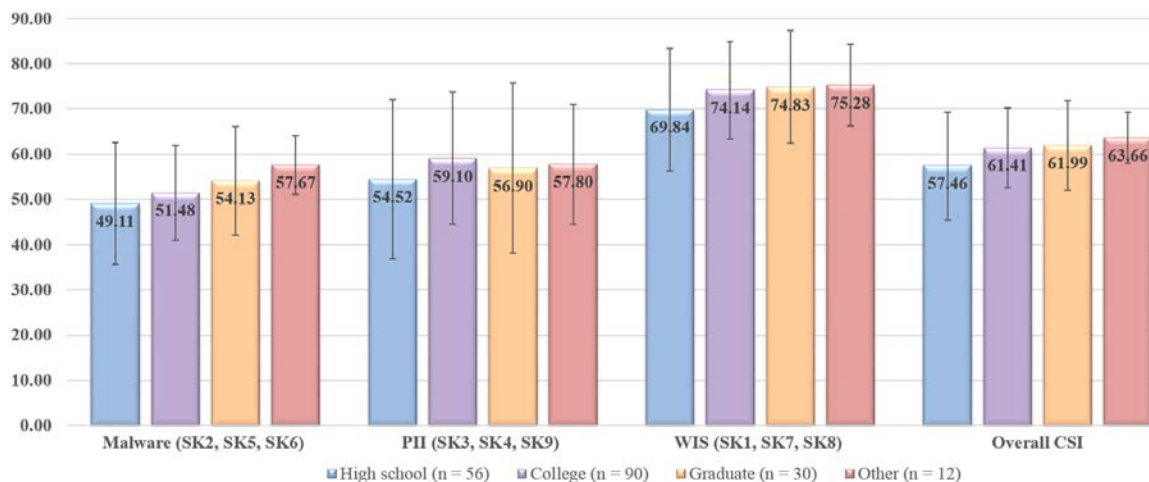


Figure 19. Means and Standard Deviations of the Skill Categories and Overall CSI by Education (N=188)

Table 29

ANOVA Results for Education (N=188)

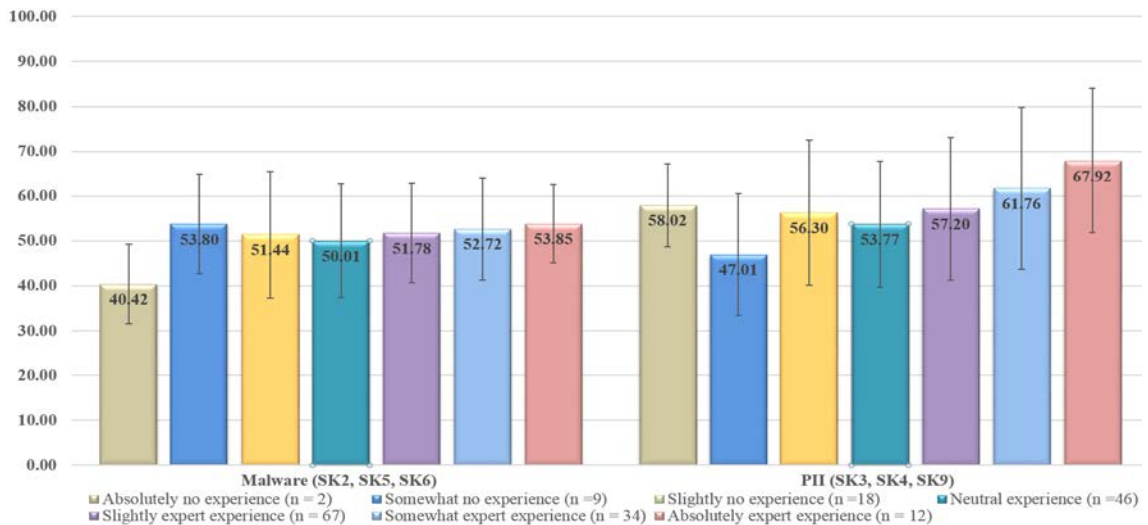
Item	df	Mean Square between Groups	ANOVA	
			F	Sig.
Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	3	0.032	2.461	0.064
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	3	0.024	0.937	0.423
WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	3	0.028	2.000	0.115
Overall CSI	3	<b>0.025</b>	<b>2.670</b>	<b>0.048</b> *

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

The means for the skill categories and overall CSI incremented as the level of experience identified by the participants increased. Moreover, the means of the malware and PII skills categories as well as the overall CSI revealed those reporting slightly no experience using technology had higher means than those reporting neutral experience using technology. Figure 20 presents the means and standard deviations of the malware and PII skills categories by the participants' experience using technology. Whereas, Figure 21 presents the means and standard deviations of the WIS skills category and



overall CSI. ANOVAs were conducted to assess if there were differences between the malware, PII, and WIS categories as well as overall CSI by the participants' experience using technology. Results of the ANOVA for the overall CSI was significant,  $F(6, 181) = 2.361, p = 0.032$ , suggesting there was a significant difference in overall CSI by the participants' experience using technology. Results were similar for the PII category,  $F(6, 181) = 2.387, p = 0.030$ . The ANOVA conducted for the malware category was not significant,  $F(6, 181) = 0.625, p = 0.709$ . Furthermore, the ANOVA conducted for WIS was also not significant,  $F(6, 181) = 1.746, p = 0.112$ , suggesting there were no significant differences in WIS between groups. Table 30 presents the ANOVA results of the malware, PII, WIS, and overall CSI by the participants' experience using technology.



*Figure 20. Means and Standard Deviations of Malware and PII Skills Categories by Experience Using Technology (N=188)*

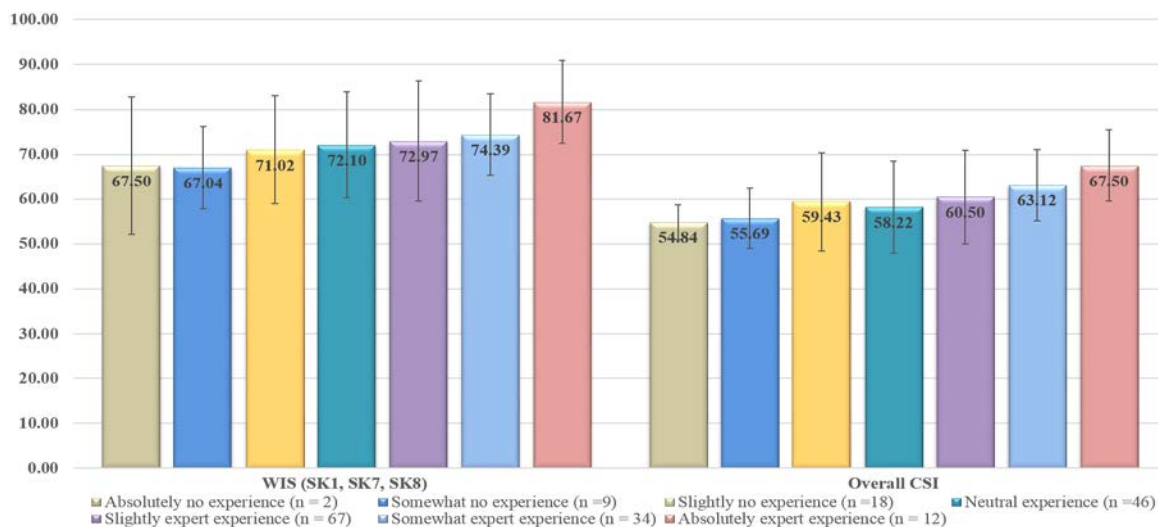


Figure 21. Means and Standard Deviations of WIS Skills Category and Overall CSI by Experience Using Technology (N=188)

Table 30

ANOVA Results for Experience Using Technology (N=188)

Item	df	Mean Square between Groups	ANOVA	
			F	Sig.
Malware (SK <sub>2</sub> , SK <sub>5</sub> , & SK <sub>6</sub> )	6	0.008	0.625	0.709
PII (SK <sub>3</sub> , SK <sub>4</sub> , & SK <sub>9</sub> )	6	<b>0.059</b>	<b>2.387</b>	<b>0.030</b> *
WIS (SK <sub>1</sub> , SK <sub>7</sub> , & SK <sub>8</sub> )	6	0.024	1.746	0.112
Overall CSI	6	<b>0.022</b>	<b>2.361</b>	<b>0.032</b> *

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

As indicated from the results above, the fifth research question and goal of this study was to empirically assess if there are significant differences on CSI based on age, education level, gender, job function, and experience using technology. As seen in the results, job function, the number of hours accessing the Internet, and primary activity completed while accessing the Internet were found to have no significant differences. Only a few items showed a significant difference on CSI. These included experience using technology for PII, gender and age group for WIS, as well as educational level and

experience using technology for overall CSI. Overall, a large majority showed no significant differences on the skill categories and overall CSI.

### **Summary**

In this chapter, the results of the study were presented. First, the chapter began with Phase One of the research study, which involved qualitative research conducted through a literature review in order to develop a new survey instrument for eliciting input from the expert panel. The results of both surveys using the Delphi technique were discussed. Furthermore, the discussion included the elicitation of the expert panel to confirm the platform independent cybersecurity threats and related skills, along with the weight allocations that were used to calculate the CSI. Next, Phase Two of the study was discussed, which involved the qualitative and quantitative research conducted to operationalize the novel CSI into the MyCyberSkills™ iPad app prototype. The discussion encompassed the engagement of the expert panel to validate the prototype using the Delphi technique and the pilot-test completed to ensure the validity and reliability of the developed prototype. The chapter concluded with Phase Three that presented the data analysis and results of the MyCyberSkills™ prototype.

The five goals of this study were attained using a three-phased approach: the first specific goal of this research study was to identify a set of cybersecurity skills pinpointed by SMEs as those that can help mitigate critical vulnerabilities. The second specific goal of this research study was to develop a set of tasks that could be categorized and linked to the SMEs identified set of cybersecurity skills. The third specific goal of this research study was to develop a benchmarking index to hierarchically aggregate the set of SMEs

identified cybersecurity skills using observable hands-on tasks. The first three goals were met with the development of the MyCyberSkills™ prototype, which operationalized the single benchmarking Cybersecurity Skills Index ranging from zero to 100. The fourth specific goal of this research study was to assess the scores of the CSI benchmarking index for the aggregated set of SMEs identified cybersecurity skills of a group of 188 non-IT professionals. This goal was met as presented in Table 19 and Table 22.

The last and fifth goal was to measure if there were any significant differences to CSI based on age, gender, educational level, job function, or experience using technology. To begin the analysis, a pre-analysis of the data for screening data purpose was performed. The screening data resulted in the elimination of 57 responses resulting in 188 usable cases. A demographic analysis was made to examine more information about the population of this study. Details of the demographics of the populations are presented in Table 20.

