Nova Southeastern University
NSUWorks

CEC Theses and Dissertations

College of Engineering and Computing

2018

Comparing Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs

Jodi Goode
Nova Southeastern University, jp1587@mynsu.nova.edu

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: https://nsuworks.nova.edu/gscis_etd

Part of the Computer Sciences Commons

Share Feedback About This Item

NSUWorks Citation

Jodi Goode. 2018. *Comparing Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1045)
https://nsuworks.nova.edu/gscis_etd/1045.

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.

Comparing Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs

by

Jodi Goode

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

2018

We hereby certify that this dissertation, submitted by Jodi Goode, 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

6/5/2018
Date

James N. Smith, Ph.D.
Dissertation Committee Member

6/5/2018
Date

Anat Hovav, Ph.D.
Dissertation Committee Member

6/5/2018
Date

Approved:

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

6/5/2018
Date

College of Engineering and Computing
Nova Southeastern University

2018

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

Comparing Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs

by
Jodi Goode
June 2018

Organizations, which have established an effective technical layer of security, continue to experience difficulties triggered by cyber threats. Ultimately, the cybersecurity posture of an organization depends on appropriate actions taken by employees whose naive cybersecurity practices have been found to represent 72% to 95% of cybersecurity threats and vulnerabilities to organizations. However, employees cannot be held responsible for cybersecurity practices if they are not provided the education and training to acquire skills, which allow for identification of security threats along with the proper course of action to mitigate such threats. In addition, awareness of the importance of cybersecurity, the responsibility of protecting organizational data, as well as of emerging cybersecurity threats is quickly becoming essential as the threat landscape increases in sophistication at an alarming rate. Security education, training, and awareness (SETA) programs can be used to empower employees, who are often cited as the weakest link in information systems (IS) security due to limited knowledge and lacking skillsets. Quality SETA programs not only focus on raising employee awareness of responsibilities in relation to their organizations' information assets but also train on the consequences of abuse while providing the necessary skills to help fulfill these requirements.

The main goal of this research study was to empirically assess if there are any significant differences on employees' cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) based on the use of two SETA program types (typical & socio-technical) and two SETA delivery methods (face-to-face & online). This study included a mixed method approach combining an expert panel, developmental research, and quantitative data collection. A panel of subject matter experts (SMEs) reviewed the proposed SETA program topics and measurement criteria for CCA per the Delphi methodology. The SMEs' responses were incorporated into the development of two SETA program types with integrated vignette-based assessment of CCA and CyS, which were delivered via two methods. Vignette-based assessment provided a nonintrusive way of measurement in a pre- and post-assessment format. Once the programs had been reviewed by the SMEs to ensure validity and reliability, per the Delphi methodology, randomly assigned participants were asked to complete the pre-assessment, the SETA program, and then the post-assessment providing for the qualitative phase of the study. Data collected was analyzed using analysis of variance (ANOVA) and analysis of covariance (ANCOVA) to address the proposed research hypothesis. Recommendations for SETA program type and delivery method as a result of data analysis are provided.

Acknowledgements

I would not have reached this milestone without guidance from the Lord, who allowed many things to fall into place over the years, providing the opportunity for my pursuit of this Ph.D. I have been fortunate to have an amazing support system throughout this process. This has included friends, co-workers, fellow students, and other researchers that I have had the pleasure of meeting along the way. In addition, I have been especially blessed by a few very special individuals, to whom this work is dedicated.

To my husband, Levi, who provided encouragement, support, and the occasional dose of reality required during this long process. I will forever be grateful for your love and for the personal sacrifices made to ensure I could pursue this dream. Thank you for your unwavering belief in me.

To my parents, Bobby and Cindy, and my grandparents who instilled in me the importance of a strong work ethic, a desire to do my best in whatever I opt to do in life, and an understanding of the benefits of higher education. I am so thankful for you, as well as for my brother, Ryan. You have provided love, support, and encouragement, and without you, obtaining my Ph.D. would not have been possible.

My most sincere appreciation to my dissertation advisor, Dr. Yair Levy. I consider myself very lucky to have had the opportunity to learn from you. You are truly an inspiration, and I am incredibly grateful for your guidance and support throughout the dissertation process. Thank you for believing in me and in the value of my work. I also wish to thank my committee members, Dr. Anat Hovav and Dr. James Smith, for providing direction for this research study that made it truly impactful. Thank you for sharing your expertise and insight throughout the process.