This study performed one-way ANOVAs to analyze if there were any significant differences to CSI based on age, gender, educational level, job function, or experience with technology. Experience using technology for PII, gender and age group for WIS, as well as educational level and experience using technology for overall CSI had significant differences with a  $p < 0.05$ . The results of the ANOVA as presented in Table 24, Table 25, Table 26, Table 29, and Table 30 met the last and fifth goal of this research study.

## Chapter 5

### Conclusions, Implications, Recommendations, and Summary

#### **Conclusions**

Because cyber-attacks have intensified over time, organizations are increasing the priority of cybersecurity skills due to substantial financial and information losses caused by insiders (APWG, 2016; PwC, 2016). Thus, the main goal of this research study was to design, develop, and empirically test a set of hands-on tasks set to measure the cybersecurity skills level of non-IT professionals. This study built on prior research that defined cybersecurity skills as (i.e., preventing malware, PII theft, & WIS breaches) the combination of an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS security to mitigate cyber-attacks (Axelrod, 2006; Boyatzis & Kolb, 1991; Choi et al., 2015). This research study achieved the five goals with a three-phased approach. First, an expert panel using the Delphi expert methodology was used to design and validate the scenarios-based, hands-on benchmarking index for measuring cybersecurity skills (Ramim & Lichvar, 2014). Second, the previously developed and validated scenarios-based, hands-on benchmarking index was operationalized into an iPad app prototype that was used to assess the cybersecurity skill of non-IT professionals. Last, the previously developed and validated iPad app prototype was used to empirically assess the hands-on cybersecurity skills of

non-IT professionals based on demonstrated skills on cybersecurity tasks and document the results of the measure.

## **Discussion**

The first result of this study was the development of a validated and reliable app set to measure the observable cybersecurity skills of non-IT professionals. Furthermore, the second result of this study indicated there was a significant difference in the cybersecurity skills level of non-IT professionals based on educational level and experience using technology. Moreover, there was a significant difference in WIS breaches based on gender and age group. In addition, there was a significant difference in PII theft based on experience using technology. No significant difference was found in CSI, malware, PII theft, or WIS breaches based on a non-IT professional's job function, number of hours accessing the Internet, or primary activity completed while accessing the Internet.

Overall, not one participant demonstrated 100% skilled in all of the cybersecurity tasks. This suggests a need for cybersecurity skilled non-IT professionals and the MyCyberSkills™ tool to help mitigate the opportunities for organizational information vulnerabilities and breaches. Third, the results indicated that higher levels of education increased a non-IT professional's demonstrated cybersecurity skills. Fourth, as experience using technology increased, the non-IT professionals demonstrated improved skills on cybersecurity tasks. Fifth, the results of those in administrative staff positions demonstrated higher cybersecurity skills than those in managerial job functions. Last, those 18 to 24 as well as 65 and older demonstrated less cybersecurity skills than those

ages 20 to 64. This insinuates non-IT professionals entering or exiting the workforce may be at a higher risk of falling for a cyber-attack.

Limitations were noted with this study. The first limitation of this study is the generalizability of the specific index values (not the weights) due to the sample used. It is expected that the SMEs composed hierarchical weights will be generalized in the future, but over time, the use of the CSI on different organizations may gather different values. Next, the collected data were limited to several organizations within the Southeastern United States. While the sample size of 188 non-IT professionals is valid, further studies conducted can recruit participants from a wider community approach to increase validation of the results and generalizability. Furthermore, the scenarios-based, hands-on skills measured are another limitation. As new cyber threats arise, other scenarios-based, hands-on tasks can be developed and incorporated into the CSI for revising the MyCyberSkills™ prototype used in this study. Finally, the quantity of time needed to complete the MyCyberSkills™ prototype was another limitation.

## **Implications**

The outcomes of this study contributed notably to the body of knowledge, and has several implications for providing researchers and practitioners insight into the cybersecurity skills level of non-IT professionals. Understanding an employee's cybersecurity skills levels is critical to securing information and the systems that stores it as organizations continue to rely on the Internet for conducting their daily operations. This research study validated that the CSI benchmarking index could be used to assess the hands-on cybersecurity skills of non-IT professionals based on their demonstrated

skills on cybersecurity tasks. Furthermore, this research study provides the MyCyberSkills™ tool that can be used to assess the cybersecurity skills level of non-IT professionals within an organization. This tool could assist organizations with assessing cybersecurity skills levels to provide insight into what the organization can do to further mitigate threats due to vulnerabilities and breaches caused by non-IT professionals.

### **Recommendations and Future Research**

This study was a developmental research and outlined the research approach to design and validate the scenarios-based, hands-on benchmarking cybersecurity skills index that was used to measure the cybersecurity skills of non-IT professionals. Moreover, the inclusion of the sequential-exploratory research method within the development contributed to the goodness of data collected and validity of the results (Terrell, 2011; Wisdom & Creswell, 2013). The threats, relative skills, and weights of the hierarchical measure for observable cybersecurity skills of non-IT professionals were developed using the Delphi technique. Followed by the development of the MyCyberSkills™ iPad app prototype, which was used for collecting and analyzing data using the research plan discussed here. The findings and results of the statistical analyses were reported.

There are many areas for future research that were identified based on the results of this developmental research. First, future studies are warranted to increase the validity of the MyCyberSkills™ tool. In addition, more research is needed to take place in and outside the Southeastern United States while expanding the sample size to increase the generalizability. The second recommendation includes selection of a population with



criteria specifically for supervisors and subordinates to determine if the CSI level of a supervisor affects the CSI of a subordinate. A third recommendation for future research study could be set to determine the effects of organizational culture on the CSI level of the employees. Whereas, a fourth recommendation for future research study includes investigating the effects of behaviors (i.e., curiosity, boredom, etc.) or emotions (i.e., depression, sadness, etc.) on the CSI level of an individual. The fifth recommendation is to investigate the relationship, if any, between self-reported cybersecurity skills levels and actual demonstrated cybersecurity skills measured using the MyCyberSkills™ tool. Finally, the study could be replicated with the scenarios-based, hands-on tasks adapted into a video presentation using an audience response system.

## **Summary**

This dissertation study addressed the research problem of threats to organizational IS due to vulnerabilities and breaches caused by employees (Hovav & Gray, 2014; Jensen et al., 2014; Peha, 2013). Conducting transactions, interacting, and sharing information on the Internet are a part of everyday life. But, completing activities online does not come without its risks as well as potential for harm. Organizations, individuals, and governments continue to regularly report substantial information and financial losses due to vulnerabilities as well as breaches caused by insiders. But, when it comes to protection of corporate IS, human errors and social engineering appear to prevail in circumventing such IT protections. This research study facilitated an increase in the body of knowledge regarding non-IT professionals as it relates to their cybersecurity skills in the context of

malware, PII, and WIS related threats. Moreover, it addressed a valid problem with practical significance (Terrell, 2015).

The main goal of this research was to design, develop, and empirically test a set of hands-on tasks set to measure the cybersecurity skills level of non-IT professionals. Building on the work of Berendonk et al. (2013), Choi (2013), Morcke et al., (2013), Weigel and Hazen (2014), as well as Vance et al. (2014), this work was classified as a developmental research. Thus, it answered the call to develop a hierarchical measure of cybersecurity skills levels of non-IT professionals that addressed the problem of vulnerabilities and breaches caused by employees (Ellis & Levy, 2009; Ramim & Lichvar, 2014). Furthermore, this study sought to determine if there are any significant differences to cybersecurity skills levels based on gender, age, level of education, job function, primary online activity, hours accessing the Internet, and experience using technology. Therefore, a three-phased approach was used to meet the goals of this study and answer five research questions.

In Phase One, a panel of subject matter experts from the Florida chapter of the InfraGard, a public-private partnership between the United States Federal Bureau of Investigation (FBI)'s cyber division and private sector that focus on cybersecurity along with SMEs from other federal agencies such as the United States Secret Services' (USSS) Electronic Crimes Task Force team and industry were engaged to answer the first three research questions as follows.

RQ1: What are the specific subject matter experts (SMEs) identified set of cybersecurity skills of non-IT professionals, which address the most common organizational cybersecurity threats?

RQ2: What are the specific SMEs identified tasks that can be categorized, linked, and validated to the set of the identified cybersecurity skills?

RQ3: What are the specific SMEs identified weights of the tasks and skills that enable a validated hierarchical aggregation to the Cybersecurity Skills Index (CSI) benchmarking index?

The Delphi technique was employed for the purpose of identifying indispensable expert opinion. After an extensive literature review, Web-based questionnaires were developed for the SMEs to indicate their agreement with the non-platform independent threats, their matching skills, and their recommendation for their ranking (weight) allocation. The outcome of the two survey rounds was the development of and the relative weight allocations for the top nine non-platform independent cybersecurity, along with their respective category.

Phase Two expanded on the developed and validated comprehensive set of scenarios-based, hands-on benchmarking index from Phase One. Each skill was designed to include a group of four tasks for the purpose of identifying demonstrated skills levels as if in a real-life situation (Hovav & D'Arcy, 2012; Vance et al., 2012). Articulate Storyline 2 was then used to transform the written scenarios-based, hands-on tasks into a digital presentation. The CSI, SMEs ranked cybersecurity skills, their respective hands-on tasks, description, range, and weight as presented in Table 17 were incorporated into the design and development of the MyCyberSkills™ iPad app prototype. A panel of SMEs were then engaged to solicit qualitative and quantitative feedback on the scenarios, tasks, and scoring of the prototype. After two rounds of the Delphi technique, pilot testing was conducted to ensure the scores were recorded accurately by the prototype.

After minor revisions, the validated and reliable MyCyberSkills™ iPad app prototype was the tool used for collecting data from 188 non-IT professionals in the third phase of this study.

The third phase of this research study achieved answers to the remaining research questions. First, the highest score of the CSI benchmarking index for the aggregated set of SMEs identified cybersecurity skills of the group was 85.5%. The minimum CSI score attained was 28.5% with a mean CSI score of 60.5%. Second, there were significant differences to CSI for level of education and experience using technology. Furthermore, significant differences with a  $p < 0.05$  were identified for WIS based on gender and age group, as well as PII based on experience using technology. Third, there were no significant differences for the malware category. Finally, no significant differences to the CSI were identified for job function, the number of hours accessing the Internet, and primary online activity. The results suggest that level of education and experience using technology may make a difference on the level of vulnerabilities and breaches caused by an employee. Whereas, the type of work duties performed, the number of hours nor the activity completed online do not appear to make any difference on a non-IT professional's cybersecurity skills level.

RQ4: What are the scores of the CSI benchmarking index for the aggregated set of SMEs identified cybersecurity skills of a group of 188 non-IT professionals?

RQ5: Are there any significant differences to CSI based on age, gender, educational level, job function, primary online activity, number of hours accessing the Internet, or experience using technology?

As with any research study, this study had three main limitations. First, the set of skills combined to form the CSI is a limitation. Second, generalization of the results from this research study were cautioned as the reliability and validation of the CSI and MyCyberSkills™ tool relied on an expert panel. The expert panel, the relative weights, criteria, and measures may not be representative of the broader population. Further studies are required with other populations to increase generalizability of the results and improve the validity of the instrument. Last, the results represent data at a point in time is a limitation.