Table of Contents

Chapters

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Concern over cybersecurity breaches continues to grow as organizations gain a greater understanding of the financial ramifications, impact to business reputation, and loss of company information assets that can transpire from cyber threats (D'Arcy, Hovav, & Galletta, 2009; Lebek, Uffen, Neumann, & Hohler, 2013). Employees' naive cybersecurity practices have been found to represent 72% to 95% of cybersecurity threats and vulnerabilities to organizations (D'Arcy et al., 2009; IBM Global Technology Services, 2014). This revelation has initiated research concentrated on technological solutions to secure information systems, motivation of attackers, profile aspects, and loss that can result from the impact of breaches (D'Arcy et al., 2009; Lebek et al., 2013; Vance, Siponen, & Pahnila, 2012). However, organizations that have established an effective technical layer of information security continue to experience difficulties triggered by cyber threats. Ultimately, the cybersecurity posture of an organization depends on appropriate actions taken by employees, who are often cited as the weakest link in information systems security domain (Al-Omari, El-Gayar, & Deokar, 2012b; Albrechtsen, 2007; Rhee, Kim, & Ryu, 2009).

Although systematic enhancements are essential to increase the security of information systems and to strengthen protection of data within organizations, it is also critical that emphasis is placed on ways in which employees' naive cybersecurity actions may be mitigated (Al-Omari et al., 2012b; Bowen, Devarajan, & Stolfo, 2011). D'Arcy et al. (2009) established that implementation of a security education, training, and awareness (SETA) program is critical to the mitigation of cybersecurity threats within an organization. Prior studies have touted the need for SETA, but very few have focused on what SETA should encompass and the factors that are likely to increase success. The development of cybersecurity countermeasures awareness (CCA) as well as cybersecurity skills (CyS) through SETA initiatives is imperative, however, additional research was needed to determine the most valuable program type and delivery method (D'Arcy et al., 2009). Therefore, this study contributed to the body of knowledge by empirically assessing if there are significant differences in CCA along with CyS based on SETA program types and delivery methods.

Problem Statement

The research problem that this study addressed is employees' naive cybersecurity practices, which can lead to organizational hazards including financial implications, impact on business reputation, loss of company information assets, and proprietary information leakage (D'Arcy et al., 2009; Lebek et al., 2013; Vance et al., 2012). Employees' naive cybersecurity practice is defined as unintentional mistakes made by an employee that may expose an organization to potential loss of information assets (Gundu & Flowerday, 2012). These practices may include the use of weak passwords for critical systems, visiting malware infested Websites, responding to phishing attempts, storing login information in an insecure manner, or providing confidential information to unapproved requestors (Gundu & Flowerday, 2012).

Information security encompasses technical measures, policies, risk management approaches, training, and best practices for the protection of information assets. These means can be used to protect an organization's information systems and information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use (Rezgui & Marks, 2008). Cybersecurity, as an all-inclusive term, is often used interchangeably with the term information security, however, it is a subset that focuses on the cyber realm (or cyberspace) (National Institute of Standards & Technology, 2013). According to the ACM Joint Task Force on Cybersecurity Education (2017), cybersecurity is defined as a "computing-based discipline involving technology, people, information, and processes to enable assured operations" (para. 2). It involves the creation, operation, analysis, and testing of secure computer systems and is considered an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries (ACM Joint Task Force on Cybersecurity Education, 2017).

R. Von Solms and Van Niekerk (2013) put forth the idea that the impact of cybersecurity threats goes beyond that of traditional information security. Not only can an individual be personally harmed, but society as a whole can also be directly affected by cyberattacks. As technology becomes increasingly critical for achieving business objectives, state of the art security systems can provide a false sense of protection to organizations (Spears & Barki, 2010). In addition, Hovav and Gray (2014) contend that cyber-attacks not only affect the attacked organization but ripple through the ecosystem impacting other connected organizations, stakeholders, as well as innocent bystanders. Organizational perspective dictates that while technical solutions are imperative, the focus must be placed on the actions of information security management and on advancement toward a secure business environment from the human-centric side of cybersecurity (Ransbotham & Mitra, 2009). Information security managers are tasked with aligning the practices of employees with the desired cybersecurity posture of the organization (Johnston & Warkentin, 2010). Thus, research must encompass the human-centric lens, as employees are often the potential targets or unintentional facilitators in cyberattacks (R. Von Solms & Van Niekerk, 2013).

The human aspect of cybersecurity is many faceted and plays a substantial role in ensuring the security of systems, information, and data (Furnell & Clarke, 2012). Systematic improvements are essential to increase the security of systems and data within organizations, however, it is also critical that more is known about mitigation of employees' naive cybersecurity practices (Al-Omari et al., 2012b; Bowen et al., 2011). A successful approach to cybersecurity must be comprised of defenses such as the establishment and promotion of policy, security awareness campaigns, as well as training opportunities for all employees (D'Arcy et al., 2009; Furnell & Clarke, 2012).