This research study made several contributions to the information security domain and body of knowledge. The study provided empirical evidence regarding the magnitude of cybersecurity skills to mitigate the risk of vulnerabilities and breaches caused by insiders. This evidence is important to academia and practitioners to assist with understanding the cybersecurity skills of non-IT professionals. Given the heightened concerns of organizations regarding cybersecurity, the results of this research study provided organizations with empirical evidence of how to measure the cybersecurity skills of their employees. Unidentified inadequate cybersecurity skills of non-IT professionals could result in substantial financial and information losses for an individual, organization, or government.

In conclusion, other researchers can use the CSI benchmarking index to assess cybersecurity skills for new populations. The MyCyberSkills™ iPad app prototype can be used as a tool by researchers and organizations to assess and provide awareness regarding cybersecurity skills. In addition, SETA programs may include the MyCyberSkills™ tool to assess and aide in the mitigation of cyber threats.

## Appendix A

### Site Approval Letter



Mark T. McQueen  
Church Business Administrator

---

A House of Hope for all generations ... a place to connect.

Nova Southeastern University  
3301 College Avenue  
Fort Lauderdale, FL 33314-7796

**Subject:** Site Approval Letter

To whom it may concern:

This letter acknowledges that I have received and reviewed a request by Melissa Carlton to conduct a research project entitled "*Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills*" at First Baptist Church and I approve of this research to be conducted at our facility.

When the researcher receives approval for his/her research project from the Nova Southeastern University's Institutional Review Board/NSU IRB, I agree to provide access for the approved research project. If we have any concerns or need additional information, we will contact the Nova Southeastern University's IRB at (954) 262-5369 or [irb@nova.edu](mailto:irb@nova.edu).

Sincerely,



Mark McQueen  
Business Administrator  
[mmcqueen@firstbaptistpc.com](mailto:mmcqueen@firstbaptistpc.com)  
850-785-6146

## Appendix B

### Institutional Review Board Approval Letter



#### MEMORANDUM

To: **Melissa A Carlton, Information Systems  
College of Engineering and Computing**

From: **Ling Wang, Ph.D.,  
Center Representative, Institutional Review Board**

Date: **January 27, 2016**

Re: **IRB #: 2016-16; Title, "Development of a Cybersecurity Skills Index: A Scenarios-Based,  
Hands-On Measure of Non-IT Professionals' Cybersecurity Skills"**

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.**

## Appendix C

### Expert Recruitment Email

Dear Information Systems and Cybersecurity Experts,

I need your help in providing expert feedback on a measurement for my upcoming doctoral research study. I am a Ph.D. Candidate in Information Systems and Cybersecurity at the College of Engineering and Computing, Nova Southeastern University (NSU), working under the supervision of Professor Yair Levy, and a member of his [Levy CyLab](#). My research is seeking to develop an index to measure cybersecurity skills levels of non-Information Technology (IT) professionals.

Using a prior set of experts, nine platform independent cybersecurity skills needed by non-IT professionals were identified. The set of nine cybersecurity skills are established as the foundation for this phase of the research. In this part of the research, I need your assistance in validating the proposed scenarios, tasks, and scores assigned for each task. Here are the nine skills previously identified and validated in the first stage of my dissertation research:

1. Preventing the leaking of confidential digital information to unauthorized individuals
2. Preventing malware via non-secure Websites
3. Preventing personally identifiable information (PII) theft via access to non-secure networks
4. Preventing PII theft via e-mail phishing
5. Preventing malware via e-mail
6. Preventing credit card information theft by purchasing from non-secured Websites
7. Preventing information system compromise via USB or storage drive/device exploitations
8. Preventing unauthorized information system access via password exploitations
9. Preventing PII theft via social networks

The information provided will be used for this research study and in aggregated form. No personal identifiable information (PII) will be collected. As a participant, you agree to keep all information regarding this research confidential and to refrain from disclosing any details related to this survey or the material contained within it. Please be advised that this research is under process with the NSU's Cybersecurity Incubator, and as such, full confidentiality is required.

**If you are willing to participate in this phase of the research, maintain a high level of**



**confidentiality, and non-disclosure as it pertains to the scenarios, tasks, and scorings, please reply to this email by April 7, 2016. As a token of appreciation for providing your scholarly and professional contribution to the field of cybersecurity, you will receive a \$10 Starbucks gift card upon completing the questionnaire. After receiving your reply, a follow up email with the survey in the form of a fillable PDF file attached will be sent to you within 24 hours. If you prefer the PDF file be sent to an alternate email address, please provide it with your reply. If you wish to decline, please reply indicating that.**

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. Should you wish to receive the findings of the study, please indicate it with your reply to this email and I will be happy to provide you with information about the academic research publication(s) resulting from this study.

Warmest Regards,  
Melissa Carlton, Ph.D. Candidate  
E-mail: [mc2418@nova.edu](mailto:mc2418@nova.edu)  
Information Systems and Cybersecurity

## Appendix D

### Expert Qualitative and Quantitative Questionnaire

IRB protocol #: 2016-16

Principal investigator(s)  
Melissa Carlton, Ph.D. Candidate of  
Information Systems and Cybersecurity

Co-investigator(s)  
Yair Levy, Ph.D.  
Information Systems and Cybersecurity  
College of Engineering & Computing  
The DeSantis Building - Room 4058  
3301 College Avenue  
Fort Lauderdale, Florida 33314  
Phone: (954) 262-2006  
Email: levyy@nova.edu

For questions/concerns about your research rights, contact:  
Human Research Oversight Board (Institutional Review Board or IRB)  
Nova Southeastern University  
(954) 262-5369/Toll Free: 866-499-0790

Dear [Expert],

Thank you for agreeing to participate in this phase of my doctoral dissertation research study, titled, "Development of the Cybersecurity Skills Index (CSI): A Scenarios-Based, Hands-On Tasks Measure of Non-IT Professionals' Cybersecurity Skills", maintain a high level of confidentiality, and non-disclosure.

The information provided will be used for this research study and in aggregated form. No personal identifiable information (PII) will be collected. As a token of appreciation for providing your scholarly and professional contribution to the field of cybersecurity, you will receive a \$10 Starbucks gift card. There are no costs to you for participating in this study. Risks to you are minimal, meaning they are not thought to be greater than other risks you experience every day. The activities in this study may have unknown or unforeseeable risks. Please feel free to contact Mrs. Carlton or Dr. Yair Levy should you have any questions or research-related injury. You may also contact the IRB at the numbers indicated above with questions as to your research rights.

As a participant, you agree to keep all information regarding this research confidential and to refrain from disclosing any details related to this questionnaire or the material contained within it with non-NSU individuals and/or parties. You are asked to delete any material related to this study from your computer after returning the completed the

questionnaire.

You have the right to leave this study at any time or refuse to participate. If you do decide to leave or you decide not to participate, you will not experience any penalty or loss of services you have a right to receive. If you choose to withdraw, you are asked to delete any material related to this study from your computer and to contact Mrs. Carlton or Dr. Yair Levy of your decision.

The nine skills previously identified and validated are presented within the attached fillable PDF file. Each skill includes a group of four cybersecurity related scenarios-based, hands-on tasks for the non-IT professional to identify and demonstrate their skill level as if in a real-life situation. Questions are presented until you have evaluated all nine skills. If you agree with the scenario, task, or scoring presented, you only need to select 'yes' for the respective question. If you do not agree with any scenario, task, or scoring presented, select 'no' for that question and complete the respective comment field with your recommendation.

**As a cybersecurity expert, you are asked to**

- **review the scenario and respond if you believe the scenario is valid in the context of the related skill;**
- **review the task associated with its respective scenario to determine if it measures the related skill;**
- **evaluate the scoring associated with each of the four options (answers) presented for the related task; and**
- **evaluate the increment of difficulty for that set of scenarios and tasks.**

At the conclusion of the questionnaire, select the 'email form' button in order to email the form to Professor Yair Levy as a PDF attachment.

Thank you again for your time and assistance.

Warmest Regards,  
Melissa Carlton, Ph.D. Candidate  
E-mail: mc2418@nova.edu  
Information Systems and Cybersecurity



NOVA SOUTHEASTERN UNIVERSITY  
College of Engineering and Computing

IRB protocol #: 2016-16

Principal investigator(s)  
Melissa Carlton, Ph.D. Candidate of  
Information Systems and Cybersecurity

Co-investigator(s)  
Yair Levy, Ph.D.  
Information Systems and Cybersecurity  
College of Engineering & Computing  
The DeSantis Building - Room 4058  
3301 College Avenue  
Fort Lauderdale, Florida 33314  
Phone: (954) 262-2006  
Email: levyy@nova.edu

For questions/concerns about your research rights, contact:  
Human Research Oversight Board (Institutional Review Board or IRB)  
Nova Southeastern University  
(954) 262-5369/Toll Free: 866-499-0790  
IRB@nsu.nova.edu

This questionnaire will take approximately 35 minutes to complete. There are nine skills each consisting of four scenarios-based, hands-on tasks. Each scenarios-based, hands-on task has three required questions and a respective text box to provide recommended amendments (if any). At the conclusion of the scenarios-based, hands-on tasks for each skill is a required question and a tool to indicate recommended amendments (if any) to the increments of difficulty.

By continuing with completing this questionnaire, you indicate that

- this study has been explained to you
- you agree to maintain a high level of confidentiality and non-disclosure, including deleting this file after your responses have been confirmed received
- your questions about this research study have been answered
- you have been told that you may ask the researchers any study related questions in the future or contact them in the event of a research-related injury
- you have been told that you may ask Institutional Review Board (IRB) personnel questions about your study rights
- you voluntarily agree to participate in the study entitled "*Development of the Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills*"

## Appendix E

### Pilot Study Recruitment Email

Dear Fellow First Baptist Church Members,

I am a Ph.D. Candidate in Information Systems and Cybersecurity at the College of Engineering and Computing, Nova Southeastern University, working under the supervision of Professor Yair Levy, and a member of his [Levy CyLab](#). My research is seeking to develop an application (app) to measure cybersecurity skills levels of non-Information Technology (IT) professionals. Non-IT professionals are any person that performs work-related duties using a computer connected to the Internet that is not located in a formal IT or Technical Services department. Non-IT professionals include, but are not limited to, teachers, office assistants, managers, or executives. It excludes IT or Technical Services professionals.

I need your assistance to ensure the application is working accurately. The application is named MyCyberSkills™ and it will help organizations as well as industry entities to assess the cybersecurity skills of non-IT professionals. Your assistance is being solicited to complete tasks of nine cybersecurity skills previously identified.

A lab manager will manually record your score based on the responses you select within the application for comparison of the electronic scoring system, so I can ensure the scoring recorded are accurate. The study is expected to take no more than an hour of your time. The information provided will be used for this research study and in aggregated form. No personal identifiable information (PII) will be collected. Following the experiment, and as a token of appreciation for your time, I will provide a workshop on cybersecurity issues and how to protect yourself, your family, and your workplace from cyber-attacks. You are welcome to attend this important workshop free of charge right after the experiment, or contact me for additional information about future workshops, which you are welcome to attend free of charge.

If you are willing to participate, please reply to this email and a lab manager will contact you to schedule an appointment.

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

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

Warmest Regards,  
Melissa Carlton, PhD Candidate

E-mail: [mc2418@nova.edu](mailto:mc2418@nova.edu)  
Information Systems and Cybersecurity

## Appendix F

### Pilot Study Informed Consent Form

#### Adult/General Informed Consent

Consent Form for Participation in the Research Study Entitled: *Development of the Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills*

Funding Source: None.

IRB protocol #: 2016-16

Principal investigator(s)  
Melissa Carlton, Ph.D. Candidate of  
Information Systems and Cybersecurity

Co-investigator(s)  
Yair Levy, Ph.D.  
Information Systems and Cybersecurity  
College of Engineering & Computing  
The DeSantis Building - Room 4058  
3301 College Avenue  
Fort Lauderdale, Florida 33314  
Phone: (954) 262-2006  
Email: [levyy@nova.edu](mailto:levyy@nova.edu)

For questions/concerns about your research rights, contact:  
Human Research Oversight Board (Institutional Review Board or IRB)  
Nova Southeastern University  
(954) 262-5369/Toll Free: 866-499-0790  
[IRB@nsu.nova.edu](mailto:IRB@nsu.nova.edu)

Site location:  
First Baptist Church  
640 Grace Ave  
Panama City, FL 32401

#### **What is the study about?**

You are invited to participate in this research study to be submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems with a concentration in Cybersecurity at Nova Southeastern University. The goal of this study is to measure the cybersecurity skills of non-IT professionals using a novel scenarios-based, hands-on cybersecurity skills index developed as an online application as well as evaluate the validity of the application's scoring.

#### **Why are you asking me?**

You are invited to participate because of your interest demonstrated by responding to the posted announcement, are considered a non-IT professional, and 18 years of age or older. There will be a minimum of 20 participants in this research study.

Initials: \_\_\_\_\_ Date: \_\_\_\_\_

Page 1 of 3

**What will I be doing if I agree to be in the study?** Using a mobile device (iPad), you will be asked access the MyCyberSkills™ application. The application will collect some demographic information about you, but no personally identifiable information (PII). You will then be presented a scenario (short story), which you will read. Audio is available if you prefer to listen to the scenario with earbuds or headphones. After the scenario completes, you will then be asked to choose how the person in the scenario should respond to the situation (task). A lab manager will manually record your response as well for the purpose of verifying the application is properly scoring an individual's responses. This process will continue until you all 36 scenarios (stories) and their respective tasks are presented. At the end of the application, you will be provided the individual scores of your responses and an overall cybersecurity skills index (CSI) score ranging from 0 -100. Completing the MyCyberSkills™ app will take no more than one hour of your time.

**Is there any audio or video recording?**

There will be no audio or video recordings of this evaluation.

**What are the dangers to me?**

Risks to you are minimal, meaning they are not thought to be greater than other risks you experience every day. Having someone sitting with you to record your selected responses to the tasks may make you feel anxious or frustration. The activities in this study may have unknown or unforeseeable risks. If this happens the lab manager will try to help you. If you need further help, a lab manager will suggest someone you can see but you will have to pay for that yourself. If you have any questions about the research, your research rights, or have a research-related injury, please contact Mrs. Carlton or Dr. Yair Levy. You may also contact the IRB at the numbers indicated above with questions as to your research rights.

**Are there any benefits for taking part in this research study?**

There are no direct benefits.

**Will I get paid for being in the study? Will it cost me anything?**

There are no costs to you or payments made for participating in this study.

**How will you keep my information private?**

Any information collected could not be linked to you. Responses submitted will be collected with the use of a Google spreadsheet. At the conclusion of the data collection period, all information will be removed from online and stored on a USB drive. The USB drive will be kept in a locked filing cabinet for 36 months from the conclusion of the study. All information obtained in this study is strictly confidential unless disclosure is required by law. The IRB, regulatory agencies, and if the PI is a student that the dissertation chair/thesis adviser may review research records.

**What if I do not want to participate or I want to leave the study?**

You have the right to leave this study at any time or refuse to participate. If you do decide to leave or you decide not to participate, you will not experience any penalty or loss of services you

Initials: \_\_\_\_\_ Date: \_\_\_\_\_

Page 2 of 3



have a right to receive. If you choose to withdraw, any information collected about you **before** the date you leave the study will be kept in the research records for 36 months from the conclusion of the study and may be used as part of the research.

**Other Considerations:**

If significant new information relating to the study becomes available, which may relate to your willingness to continue to participate, this information will be provided to you by the investigators.

**Voluntary Consent by Participant:**

By signing below, you indicate that

- this study has been explained to you
- you have read this document or it has been read to you
- your questions about this research study have been answered
- you have been told that you may ask the researchers any study related questions in the future or contact them in the event of a research-related injury
- you have been told that you may ask Institutional Review Board (IRB) personnel questions about your study rights
- you are entitled to a copy of this form after you have read and signed it
- you voluntarily agree to participate in the study entitled "*Development of the Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills*"

Participant's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Participant's Name: \_\_\_\_\_ Date: \_\_\_\_\_

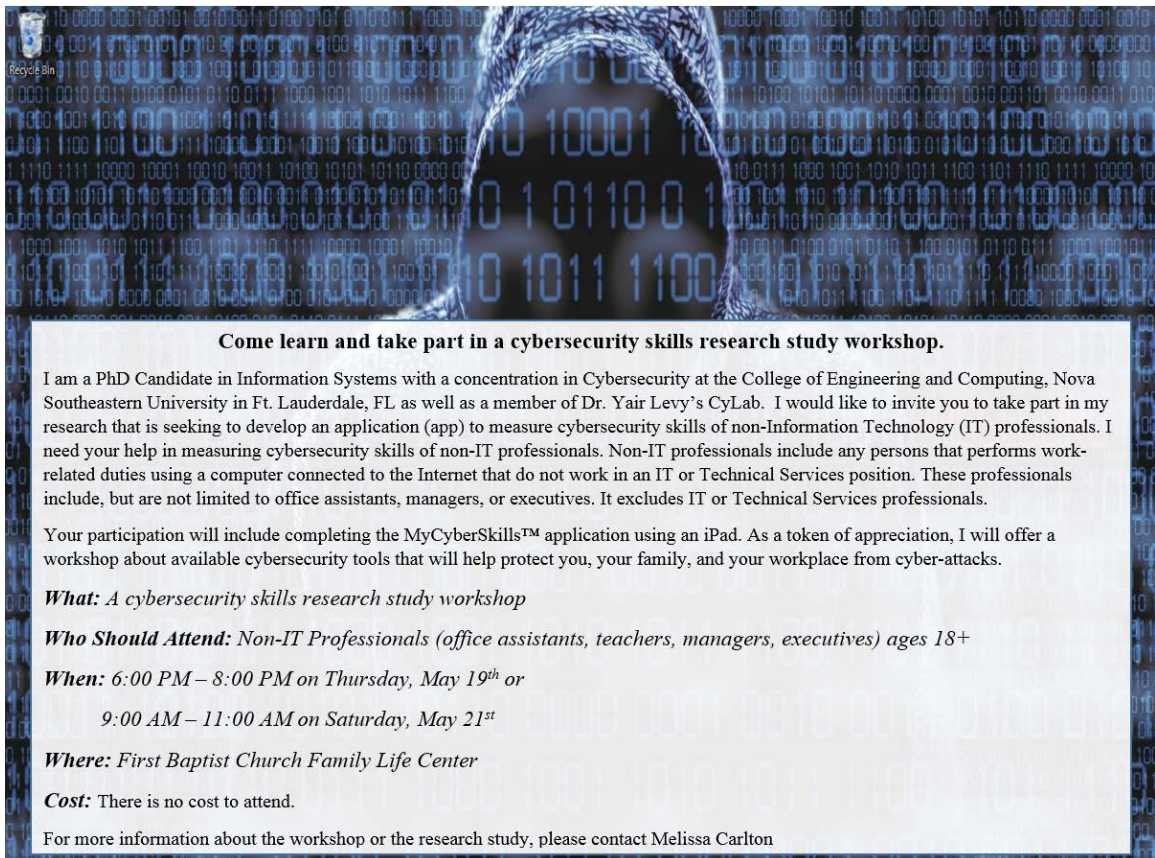
Signature of Person Obtaining Consent: \_\_\_\_\_

Date: \_\_\_\_\_

Initials: \_\_\_\_\_ Date: \_\_\_\_\_

## Appendix G

### Research Study Recruitment Flyer



**Come learn and take part in a cybersecurity skills research study workshop.**

I am a PhD Candidate in Information Systems with a concentration in Cybersecurity at the College of Engineering and Computing, Nova Southeastern University in Ft. Lauderdale, FL as well as a member of Dr. Yair Levy's CyLab. I would like to invite you to take part in my research that is seeking to develop an application (app) to measure cybersecurity skills of non-Information Technology (IT) professionals. I need your help in measuring cybersecurity skills of non-IT professionals. Non-IT professionals include any persons that performs work-related duties using a computer connected to the Internet that do not work in an IT or Technical Services position. These professionals include, but are not limited to office assistants, managers, or executives. It excludes IT or Technical Services professionals.

Your participation will include completing the MyCyberSkills™ application using an iPad. As a token of appreciation, I will offer a workshop about available cybersecurity tools that will help protect you, your family, and your workplace from cyber-attacks.

**What:** *A cybersecurity skills research study workshop*

**Who Should Attend:** *Non-IT Professionals (office assistants, teachers, managers, executives) ages 18+*

**When:** *6:00 PM – 8:00 PM on Thursday, May 19<sup>th</sup> or  
9:00 AM – 11:00 AM on Saturday, May 21<sup>st</sup>*

**Where:** *First Baptist Church Family Life Center*

**Cost:** There is no cost to attend.

For more information about the workshop or the research study, please contact Melissa Carlton

## Appendix H

### Research Study Informed Consent Form

#### Adult/General Informed Consent

Consent Form for Participation in the Research Study Entitled: *Development of the Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills*

Funding Source: None.