Although an organization may employ an effective technical layer of information security, organizational cybersecurity posture ultimately depends on appropriate action on the part of the employee (Al-Omari, El-Gayar, & Deokar, 2012a; Rhee et al., 2009). An organization's cybersecurity posture refers to the combination of all policy, procedures, technology, employees' competencies, capabilities, efforts, and projects that make up the total organizational information security resilience to cyber threats (Spears, 2006). In addition, it is also comprised of present employee attitudes, knowledge, and practices in regard to cybersecurity (Gundu & Flowerday, 2012; Rhee, Ryu, & Kim, 2005). D’Arcy et al. (2009) focused on security incidents within the organization and utilized 269 employees from eight different companies. In order to encourage a positive organizational cybersecurity posture, their research found raising employee awareness of security policies, as well as the implementation of SETA programs to be beneficial in mitigating cybersecurity threats (D’Arcy et al., 2009). SETA programs can be used to empower employees, who are often cited as the weakest link in information systems (IS) security due to limited knowledge and lacking skillsets (Albrechtsen, 2007).

SETA programs not only focus on raising employee awareness of responsibilities in relation to their organizations’ information assets but also train on the consequences of abuse while providing the necessary skills to help fulfill these requirements (D'Arcy & Hovav, 2007). Therefore, development of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) through SETA initiatives is critical to the mitigation of cybersecurity threats (D’Arcy et al., 2009). Straub and Welke (1998) used the term security countermeasures to collectively describe a mix of procedural and technical controls to mitigate IS risk. Building upon previously used security countermeasures definitions, CCA can be said to include employee awareness of cybersecurity policies, SETA programs, computer monitoring, and computer sanctions (Choi, Levy, & Hovav, 2013; D’Arcy et al., 2009). CCA can also be described as the state where individuals are aware of their cybersecurity mission within the organization (Katz, 2005; Rezgui & Marks, 2008). Awareness of the importance of cybersecurity, the responsibility of protecting organizational data, as well as of emerging cybersecurity threats is quickly becoming essential as the threat landscape is increasing in sophistication at an alarming rate (Choo, 2011; Shaw, Chen, Harris, & Huang, 2009).

Employees cannot be held responsible for cybersecurity practices if they are not provided the education and training to acquire skills, which allow for identification of information security threats along with the proper course of action (Choi et al., 2013; B. Von Solms & Von Solms, 2004). Boyatzis and Kolb (1991) defined skill as a "combination of ability, knowledge, and experience that enables a person to do something well" (p. 280). Skill is also described as the capability to utilize knowledge, intellectual capabilities, and past experiences to perform the best course of action well in a given situation (Choi et al., 2013; Levy, 2005). Accordingly, cybersecurity skill "corresponds to an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS in protecting their information technology against damage, unauthorized use, modification, and/or exploitation" (National Initiative for Cybersecurity Careers & Studies, 2014). While computing skills have been the focus of IS literature, studies such as that of Torkzadeh and Lee (2003) have failed to evaluate the role of skills in the mitigation of cybersecurity threats (Choi et al., 2013).

The majority of employees are not aware of or do not truly care about the importance of protecting personal and organizational information or IS. Therefore, their naive cybersecurity practices reflect this lack of understanding (Thomson & Von Solms, 2005). Research suggests that the cost to comply with security policies is much higher than the potential losses (in the form of punishment) that users might sustain (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009). To this point, Vance et al. (2012) utilized 42 graduate students to study the importance of awareness and education efforts for IS security compliance and found that more than half of IS security breaches were caused by naive actions on the part of the individual. B. Von Solms and Von Solms (2004) stated that addressing this naive practice with the implementation of SETA programs is imperative. Recent studies provide evidence that employees' naïve practices continue to be a cause for organizational concern when it comes to cybersecurity (Choi et al., 2013; D'Arcy et al., 2009; Vance et al., 2012).

The ultimate purpose of organizational learning is to bring about a positive change in the work environment and employees' practices (Cheng, Wang, Yang, & Peng, 2011; Park & Wentling, 2007). IS security training is designed to produce cognitive change, affecting the decisions of the individual in relation to the secure use of IS and ensuring the employee realizes the value in complying. However, many SETA programs focus on the memorization of organizational IS security policies and procedures (Parrish & Nicolas-Rocca, 2012). These typical SETA campaigns often involve coercion, fear tactics, or perception of external pressures, which previous studies found to have no influence on employee compliance with organizational IS policies (Kranz & Haeussinger, 2014). Typical SETA programs fall short in that they do not employ socio-technical philosophies, providing a means for employees to see how training materials correlate to their day-to-day practices (Kruger & Kearney, 2006; Netteland, Wasson, & Morch, 2007). Socio-technical philosophies embrace social as well as technical elements for optimal design and use of organizational systems (Davis, Challenger, Jayewardene, & Clegg, 2014). Training and education efforts are more effective if they not only outline what is expected, but also provide an understanding of why this is important to the individual (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

While training was once conducted almost exclusively face-to-face, technological advances now allow learning to occur on demand and virtually anywhere (Kraiger & Ford, 2006). Advancing organizational understanding of how to best design and deliver training and development has garnered the attention of researchers for years. Early IS research focused on traditional training methods in a classroom environment, however, e-learning methods are increasingly being used as an approach for the enhancement of skills and knowledge (Arbaugh, Desai, Rau, & Sridhar, 2010; Levy, 2006; Salas, Kosarzycki, Burke, Fiore, & Stone, 2002). A considerable amount of research in the education realm has focused on the comparison of face-to-face and online learning. Both face-to-face and online training delivery methods have their advantages, and in previous research, both have been deemed successful (Gupta, Bostrom, & Huber, 2010). However, with online training in organizations becoming more prominent, it is crucial that empirical research is conducted to increase understanding of how such programs can be designed to improve employee engagement and learning (Orvis, Fisher, & Wasserman, 2009; Sitzmann & Ely, 2010). Although some have found no discernible difference in learning outcomes between training delivered face-to-face vs. online (Clark, 1994; McLaren, 2004), others have found variations by discipline (Smith, Heindel, & Torres-Ayala, 2008) and delivery method (Faux & Black-Hughes, 2000). Research suggests that courses in topics such as management and marketing may be more conducive to successful learning outcomes via online delivery than disciples like finance (Arbaugh, Bangert, & Cleveland-Innes, 2010). Likewise, the question of whether online students learn and retain as much of the course content as face-to-face students has yet to be definitely answered (Callister & Love, 2016). Cybersecurity specific training for the organization is a new and increasingly important discipline, making it imperative that the most effective delivery method for the specific program type be empirically investigated (Paul, 2014).

Much of the previous research regarding design and delivery of training has focused on university education outcomes (Callister & Love, 2016). While learning in a university environment may provide some similarities to employee learning within the organization, differences based on the factors of age, role in the organization, and previous education level must be considered. Additionally, to better understand organizational SETA programs, it is imperative that attention is given to the impact of learning delivery method on skills-based forms of instruction (Arbaugh, DeArmond, & Rau, 2013). Callister and Love (2016) stated that skills-based forms of instruction have received little attention to date. Their empirical research compared differences in online and face-to-face skills-based instruction and found that both groups mastered the course content at essentially the same rate, while students in the face-to-face format showed better mastery of the actual skills (Callister & Love, 2016). Parlamis and Mitchell (2014) came to a similar conclusion in their study of 37 masters students in face-to-face and online sections of the same course. While grades were comparable, those taking the online course reported lower levels of learning (Parlamis & Mitchell, 2014).

Organizations seek to best utilize training funds and resources and to produce a motivated employee who has the skills needed to apply their training to job-related tasks. However, organizational training usually provides skills that employees can utilize to improve their job performance, while the same is not true about cybersecurity-focused SETA. Thus, empirical research is needed to determine the effectiveness of different types of SETA programs (typical vs. socio-technical) (Kruger & Kearney, 2006; Parrish & Nicolas-Rocca, 2012). Additionally, a better understanding of such SETA program types delivered via face-to-face and online methods appears to be valuable for both researchers and practitioners alike (Gupta et al., 2010).

Dissertation Goal

The main goal of this research study was to empirically assess if there are any significant differences on employees' cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) based on the use of two SETA program types (typical & socio-technical) and two SETA delivery methods (face-to-face & online). Previous research has focused on the decisions made by the individual that cause damaging effects, not out of maliciousness, but because they lack the skill level required to respond to threats in a conscious way (Rhee et al., 2009; Stanton, Stam, Mastrangelo, & Jolton, 2005). Employee practices are a key factor in the mitigation of cybersecurity threats within the organization. Consequently, there is a need to develop good cybersecurity practice on the part of the employee and to promote compliance with information security policies (Bulgurcu et al., 2010; Vance et al., 2012). CCA has been found to influence cybersecurity practices by producing employees that think through and anticipate 'what if' scenarios, preparing them to apply the learned CyS when required (Ross, 2006). Therefore, this study assessed if there are any significant differences on employees' CCA and CyS based on SETA program type and delivery method.