IRB protocol #: 2016-16

Principal investigator(s)  
Melissa Carlton, Ph.D. Candidate of  
Information Systems and Cybersecurity

Co-investigator(s)  
Yair Levy, Ph.D.  
Information Systems and Cybersecurity  
College of Engineering & Computing  
The DeSantis Building - Room 4058  
3301 College Avenue  
Fort Lauderdale, Florida 33314  
Phone: (954) 262-2006  
Email: [levyy@nova.edu](mailto:levyy@nova.edu)

For questions/concerns about your research rights, contact:  
Human Research Oversight Board (Institutional Review Board or IRB)  
Nova Southeastern University  
(954) 262-5369/Toll Free: 866-499-0790  
[IRB@nsu.nova.edu](mailto:IRB@nsu.nova.edu)

Site location:  
First Baptist Church  
640 Grace Ave  
Panama City, FL 32401

#### **What is the study about?**

You are invited to participate in this research study to be submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems with a concentration in Cybersecurity at Nova Southeastern University. The goal of this study is to measure the cybersecurity skills of non-IT professionals using a novel scenarios-based, hands-on cybersecurity skills index developed as an online application.

#### **Why are you asking me?**

You are invited to participate because of your interest demonstrated by responding to the posted announcement, are considered a non-IT professional, and 18 years of age or older. There will be a minimum of 100 participants in this research study.

Initials: \_\_\_\_\_ Date: \_\_\_\_\_

Page 1 of 3

**What will I be doing if I agree to be in the study?** Using a mobile device (iPad), you will be asked access the MyCyberSkills™ application. The application will collect some demographic information about you, but no personally identifiable information (PII). You will then be presented a scenario (short story), which you will read. Audio is available if you prefer to listen to the scenario with earbuds or headphones. After the scenario completes, you will then be asked to choose how the person in the scenario should respond to the situation (task). This process will continue until you all 36 scenarios (stories) and their respective tasks are presented. At the end of the application, you will be provided the individual scores of your responses and an overall cybersecurity skills index (CSI) score ranging from 0 -100. Completing the MyCyberSkills™ app will take no more than 45 minutes.

**Is there any audio or video recording?**

There will be no audio or video recordings of this evaluation.

**What are the dangers to me?**

Risks to you are minimal, meaning they are not thought to be greater than other risks you experience every day. Having to select a response to the tasks may make you feel anxious or frustration. The activities in this study may have unknown or unforeseeable risks. If this happens a lab manager will try to help you. If you need further help, a lab manager will suggest someone you can see but you will have to pay for that yourself. If you have any questions about the research, your research rights, or have a research-related injury, please contact Mrs. Carlton or Dr. Yair Levy. You may also contact the IRB at the numbers indicated above with questions as to your research rights.

**Are there any benefits for taking part in this research study?**

There are no direct benefits.

**Will I get paid for being in the study? Will it cost me anything?**

There are no costs to you or payments made for participating in this study.

**How will you keep my information private?**

Any information collected could not be linked to you. Responses submitted will be collected with the use of a Google form. At the conclusion of the data collection period, all information will be removed from online and stored on a USB drive. The USB drive will be kept in a locked filing cabinet for 36 months from the conclusion of the study. All information obtained in this study is strictly confidential unless disclosure is required by law. The IRB, regulatory agencies, and if the PI is a student that the dissertation chair/thesis adviser may review research records.

**What if I do not want to participate or I want to leave the study?**

You have the right to leave this study at any time or refuse to participate. If you do decide to leave or you decide not to participate, you will not experience any penalty or

Initials: \_\_\_\_\_ Date: \_\_\_\_\_

Page 2 of 3

loss of services you have a right to receive. If you choose to withdraw, any information collected about you **before** the date you leave the study will be kept in the research records for 36 months from the conclusion of the study and may be used as part of the research.

**Other Considerations:**

If significant new information relating to the study becomes available, which may relate to your willingness to continue to participate, this information will be provided to you by the investigators.

**Voluntary Consent by Participant:**

By signing below, you indicate that

- this study has been explained to you
- you have read this document or it has been read to you
- your questions about this research study have been answered
- you have been told that you may ask the researchers any study related questions in the future or contact them in the event of a research-related injury
- you have been told that you may ask Institutional Review Board (IRB) personnel questions about your study rights
- you are entitled to a copy of this form after you have read and signed it
- you voluntarily agree to participate in the study entitled "*Development of the Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills*"

Participant's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Participant's Name: \_\_\_\_\_ Date: \_\_\_\_\_

Signature of Person Obtaining Consent: \_\_\_\_\_

Date: \_\_\_\_\_

Initials: \_\_\_\_\_ Date: \_\_\_\_\_

## References

- Adomßent, M., & Hoffman, T. (2013). *The concept of competencies in the context of Education for Sustainable Development (ESD)*. Retrieved from <http://esd-expert.net/assets/130314-Concept-Paper-ESD-Competencies.pdf>
- Algarni, A., Xu, Y., & Chan, T. (2015). Susceptibility to social engineering in social networking site: The case of Facebook. *Proceedings of the 36<sup>th</sup> International Conference on Information Systems (ICIS) 2015*, Ft. Worth, TX.
- Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). Social engineering in social networking sites: How good become evil. *Proceedings of the 18<sup>th</sup> Pacific Asia Conference on Information Systems (PACIS 2014)* (Paper 271).
- Alias, N. A. (2015). *Designing, developing and evaluating a learning support tool: A case of design and development research (DDR)*. Retrieved from Sage Research Methods website: <http://srmo.sagepub.com/view/methods-case-studies-2015/n14.xml?rskey=q0vTAG&row=1th>
- Airoidi, E. M., Bai, X., & Malin, B. A. (2011). An entropy approach to disclosure risk assessment: Lessons from real applications and simulated domains. *Decision Support Systems*, 51(1), 10-20.
- Anderson, J. R. (1982). Acquisition of cognitive skill. *Psychological Review*, 89(4), 369-406.
- Andrews, M., & Whittaker, J. A. (2004). Computer security. *IEEE Security & Privacy*, 2(5), 68-71.
- Anti-Phishing Working Group (APWG). (2010). *Phishing activity trends report (4<sup>th</sup> quarter 2009)*. Retrieved from [http://docs.apwg.org/reports/apwg\\_report\\_Q4\\_2009.pdf](http://docs.apwg.org/reports/apwg_report_Q4_2009.pdf)
- Anti-Phishing Working Group (APWG). (2014). *Phishing activity trends report (4<sup>th</sup> quarter 2013)*. Retrieved from [http://docs.apwg.org/reports/apwg\\_trends\\_report\\_q4\\_2013.pdf](http://docs.apwg.org/reports/apwg_trends_report_q4_2013.pdf)
- Anti-Phishing Working Group (APWG). (2016). *Phishing activity trends report (1<sup>st</sup> quarter 2016)*. Retrieved from [http://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2016.pdf](http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf)
- Axelrod, C. W. (2006). Cybersecurity and the critical infrastructure: Looking beyond the

- perimeter. *Information Systems Control Journal*, 6(3). Retrieved from <http://www.isaca.org/Journal/Past-Issues/2006/Volume-3/Pages/Cybersecurity-and-the-Critical-Infrastructure-Looking-Beyond-the-Perimeter1.aspx>.
- Baer, J. (2015, January 5). Morgan Stanley fires employee over client-data leak. *The Wall Street Journal, Markets*. Retrieved from <http://www.wsj.com/articles/morgan-stanley-terminates-employee-for-stealing-client-data-1420474557>
- Ball, A., Ramim, M. M., Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management*, 3(1), 180-207.
- Barrett, D., Perez, E., & Gorman, S. (2012, November 13). FBI agent in Petraeus case under scrutiny. *The Wall Street Journal, U.S. News*. Retrieved from <http://www.wsj.com/articles/SB10001424127887324439804578115410189757452>
- Bauer, L., Bravo-Lillo, C., Fragkaki, E., & Melicher, W. (2013). A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality. *Proceedings of the 2013 ACM workshop on Digital Identity Management*, (pp. 25-36). doi:10.1145/2517881.2517886
- Beaudoin, M. F., Kurtz, G., & Eden, S. (2009). Experiences and opinions of e-learners: What works, what are the challenges, and what competencies ensure successful online learning. *Interdisciplinary Journal of E-Learning & Learning Objects*, 5, 275-289.
- Benilian, A. (2015). IT feature use over time and its impact on individual task performance. *Journal of the Association for Information Systems*, 16(3), 144-173.
- Bensinger, G., & Calia, M. (2014, May 21). Ebay asks users to change passwords after cyberattack: Compromised database contains encrypted passwords, not financial data. *Wall Street Journal (Online)*. Retrieved from <http://online.wsj.com>
- Bere, M., Bhunu-Shava, F., Gamundani, A., & Nhamu, I. (2015). Advanced persistent threats exploit humans. *International Journal of Computer Science Issues*, 12(6), 170-174.
- Berendonk, C., Stalmeijer, R. E., & Schuwirth, L. W. (2013). Expertise in performance assessment: Assessors' perspectives. *Advances in Health Sciences Education*, 18(4), 559-571.
- Boritz, J. E., & No, W. G. (2011). E-commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems*, 25(2), 11-45.

- Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1-16.
- Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology*, 11(3/4), 279-295.
- Brancheau, J. C., & Wetherbe, J. C. (1987). Key issues in information systems management. *MIS Quarterly*, 11(1), 23-45.
- Bravo-Lillo, C., Komanduri, S., Cranor, L. F., Reeder, R. W., Sleeper, M., Downs, J., & Schechter, S. (2013). Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. *Proceedings of the Ninth Symposium of Usable Privacy and Security (SOUPS)* (Article 6). doi:10.1145/2501604.2501610
- Bronsburg, S. E. (2011). *The impact of an osteopathic medical program on information technology skills of physicians entering the workforce* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 3465615)
- Brown, S. D., Levy, Y., Ramim, M. M., & Parrish, J. (2015). Pharmaceutical companies' documented and online privacy practices: Development of an index measure and initial test. *Online Journal of Applied Knowledge Management*, 3(2), 68-88.
- Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1), 97-115.
- Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Privacy and security: Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM*, 57(2), 24-27.
- Burning Glass Technologies. (2015). *Job market intelligence: Cybersecurity jobs, 2015*. Retrieved from [http://burning-glass.com/wp-content/uploads/Cybersecurity\\_Jobs\\_Report\\_2015.pdf](http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf)
- Chabrow, E. (2014, September 20). *Senate passes cybersecurity skills shortage bill: Measure aims to boost IT security employment at DHS*. Retrieved from Gov Info Security website: <http://www.govinfosecurity.com/senate-passes-cybersecurity-skills-shortage-bill-a-7340>
- Chakhssi, F., de Rulter, C., & Bernstein, D. (2010). Reliability and validity of the Dutch version of the behavioural status index: A nurse-rated forensic assessment tool. *Assessment*, 17(1) 58.69.
- Chen, K. Z., Gu, G., Zhuge, J., Nazario, J., & Han, H. (2011). WebPatrol: Automated collection and replay of web-based malware scenarios. *Proceedings of the 6<sup>th</sup> ACM Symposium on Information, Computer and Communications Security* (pp. 186-195). doi: 10.1145/1966913.1966938