The need for this work is demonstrated by the research of Dinev, Goo, Hu, and Nam (2009), which focused on the impact that computer self-efficacy and virtual working status had on the deterrent effectiveness of security countermeasures (security policies, SETA programs, & computer monitoring) on computer misuse intention. Choi et al. (2013) built upon their work by expanding the research to determine the role of computer self-efficacy, CCA, and CyS on computer misuse intention. Based on survey results from 185 government transportation agency employees, empirical findings led Choi et al. (2013) to recommend additional study on the role of SETA programs on cybersecurity skills development. However, Choi et al. (2013) have several limitations. First, the construct of computer self-efficacy provides measurement, not of the skill of the individual but is a self-assessment of his/her perceptions about their capability to execute certain courses of action (Bandura, 1997; Choi et al., 2013; Compeau & Higgins, 1995). Secondly, grounded empirical studies have found the basing of research upon intention to comply with information security policies and procedures to be a significant limitation, as intention does not necessarily translate to practice (Vance et al., 2012). Finally, survey-based self-assessment measures have been used in other studies and were found to be generally ineffective predictors of security practice (Vance, Anderson, Kirwan, & Eargle, 2014).

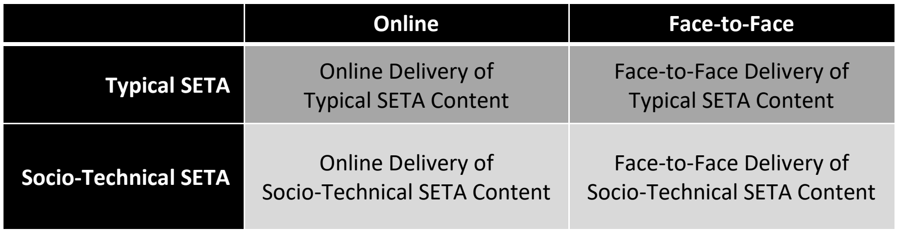
Additional challenges for the determination of SETA program outcomes competency are posed by the existing measures of CyS and CCA, which are dated and limited (Carlton & Levy, 2015). To address this, Carlton (2016) developed a CyS index and a corresponding vignette-based assessment (MyCyberSkills™) of employee skills in relation to cybersecurity. Likewise, due to difficulties with prior construct measures, it was important that further research be conducted to develop and validate a measurement tool to properly assess the CCA level of employees. For the purposes of this research, vignette-based assessments of CCA and CyS were utilized. According to Finch (1987), vignettes are "short stories about hypothetical characters in specified circumstances, to whose situation the interviewee is invited to respond" (p. 105). The vignettes were drafted using anonymized situations based on previous cybersecurity research (D'Arcy et al., 2009; Hovav & D'Arcy, 2012). Each vignette was designed to appear plausible to participants and was validated by cybersecurity SMEs (Barter & Renold, 1999; Neff, 1979).

Vignettes have been used in various disciplines to study a range of topics, including emergency management (Alexander, 2000), nursing and medical students (Gould, 1996; Hughes & Huby, 2002; Schigelone & Fitzgerald, 2004), management (Hall, Mero, & Cheramie, 2017), in the social sciences (Finch, 1987; Wilks, 2004), and more recently in IS and cybersecurity specific studies (Carlton, 2016; D'Arcy et al., 2009; Hovav & D'Arcy, 2012). Gould (1996) popularized the use of vignettes as a part of training and assessment, while their use is now prevalent in fields such as human resources and aviation as an integrated piece of organizational learning. The vignette approach has grown in popularity with the increasing recognition of questionnaire limitations and has been found particularly useful for awareness topics (Hughes & Huby, 2002). The ability to modify the story to be consistent with any research topic, the relaxing nature of the 'story-telling' process, as well as the hypothetical and general nature of the vignette allow for depersonalization that leads to an ease of obtaining information from the participant (Finch, 1987; Schoenberg & Ravdal, 2000). Also referred to as scenarios or simulations in previous research, vignettes have been found to be a versatile means of training personnel as they bridge the gap between instruction and practical training (Alexander, 2000).

The Delphi methodology was employed to validate and improve upon the developed CCA vignette-based assessment, which in conjunction with the CyS assessment validated by Carlton (2016), were applied as both a pre- and post-assessments during SETA program delivery. The Delphi methodology is used when a group is needed to ensure that all aspects of a problem are considered (Gray & Hovav, 2008). It has also been found useful in situations where accurate information is unavailable as the cyclical process aims to achieve an informed judgment with consensus on a particular topic (Best, 1974; Brown, 1968). This methodology has been found to efficiently utilize a group communication process to refine measures based on the input of the expert panel (Ramim & Lichvar, 2014). Per best practice, Delphi surveys were administered by a facilitator and anonymity provided to the SMEs to ensure they were not influenced by the responses of others (Gray & Hovav, 2008). According to Clayton (1997), the panel size can vary depending on the complexity and the expertise required for consensus on the topic. Best practice for homogeneous populations, such as cybersecurity SMEs, is a panel of 15 to 30 professionals with diverse backgrounds and expertise within the field, as well as varying in age and education (Clayton, 1997).

While traditional training has been held in face-to-face format, online methods are increasing in popularity as they have proven to be cost-effective, flexible options for organizations (Dimeff et al., 2009; Salas et al., 2002; Vernadakis, Antoniou, Giannousi, Zetou, & Kioumourtzoglou, 2011). However, more work is needed to determine the most successful delivery method for cybersecurity-focused SETA programs. For the purposes of this research, the SETA programs were delivered via online and face-to-face methods. The pre- and post-assessments were used to determine if there are significant differences in the CCA and CyS of the employee based on delivery method.

Two SETA program types were developed: 1) a typical SETA program that informed the employee of organizational policies and actions that should and should not be taken, as well as 2) a socio-technical SETA program that also included explanations of why certain actions may cause difficulties and the potential organizational outcomes associated (See Figure 1). An expert panel provided input to ensure the validity of the two SETA programs' content per the Delphi methodology and participants were randomly assigned.



	Online	Face-to-Face
Typical SETA	Online Delivery of Typical SETA Content	Face-to-Face Delivery of Typical SETA Content
Socio-Technical SETA	Online Delivery of Socio-Technical SETA Content	Face-to-Face Delivery of Socio-Technical SETA Content

Figure 1. Quasi-experimental factorial design for SETA program types and delivery methods.

Vance et al. (2012) addressed a gap in the body of knowledge by examining the influence of past behavior on individuals' compliance with information policies. Vance et al. (2012) utilized the full model of protection motivation theory (PMT) to investigate the impact of past information security compliance behavior on threat appraisal and coping responses. PMT suggests that past behavior will have a significant influence on the process of accessing threats and on an individuals' ability to cope with the threat (Boer & Seydel, 1996; Limayem & Hirt, 2003; Vance et al., 2012). Protection motivation processes attempt to influence individuals' established practices and typical response. However, the work of Vance et al. (2012) was limited by the use of intention as a dependent variable, and the measurement of compliance in only four scenarios, which might not work well for all employees or in all organizational situations. Additionally, the use of PMT should be done with caution since the assertion that users view security risk the way they view health risk was questioned in subsequent work (Hovav & Putri, 2016; Johnston, Warkentin, & Siponen, 2015; Putri & Hovav, 2014).

Putri and Hovav (2014), as well as Johnston et al. (2015), suggest that PMT-grounded IS studies miss the dimension of personal relevance, which is critical to ensuring employees are not only aware of cybersecurity risks but that they realize their personal role in the protection of organizational information assets. Selective attention theory (SAT) suggests that information is recognized but quickly forgotten unless it holds personal relevance to the individual (Deutsch & Deutsch, 1963). SAT has been determined to play a significant role in learning outcomes by Yli-Krekola, Särelä, and Valpola (2009) and was used as an underlying theory in the foundation of this study. Although theoretical approaches to SAT have varied, previous research has found that individuals have a tendency to orient themselves toward, or process information from only one part of the environment while excluding other parts (Broadbent, 1958; Treisman, 1960).

Oyserman (2009) put forth the idea that for education efforts to be successful, participants must identify with the content, providing the aspect of personal relevance. Once that identity is formed, action and procedural readiness can be called upon without conscious awareness (Oyserman, 2009). This is especially important for cybersecurity-focused education, where awareness is key and skills must be called upon quickly when threats arise. Oyserman (2009) formed a theoretical model known as identity-based motivation (IBM) that focuses on the motivational pull toward identity-congruent action as well as related cognitive procedures. IBM proposes that cognition and action are not separate from contexts but instead, are dynamically shaped by them (Oyserman, 2009). Research studies in healthcare, consumer behavior, and school outcomes have tested the prediction that students would be more engaged and invested in the topic if they were led to relate training content to previous experiences, providing context (Oyserman, 2008, 2013; Oyserman & Smith, 2015; Oyserman, Smith, & Elmore, 2014). Likewise, this study tested the outcomes when using typical vs. socio-technical SETA programs to determine if there are significant differences in employee CCA and CyS, which were determined based on comparison data from the pre- and post-assessments.