- Chhabra, S., Aggarwal, A., Benevenuto, F., & Kumaraguru, P. (2011). Phishing landscape through short URLs. *Proceedings of the 8<sup>th</sup> Annual Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference*, (pp. 92-101).
- Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS)* (Article 1). doi:10.1145/2335356.2335358
- Chisholm, C. B., Dodge, W. R., Balise, R. R., Williams, S. R., Gharahbaghian, L., & Beraud, A.-S. (2013). Focused cardiac ultrasound training: How much is enough? *The Journal of Emergency Medicine*, 44(4), 818-822.
- Choi, M. S. (2013). *Assessing the role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills toward computer misuses intention at government agencies* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 3599848)
- Choi, M. S., 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* (Paper 29), Milan, Italy. Retrieved from <http://aisel.aisnet.org/wisp2012/29>.
- Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 710-731.
- Clinton, H. (2015, March 10). *Hillary Clinton on her personal electronic mail account (C-SPAN)* [Video file]. Retrieved from <http://www.c-span.org/video/?324777-1/hillary-clinton-news-conference>
- Collins, K. M. T., Onwuegbuzie, A. J., & Sutton, I. L. (2006). A model incorporating the rationale and purpose for conducting mixed-methods research in special education and beyond. *Learning Disabilities: A Contemporary Journal*, 4(1), 67-100.
- Comesongsri, V. (2010). *Motivation for the avoidance of phishing threat* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 3421381)
- Committee on National Security Systems (CNSS). (2010, April 26). *National information assurance (IA) glossary* (Instruction No. 4009). Retrieved from [http://www.ncix.gov/publications/policy/docs/CNSSI\\_4009.pdf](http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf)
- CompTIA. (2015). *Trends in information security* [Research report]. Retrieved from

<https://www.comptia.org/resources/trends-in-information-security-study>

- Cox, C. (2015). Cyber capabilities and intent of terrorist forces. *Information Security Journal: A Global Perspective*, 24(1-3), 31-38.
- Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced mixed methods research designs. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioral research* (pp. 209-240). Thousand Oaks, CA: Sage Publications, Inc.
- Cyberedge Group. (2014). *2014 Cyberthreat defense report: North America & Europe*. Retrieved from <http://cyber-edge.com/wp-content/uploads/2014/01/CyberEdge-2014-CDR.pdf>
- 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.
- Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science*, 9(3), 458-467.
- Davinson, N., & Silience, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, 26(6), 1739-1747.
- Downey, J. P., & Smith, L. A. (2011). The role of computer attitudes in enhancing computer competence in training. *Journal of Organizational and End User Computing*, 23(3), 81-100.
- Eargle, D., Taylor, R., Sawyer, L., & Gaskin, J. (2014). Acquiring IS skill through habitual use. In *System Sciences (HICSS), 2014 47<sup>th</sup> Hawaii International Conference on* (pp. 3-12).
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323-337.
- Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceedings of Informing Science & IT Education Conference, InSITE*.
- Enterprise Risk Management (ERM). (2014). *Explaining the importance of information risk management: Engaging your directors with a powerful dashboard*. Retrieved from <http://emrisk.web8.hubspot.com/it-risk-management-portraying-the-importance-of-information-security>
- Eschenbrenner, B., & Nah, F. F.-H. (2014). Information systems user competency: A

conceptual foundation. *Communications of the Association for Information systems*, 34, 1363-1378.

Exec. Order No. 13,636, 78 Fed. Reg. 11739 (2013).

Exec. Order No. 13,681, 79 Fed. Reg. 63491 (2014).

Fenrich, P. (2005). What can you do to virtually teach hands-on skills? *Issues in Informing Science & Information Technology*, 2, 347-354.

Fitts, P. M. (1964). Perceptual-motor skill learning. In A. W. Melton (Ed.), *Categories of human learning* (pp. 243-292). New York: Academic Press.

Furnell, S. (2004). Qualified to help: In search of the skills to ensure security. *Computer Fraud & Security*, 2004(12), 10-14.

Furnell, S. (2007). Phishing: Can we spot the signs? *Computer Fraud & Security*, 2007(3), 10-15.

Furnell, S., & Moore, L. (2014). Security literacy: The missing link in today's online society? *Computer Fraud & Security*, 2014(5), 12-18.

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS)* (pp. 44-55).

Gemalto. (2015). *2015 first half review: Findings from the breach level index*. Retrieved from [http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto\\_H1\\_2015\\_BLI\\_Report.pdf](http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf)

Gemalto. (2016). *Breach level index: Data breach database & risk assessment calculator*. Retrieved from <http://www.breachlevelindex.com/>

Glazer, E., & Yadron, D. (2014, October 2). J.P. Morgan says about 76 million households affect by cyber breach. *The Wall Street Journal, Markets*. Retrieved from <http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372>

Goodman, S. E., & Lin, H. S. (Eds.). (2007). *Toward a safer and more secure cyberspace*. Washington, D.C.: The National Academies Press.

Gordon, T. J. (1994). The Delphi method. In J. C. Glenn, & T. J. Gordon (Eds.), *Futures Research Methodology* (Chapter 4). Washington, DC: Millennium Project.

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

378-394.

- Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis, 11*(3), 255-274.
- Grimes, G. M., Marquardson, J., & Nunamaker, Jr., J. F. (2014). Broken windows bad passwords: Influencing secure user behavior via website design. *Proceedings of the Twentieth Americas Conference on Information Systems – Information Systems Security, Assurance, and Privacy* (Paper 3), Savannah, GA.
- Gundecha, P., Barbier, G., & Liu, H. (2011). Exploiting vulnerability to secure user privacy on a social networking site. *Proceedings of the 17<sup>th</sup> ACM SIGKDD international conference on knowledge discovery and data mining* (pp. 511-519).
- Guzman, I. R., Stam, K. R., & Stanton, J. M. (2008). The occupational culture of IS/IT personnel within organizations. *Database for Advances in Information Systems, 39*(1), 33-50.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7<sup>th</sup> Ed.). Upper Saddle River, NJ: Prentice Hall.
- Hajgude, J., & Ragha, L. (2012). Phish mail guard: Phishing mail detection technique by using textual and URL analysis. In *Information and Communication Technologies (WICT), 2012 World Congress on* (pp. 297-302).
- Harris, M. A., Furnell, S., & Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy and Security, 10*(4), 186-202.
- Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination*. London, UK: Sage Publications.
- Havelka, D., & Merhout, J. W. (2009). Toward a theory of information technology professional competence. *The Journal of Computer Information Systems, 50*(2), 106-116.
- He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security, 21*(5), 381-400.
- Heartfield, R., & Loukas, G. (2013). On the feasibility of automated semantic attacks in the cloud. In E. Gelenbe, & R. Lent (Eds.), *27th International Symposium on Computer and Information Sciences III* (pp. 343-351).

- Helminen, A., Halonen, P., Rankinen, T., Nissinen, A., & Rauramaa, R. (1995). Validity assessment of a social support index. *Scandinavian Journal of Public Health*, 23(1) 66-74.
- Hevner, A., & Chatterjee, S. (2010). Design research in information systems. In R. Sharda & S. Voß (Eds.), *Integrated Series in Information Systems* (pp. 292-294). New York: Springer.
- Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74-81. doi:10.1145/2063176.2063197
- Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, 49(2), 99-110.
- Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Associations for Information Systems*, 34(Article 50), 893-912.
- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6), 54-60.
- Huang, C.-Y., Ma, S.-P., & Chen, K.-T. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications*, 34(4), 1292-1301. doi:10.1016/j.jnca.2011.02.004
- International Business Machines (IBM) Global Technology Services, Managed Security Services. (2014). *IBM security services 2014 cyber security intelligence index*. Retrieved from <http://www-935.ibm.com/services/us/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic/>
- Identity Force. (2016, May 27). The biggest data breaches in 2016, so far [Web log]. Retrieved from <https://www.identityforce.com/blog/2016-data-breaches>
- Identity Theft Resource Center (ITRC). (2015). *ITRC Breach Report*. Retrieved from <http://www.idtheftcenter.org/images/breach/ITRCBreachReport2015.pdf>
- Identity Theft Resource Center (ITRC). (2016). *ITRC Breach Report*. Retrieved from <http://www.idtheftcenter.org/images/breach/ITRCBreachReport2016.pdf>
- International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2013). *ISO/IEC 27002: Information technology – security techniques – code of practice for information security controls*.
- Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse.

*Communications of the ACM*, 47(4), 75-78.

- Jacob, N. A., & Antony, G. V. (2014). Insider information security threats in Indian banking context. *International Journal of Information Technology & Computer Sciences Perspectives*, 3(4), 1220-1226.
- James, L. (2005). *Phishing exposed*. Rockland, MA: Syngress.
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.
- Jenkins, J. L. (2013). *Alleviating insider threats: Mitigation strategies and detection techniques* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 3587255).
- Jensen, B. K., Bailey, J. L., & Baar, S. (2014). Making security policies memorable: the first line of defense. *International Journal of Business, Humanities and Technology*, 4(2). Retrieved from [http://www.ijbhtnet.com/journals/Vol\\_4\\_No\\_2\\_March\\_2014/4.pdf](http://www.ijbhtnet.com/journals/Vol_4_No_2_March_2014/4.pdf)
- J. P. Morgan Chase & Company. (2014, October 2). *Form 8-K*. Retrieved from the U.S. Securities & Exchange Commission SEC Filings EDGAR database. (Accession No. 0001193125-14-362173)
- Kane, G. C., Alavi, M., Labianca, G., & Borgatti, S. P. (2014). What's different about social media networks? A framework and research agenda. *MIS Quarterly*, 38(1), 275-304.
- Kaspersky Lab, Global Research and Analysis Team (GREAT). (2013). *Kaspersky security bulletin 2013*. Retrieved from [http://media.kaspersky.com/pdf/KSB\\_2013\\_EN.pdf](http://media.kaspersky.com/pdf/KSB_2013_EN.pdf)
- Katz, R. L. (1974). Skills of an effective administrator. *Harvard Business Review*, 52(5), 90-102.
- Kessem, L. (2016). Cybercrime's epic year. In IBM Security (Ed.), *IBM X-Force Threat Intelligence Report 2016* (pp. 9-15) Retrieved from <https://securityintelligence.com/media/xforce-tir-2016/>
- Kim, J., Park, E. H., & Baskerville, R. L. (2016). A model of emotion and computer abuse. *Information & Management*, 53(1), 91-108.
- Kissel, R. (2013). *Glossary of key information security terms* (NIST IR 7298 revision 2). Retrieved from National Institute of Standards and Technology website: <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

- Kozak, M., Iefremova, O., Szkola, J., & Sas, D. (2014). Do researchers provide public or institution e-mail accounts as correspondence e-mails in scientific articles? *Journal of the Association for Information Science and Technology*. Advance online publication. doi: 10.1002/asi.23401
- Kraiger, K., Ford, J. K., & Salas, E. (1993). Application of cognitive, skill-based, and affective theories of learning outcomes to new methods of training evaluation. *Journal of Applied Psychology Monograph*, 78(2), 311-328.
- Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. *Proceedings of the 2<sup>nd</sup> ACM Workshop on Online Social Networks* (pp. 7-12).
- Krombholz, K. Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113-122.
- Kushniruk, A. W., Triola, M. M., Borycki, E. M., Stein, B., & Kannry, J. L. (2005). Technology induced error and usability: The relationship between usability problems and prescription errors when using a handheld application. *International Journal of Medical Informatics*, 74(7-8), 519-526.
- Kvedar, D., Nettis, M., & Fulton, S. P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *Journal of Computing Sciences in Colleges*, 26(2), 80-87.
- Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (10<sup>th</sup> Ed.). Upper Saddle River, NJ: Prentice Hall.
- Lerouge, C., Newton, S., & Blanton, J. E. (2005). Exploring the systems analyst skill set: Perceptions, preferences, age, and gender. *The Journal of Computer Information Systems*, 45(3), 12-23.
- Lévesque, F. L., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013). A clinical study of risk factors related to malware infections. *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security* (pp. 97-108).
- Levy, Y. (2005). A case study of management skills comparison in online MBA programs. *International Journal of Information and Communication Technology Education*, 1(3), 1-20.
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.

- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science Journal*, 9(1), 181-212.
- Levy, Y., & Ramim, M. M. (2015). An assessment of competency-based simulations on e-learners' management skills enhancements. *Interdisciplinary Journal of E-Learning and Lifelong Learning*, 11, 179-190. Retrieved from <http://www.ijello.org/Volume11/IJELLv11p179-190Levy1958.pdf>
- Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011). Comparing intentions to use university provided vs. vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems*, 28(2), 102-113.
- Li, W., & Liu, P. (2011). Teaching computer networks for distance computer science students: An instructor's perspective. In *Electrical and Control Engineering (ICECE), 2011 International Conference on* (pp. 6814-6818). IEEE.
- Libicki, M. C., Senty, D., & Pollak, J. (2014). *H4cker5 wanted: An examination of the cybersecurity labor market*. Retrieved from RAND Corporation website: [www.rand.org/content/dam/rand/pubs/research\\_reports/RR400/RR430/RAND\\_RR430.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf)
- Lichvar, B. T. (2011). *An empirical investigation of the effect of knowledge sharing and encouragement by others in predicting computer self-efficacy and use of information systems in the workplace* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 3461673)
- Lin, E., Greenberg, S., Trotter, E., Ma, D., & Aycocock, J. (2011). Does domain highlighting help people identify phishing sites? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2075-2084). doi:10.1145/1978942.1979244
- MacMillan, D., & Yadron, D. (2014, October 14). Dropbox blames security breach on password reuse. *The Wall Street Journal, Digits*. Retrieved from <http://blogs.wsj.com/digits/2014/10/14/dropbox-blames-security-breach-on-password-reuse/>
- Malin, B. (2005). Betrayed by my shadow: Learning data identity via trail matching. *Journal of Privacy Technology*, 20050609001.
- Mann, K. V. (2010). Self-Assessments: The complex process of determining "how we are doing" – a perspective from medical education. *Academy of Management Learning & Education*, 9(2), 305-313.



- Marakas, G. M., Yi, M. Y., & Johnson, R. D. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research*, 9(2), 126-163.
- 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.
- Mata, F. J., Fuerst, W. L., & Barney, J. B. (1995). Information technology and sustained competitive advantage: A resource-based analysis. *MIS Quarterly*, 19(4), 487-505.
- Mathews, A. W., & Yadron, D. (2015, February 5). Anthem health insurer hit by big data breach. *The Wall Street Journal, Business*, A1.
- Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies*, 63(1-2), 25-50.
- McAfee Labs. (2014). *Threats report: August 2014*. Retrieved from <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2014.pdf?cid=BHP030>
- McCallister, E., Grance, T., & Scarfone, K. (2010). *Guide to protecting the confidentiality of personally identifiable information (PII)* (NIST special publication 800-122). Retrieved from National Institute of Standards and Technology website: <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
- McDowell, K. (2006). Now that we are all so well-educated about spyware, can we put the bad guys out of business? *ACM Proceedings of the 24<sup>th</sup> Annual Special Interest Group on University & College Computing Services 2006 (SIGUCCS 06)* (pp. 235-239).
- McFadzean, E., Ezingear, J.-N., & Birchall, D. (2011). Information assurance and corporate strategy: A Delphi study of choices, challenges, and developments for the future. *Information Systems Management*, 28(2), 102-129.
- Mendoza, V. D. (2014). *Measurement, tips, and errors: Making an instrument design in risk perception*. Retrieved from Sage Research Methods website: <http://srmo.sagepub.com/view/methods-case-studies-2014/n237.xml>
- Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods: Practical application and interpretation* (Fourth Ed.). Glendale, CA: Pyrczak Publishing.

- Mills, D. (2009). Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking websites. *ACM Proceedings of the 2009 Information Security Curriculum Development Conference* (pp. 139-141).
- Min, B., Varadharajan, V., Tupakula, U., & Hitchens, M. (2014). Antivirus security: Naked during updates. *Software – Practice and Experience*, 44(10), 1201-1222.
- Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley Publishing, Inc.
- Mitnick, K. D., & Simon, W. L. (2005). *The art of intrusion: The real stories behind the exploits of hackers*. Indianapolis, IN: Wiley Publishing, Inc.
- Morcke, A. M., Dorman, T., & Eika, B. (2013). Outcome (competency) based education: An exploration of its origins, theoretical basis, and empirical evidence. *Advances in Health Sciences Education*, 18(4), 851-863.
- Moskal, B. M. (2010). Self-Assessments: What are their valid uses? *Academy of Management Learning & Education*, 9(2), 314-320.
- Mouton, F., Leenen, L., Malan, M. M., & Venter, H.S. (2014). Towards an ontological model defining the social engineering domain. In K. Kimppa, D. Whitehouse, T. Kuusela, & J. Phahlamohlaka (Eds.), *ICT and Society* (pp. 266-279).
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013.). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, 56(December), 11-26.
- National Initiative for Cybersecurity Careers and Studies (NICCS). (2014). *Cyber Glossary*. Retrieved from <http://niccs.us-cert.gov/glossary#cybersecurity>
- National Institute of Standards and Technology (NIST). (2014, February 12). *Framework for improving critical infrastructure cybersecurity* (version 1.0). Retrieved from <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>
- National Institute of Standards and Technology (NIST), Computer Security Division. (2006, March). *Federal information processing standards publication: Minimum security requirements for Federal information and information systems* (FIPS PUB 200). Retrieved from <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>
- National Research Council (NRC). (2013). *Professionalizing the nation's cybersecurity workforce? Criteria for decision-making*. Washington, DC: National Academies Press.

- Nelson, J. A., Bustamante, R. M., Wilson, E. D., & Onwuegbuzie, A. J. (2008). The school-wide cultural competence observation checklist for school counselors: An exploratory factor analysis. *Professional School Counseling, 11*(4), 207-217.
- Neves, D. M., & Anderson, J. R. (1981). Knowledge compilation: Mechanisms for the automatization of cognitive skills. In J. R. Anderson (Ed.), *Cognitive skills and their acquisition* (pp. 57-84). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.
- Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011, September). Guidelines for usable cybersecurity: Past and present. In *Cyberspace Safety and Security (CSS), 2011 Third International Workshop on* (pp. 21-26). IEEE.
- O'Fallon, M. J., & Butterfield, K. D. (2005). A review of empirical ethical decision-making literature: 1996-2003. *Journal of Business Ethics, 59*(4), 375-413.
- 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.
- Onwuegbuzie, A. J., Bustamante, R. M., & Nelson, J. A. (2010). Mixed research as a tool for developing quantitative instruments. *Journal of Mixed Methods Research, 4*(1), 56-78.
- Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management, 52*(2), 183-199.
- Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice, 43*(4), 626-642.
- Peha, J. M. (2013). *The dangerous policy of weakening security to facilitate surveillance*. Retrieved from [http://users.ece.cmu.edu/~peha/Peha\\_on\\_weakened\\_security\\_for\\_surveillance.pdf](http://users.ece.cmu.edu/~peha/Peha_on_weakened_security_for_surveillance.pdf)
- Phish Tank. (2009). *Statistics about phishing activity and Phish Tank usage: November, 2009*. Retrieved from <http://www.phishtank.com/stats/2009/11/>
- Podhradsky, A., D'Ovidio, R., Engbretson, P., & Casey, C. (2013). Xbox 360 hoaxes, social engineering, and gamertag exploits. In *System Sciences (HICSS), 2013 46<sup>th</sup> Hawaii International Conference on* (pp. 3239-3250).
- Ponemon Institute. (2014a). *2014 cost of data breach study: Global analysis*. Retrieved from <http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>

- Ponemon Institute. (2014b). *Understaffed and at risk: Today's IT security department*. Retrieved from HP Enterprise Security website: [http://www.hp.com/hpinfo/newsroom/press\\_kits/2014/RSAConference2014/Ponemon\\_IT\\_Security\\_Jobs\\_Report.pdf](http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_IT_Security_Jobs_Report.pdf)
- PricewaterhouseCoopers (PwC). (2013, October 21). *Defending yesterday: Key findings from the global state of information security survey 2014*. Retrieved from <http://www.pwc.com/gx/en/consulting-services/information-security-survey/pwc-gsiss-2014-key-findings-report.pdf>
- PricewaterhouseCoopers (PwC). (2014, May 1). *Why you should adopt the NIST cybersecurity framework*. Retrieved from [http://www.pwc.com/en\\_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf](http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf)
- PricewaterhouseCoopers (PwC). (2016). *Turnaround and transformation in cybersecurity: Key findings from the global state of information security survey 2016*. Retrieved from <http://www.pwc.com/gsiss>
- Privacy Rights Clearinghouse. (2014). *Chronology of data breaches*. Retrieved from <https://www.privacyrights.org/data-breach>
- Provos, N., Rajab, M. A., & Mavrommatis, P. (2009). Cybercrime 2.0: When the cloud turns dark. *Communications of the ACM*, 53(4), 42-47.
- Qin, T., & Burgoon, J. K. (2007). An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In G. Muresan, T. Altiok, B. Melamed, & D. Zeng (Eds.), *2007 IEEE Intelligence and Security Informatics* (pp. 152-259).
- Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber-attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24-34.
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.
- Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly*, 36(1), 43-64.
- Rastello, S., & Smialek, J. (2013, May 16). Cybersecurity starts in high school with tomorrow's hires. *Bloomberg*