This dissertation study built on previous research by D'Arcy et al. (2009), Levy (2005), Choi et al. (2013), Vance et al. (2012), Oyserman (2009) and Dinev et al. (2009). PMT and IBM will serve as the foundational theories for comparison of SETA delivery method as well as program type on the CCA and CyS of the employee. In addition, the Delphi methodology was utilized to validate an assessment instrument developed to measure CCA as part of the SETA programs' delivery. The first specific goal of this research study developed and assessed the SMEs' approved topics for two SETA program types using the Delphi methodology. The second specific goal of this research study developed and assessed the SMEs' approved measurement criteria for CCA using the Delphi methodology. The third specific goal of this research study assessed the SMEs' approved weights for the three CCA categories (awareness of policy, SETA, & monitoring). The fourth specific goal of this research study developed and assessed the SMEs' approved two SETA programs with integrated vignette-based pre- and post-assessments for CCA and CyS using the Delphi methodology. The fifth specific goal of this research study was a pilot of the vignette-based pre- and post-assessments of CCA and CyS to empirically assess if there are significant differences between the two SETA program types and the two SETA delivery methods. The sixth specific goal of this research study utilized the vignette-based pre- and post-assessments to empirically assess if there are significant differences in employees' CCA and CyS between the two SETA program types, and the two SETA delivery methods. The seventh specific goal of this research study empirically assessed if there are any significant differences in employees' CCA and CyS between the two SETA program types, and the two SETA delivery methods when controlled for demographic factors.

Research Questions

The main research question (RQ) that this study addressed is: Are there any significant differences in employees' CCA and CyS between two SETA program types and two SETA delivery methods?

Development and validation of a measurement tool to properly assess the CyS and CCA level of employees was imperative to this research study due to the limitations of construct measurement in previous research. To address this need, the first four specific RQs focused on the use of the Delphi methodology to determine SMEs' approved measurement criteria for CCA, weights of the three CCA categories, as well as the development of two SETA programs with integrated vignette-based assessment.

RQ1: What are the SMEs' approved topics for the two SETA program types using the Delphi methodology?

RQ2: What are the SMEs' approved measurement criteria for CCA using the Delphi methodology?

RQ3: What are the SMEs' approved weights for the three CCA categories (awareness of policy, SETA, & monitoring)?

RQ4: What are the SMEs' approved two SETA programs with integrated vignette-based assessments for CCA and CyS using the Delphi methodology?

The next three research questions addressed the results of the pilot and main study in relation to CCA and CyS levels of employees. Pre- and post-assessment allowed for a better understanding of significant differences between two SETA program types and two SETA delivery methods. Examination of these research questions expanded the body of knowledge, providing insight into the most effective use of organizational resources as cybersecurity threats become an increasing concern to information assets, information systems, and day-to-day operations.

RQ5: Are there any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using a pilot group of participants?

RQ6: Are there any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study group of participants?

RQ7a-e: Are there any significant differences between the two SETA program types, and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study participants, when controlled for participants' (a) age, (b) gender, (c) role in the organization, (d) highest

educational level, (e) years working at the organization, and (f) years since last attended formal education?

The specific hypotheses for RQ5 and RQ6 (in null form) were:

Ho1a: There will be no statistically significant mean differences in employee's pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the typical SETA program based on the two delivery methods (face-to-face & online).

Ho1b: There will be no statistically significant mean differences in employee's pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the socio-technical SETA program based on the two delivery methods (face-to-face & online).

Ho2: There will be no statistically significant mean differences on employee's cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) between the two SETA program types (typical & socio-technical).

Ho3: There will be no statistically significant interaction between the two SETA program types and the two delivery methods.

Figure 2 presents the conceptual map for this research. All measures were tested between comparisons for SETA type (typical & socio-technical) and delivery method (face-to-face & online) shown in Figure 1.