- Raytheon – National Cyber Security Alliance (NCSA). (2015). *Securing our future: Closing the cybersecurity talent gap*. Retrieved from [http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn\\_278208.pdf](http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_278208.pdf)
- Reece, R. P., & Stahl, B. C. (2015). The professionalisation of information security: Perspectives of UK practitioners. *Computers & Security*, 48, 182-195.
- Reinard, J. C. (2006). *Communication research statistics*. Thousand Oaks, CA: Sage Publications, Inc.
- Richey, R. C., & Klein, J. D. (2014). Design and development research. In J. M. Spector, M. D. Merrill, J. Elen, & M. J. Bishop (Eds.), *Handbook of Research on Educational Communications and Technology* (pp. 141-150). New York: Springer.
- Rogers, T. B. (1995). *The psychological testing enterprise: An introduction*. Pacific Grove, CA: Brooks/Cole Publishing Company.
- Romanosky, S., Hoffman, D., & Acquisti, A. (2013). Empirical analysis of data breach litigation. *iConference 2013 Proceedings*, 124-137. doi:10.9776/13162
- Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting*, 15(4), 353-375.
- Rubin, R. S., & Dierdorff, E. C. (2009). How relevant is the MBA? Assessing the alignment of required curricula and required managerial competencies. *Academy of Management Learning & Education*, 8(2), 208-224.
- Ryan, N. (1997, April 17). Happy Hardcore [E-mail to David Cassel]. Retrieved from <http://www.yaleherald.com/archive/xxiv/10.3.97/exclusive/letter.html>
- S. 1691, 113 Cong., (2014).
- Sahami, S., & Sayed, T. (2013). How drivers adapt to drive in driving simulator, and what is the impact of practice scenario on the research? *Transportation Research Part F: Traffic Psychology and Behaviour*, 16, 41-52.
- Saltzer, J. H. (1974). Protections and the control of information sharing in Multics. *Communications of the ACM*, 17(7), 388-402.
- Scheele, D. S. (1975). Reality construction as a product of Delphi interaction. In H. A. Linstone, & M. Turoff (Eds.), *The Delphi method: Techniques and applications* (pp. 37-71). Reading, MA: Addison-Wesley Publishing Company.

- Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems*, 17(4), 5-32.
- Schwartz, M. S., & Fischer, K. W. (2004). Building general knowledge and skill: Cognition and microdevelopment in science learning. In A. Demetriou & A. Raftopoulos (Eds.), *Cognitive developmental change: Theories, models, and measurement* (pp. 157-185). Cambridge, U. K.: Cambridge University Press.
- Scott, C. (2016, May 18). Protecting our members [Web log]. Retrieved from <https://blog.linkedin.com/2016/05/18/protecting-our-members>
- Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach* (6<sup>th</sup> Ed.). West Sussex, United Kingdom: John Wiley & Sons Ltd.
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of intervention. *Proceedings of the 2010 SIGCHI Conference on Human Factors in Computing Systems*, (pp. 373-382).
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., & Cranor, L. F. (2007). *Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish*. Retrieved from Carnegie Mellon University Research Showcase website: <http://repository.cmu.edu/isr/22/>
- Siponen, M. (2001). Five dimensions of information security awareness. *Computer & Security*, 31(2), 24-29.
- Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-A12.
- Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems*, 37(Article 2). Retrieved from <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3867&context=cais>
- Spidalieri, F., & Kern, S. (2014). *Professionalizing cybersecurity: A path to universal standards and status*. Retrieved from Salve Regina University, Pell Center for International Relations and Public Policy website: <http://www.salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf>
- Spirin, V. (2014). Improving email security and management. *Computer Fraud & Security*, 2014(4), 17-19.

- Spruit, M., & Röling, M. (2014). ISFAM: The information security focus area maturity model. *Proceedings of the European Conference on Information Systems (ECIS) 2014*, Tel Aviv, Israel.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169.
- Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, 4(2), 7-41.
- Sundström, A. (2011). The validity of self-reported driver competence: Relations between measures of perceived driver competence and actual driving skill. *Transportation Research Part F: Traffic Psychology and Behaviour*, 14(2), 155-163.
- Swanson, E. B. (2004). How is an IT innovation assimilated? In B. Fitzgerald, & E. Wynn (Eds.), *IT innovation for adaptability and competitiveness* (pp. 267-287). Dordrecht, Netherlands: Kluwer Academic Publishers.
- Symantec Corporation. (2015). *Internet security threat report: Appendices*. Retrieved from <http://know.symantec.com/LP=1233>
- Tarafdar, M., D'Arcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. *MIT Sloan Management Review*, 56(2), 61-70.
- Terrell, S. (2011). Mixed-methods research methodologies. *The Qualitative Report*, 17(1), 254-280. Retrieved from <http://www.nova.edu/ssss/QR/QR17-1/terrell.pdf>
- Terrell, S. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York, NY: The Guilford Press.
- Terrell, S. (2015). *Writing a proposal for your dissertation*. New York, NY: The Guilford Press.
- Thomas, R., & Lee, C. C. (2015). Development of training scenarios in the flight training device for flight courses at Embry Riddle Aeronautical University. *Journal of Aviation/Aerospace Education & Research*, 24(3), 65-82.
- Thomson, K.-L., & von Solms, R. (2005). Information security obedience: A definition. *Computers & Security*, 24(1), 69-75.
- Torkzadeh, G., & Lee, J. (2003). Measures of perceived end-user computing skills. *Information & Management*, 40(7), 607-615.
- Toth, P., & Klein, P. (2014). *A role-based model for federal information technology / cyber security training* (NIST special publication 800-16 revision 1, 3rd draft).

Retrieved from National Institute of Standards and Technology website:  
[http://csrc.nist.gov/publications/drafts/800-16-rev1/sp800\\_16\\_rev1\\_3rd-draft.pdf](http://csrc.nist.gov/publications/drafts/800-16-rev1/sp800_16_rev1_3rd-draft.pdf)

- Tracey, M. W. (2009). Design and development research: A model validation. *Educational Technology, Research and Development*, 57(4), 553-571.
- Tracey, M. W., & Richey, R. C. (2007). ID model construction and validation: A multiple intelligences case. *Educational Technology, Research and Development*, 55(4), 369-390.
- Trevino, L. K. (1992). Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly*, 2(2), 121-136.
- U.S. Department of Homeland Security, Homeland Security Advisory Council. (2012). *CyberSkills task force report*. Retrieved from <http://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf>
- U.S. Department of Labor, Bureau of Labor Statistics. (2014). *Occupational Outlook Handbook, 2014-15 Edition: Information Security Analysts*. Retrieved from <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>
- U.S. Department of State, & the Broadcasting Board of Governors, Office of Inspector General (OIG). (2012, August). *Office of Inspections: Inspection of Embassy Nairobi, Kenya* (ISP-I-12-38A). Retrieved from <https://oig.state.gov/system/files/196460.pdf>
- U.S. Government Accountability Office (GAO). (2008). *Privacy alternatives exist for enhancing protection of personally identifiable information* (GAO-08-536). Retrieved from <http://www.gao.gov/new.items/d08536.pdf>
- U.S. National Security Council. (2011, May). The comprehensive national cybersecurity initiative. *The White House: Foreign Policy*. Retrieved from <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>
- U.S. Office of Personnel Management. (2015). *Cybersecurity incidents: What happened*. Retrieved from <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>
- Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, 15(10), 679-722.



- Vance, A., Siponen, M., & Pahnla, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3), 190-198.
- Vassiliou, M. C., Dunkin, B. J., Fried, G. M., Mellinger, J. D., Trus, T., Kaneva, P., . . . Marks, J. M. (2014). Fundamentals of endoscopic surgery: creation and validation of the hands-on test. *Surgical Endoscopy*, 28, 704-711. doi: 10.1007/s00464-013-3298-4
- Verizon Enterprise Solutions. (2014). *Verizon 2014 data breach investigations report*. Retrieved from [http://www.verizonenterprise.com/DBIR/2014/reports/rp\\_Verizon-DBIR-2014\\_en\\_xg.pdf](http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf)
- Verizon Enterprise Solutions. (2015). *Verizon 2015 data breach investigations report*. Retrieved from <http://www.verizonenterprise.com/DBIR/2015/>
- Verizon Enterprise Solutions. (2016). *Verizon 2016 data breach investigations report*. Retrieved from <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>
- Verizon Enterprise Solutions, Verizon RISK Team. (2013). *Verizon 2013 data breach investigations report*. Retrieved from [www.verizonenterprise.com/resources/reports/rp\\_data-breach-investigations-report-2013\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf)
- Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology*, 33(6), 1313-1330. doi: 10.1111/j.1559-1816.2003.tb01951.x
- Vogt, W. P., & Johnson, R. B. (2011). *Dictionary of statistics & methodology: A nontechnical guide for the social sciences*. Thousand Oaks, CA: Sage Publications, Inc.
- Wang, Q., Nieveen, N., & van den Akker, J. (2007). Designing a computer support system for multimedia curriculum development in Shanghai. *Educational Technology Research and Development*, 55(3), 275-295.
- Weber, T. (2012). Falling victim: Why users are tricked by phishing attacks (Technical Report LMU-MI-2012-2). In A. Hang, F. Hennecke, S., Löhmann, M. Maurer, H. Palleis, S. Römelin, E. Zezschwitz, A. Butz, & H. Hussmann (Eds.), *User Behavior* (pp. 63-70). Retrieved from <https://www.medien.ifi.lmu.de/pubdb/publications/pub/hang2012userbehaviorHS/hang2012userbehaviorHS.pdf>
- Weigel, F. K., & Hazen, B. T. (2014). Technical proficiency for IS success. *Computer in Human Behavior*, 31, 27-36.

- Wesolek, M. L. 2009. Analysis of the effectiveness of Army helicopter flight training. *Journal of Aviation/Aerospace Education & Research*, 18(2), 69-87.
- Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, 24(1), 43-57.
- Wilkes, M. V. (1968). *Time-sharing computer systems*. New York: American Elsevier.
- Williamson, O. E. (1975). *Markets and hierarchies: Analysis and antitrust implications*. New York: The Free Press.
- Winkler, S., & Dealy, B. (1995, June). Information security technology? Don't rely on it: A case study in social engineering. *Proceedings of the Fifth USENIX UNIX Security Symposium*. Retrieved from [https://www.usenix.org/legacy/publications/library/proceedings/security95/full\\_papers/winkler.pdf](https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/winkler.pdf)
- Wisdom, J., & Creswell, J. W. (2013). *Mixed methods: Integrating quantitative and qualitative data collection and analysis while studying patient-centered medical home model* (AHRQ publication no. 13-0028-EF). Rockville, MD: Agency for Healthcare Research and Quality. Retrieved from <https://pcmh.ahrq.gov/page/mixed-methods-integrating-quantitative-and-qualitative-data-collection-and-analysis-while>
- Xu, Y., & Yeh, C.-H. (2012). An integrated approach to evaluation and planning of best practices. *Omega*, 40(1), 65-78.
- Yadron, D., Ziobro, P., & Devlin, B. (2014, February 15). Target staff had warnings. *The Wall Street Journal, Eastern Edition*, B.1.
- Ziobro, P. (2014, February 07). Data breach at Target began with contractor. *The Wall Street Journal, Eastern Edition*, B.6.