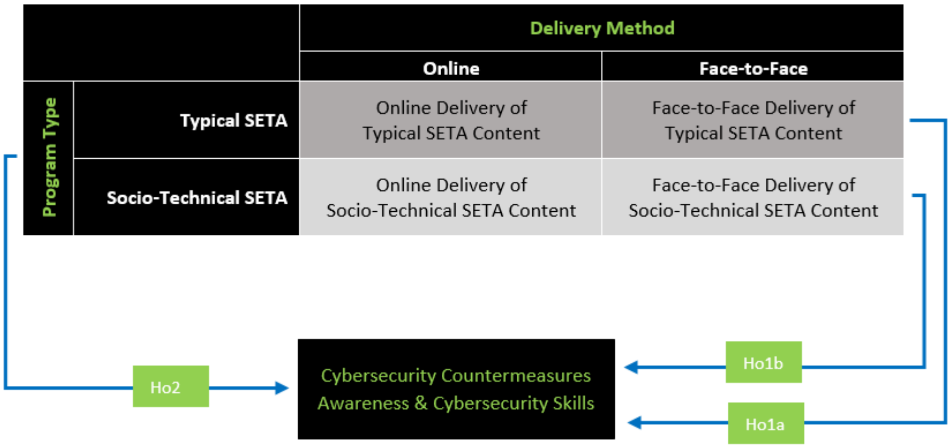

Delivery Method
Online
Face-to-Face
Program Type
Typical SETA
Online Delivery of Typical SETA Content
Face-to-Face Delivery of Typical SETA Content
Socio-Technical SETA
Online Delivery of Socio-Technical SETA Content
Face-to-Face Delivery of Socio-Technical SETA Content
Ho2
Cybersecurity Countermeasures Awareness & Cybersecurity Skills
Ho1b
Ho1a

Figure 2. Research design for comparisons of SETA program types and delivery methods.

Relevance and Significance

Relevance of this Study

Companies in the United States continue to lead the world in losses from cyberattacks, with 58 organizations recently reporting the mean cost per organization for 2015 as $12.7 million (Ponemon Institute, 2015). The protection of an organization's information systems and information assets from cybersecurity threats is increasingly important in today's world, especially as businesses become more reliant upon technology for daily business processes (D'Arcy et al., 2009). Employees who lack knowledge and skillsets are seen as a susceptible threat vector for cyberattacks, and therefore, are being targeted with continually evolving threats (Jang-Jaccard & Nepal, 2014). A study of 252 global organizations found nine key cyberattack vectors, most of which focused on the human factor in information security including viruses, malware, Web-based attacks, phishing and social engineering, malicious code, denial of services, as well as stolen devices (Ponemon Institute, 2015). Due to emerging cybersecurity threats that are now evolving rapidly and increasing in both number and sophistication, research in this area continues to be relevant (Choo, 2011; Jang-Jaccard & Nepal, 2014).

Significance of this Study

Despite considerable investment in organizational security, the majority of approaches and protection methods focus heavily on external attacks and technological defenses and have not minimized the number of security incidents (Pahnila, Siponen, & Mahmood, 2007). However, Abawajy (2012) point out that the organization is only as secure as its weakest link. Given the importance of organizational focus on IS security with a human-centric lens, the significance of this study is substantial (Furnell & Clarke, 2012). Expanding knowledge of both CCA and CyS, as well as SETA program type and delivery method are significant not only to add to the body of knowledge in relation to cybersecurity, but also for practitioners who are charged with protecting organization IS assets (Choo, 2011; Shaw, Chen, Harris, & Huang, 2009). Providing empirically validated data on the most beneficial SETA program type and delivery method for cybersecurity training will assist organizations as they decide how to best use resources for training of employees on this critical aspect of daily business. This knowledge will increase organization efficiency and decrease the chance for losses due to naïve employee cybersecurity behaviors.

Barriers and Issues

There were several potential issues with the conducting of this research. First, there was concern that the responses of the SMEs participating in the Delphi process might not be constructive if the request for SETA topics and related measurement criteria permits only open-ended responses. To address this concern, the expert panel survey was direct, as clear as possible, as well as based on prior research and previously validated assessment instruments. Reliability of the measurement tools developed for CCA was also a concern. To mitigate this potential issue, in addition to SME panel review, a pilot study was utilized to ensure validity and reliability before moving on to the main study.

Additionally, quasi-experiment design using pre- and post-assessment methods must be mindful of sensitization which can occur when participants are informed of what is to come (Salkind, 2011). If the study is not designed properly, this can impact scores which would decrease the internal validity of the research completed. A control group was given the pre- and post-assessment to address this issue, and did not complete either of the two SETA programs. Finally, organizational permission to administer the two SETA programs with integrated vignette-based assessments was required for this study, as well as Institutional Review Board (IRB) approval. All approvals were received and appropriate processes for studies involving human subjects followed during the course of the research study (See Appendices A, B, & C).

Limitations and Delimitations

Limitations

A limitation of this study is related to employee tendency to provide the expected or socially acceptable answers to cybersecurity assessments. Not only are some responses considered more socially desirable than others, employees are apt to attribute failures or problems to others or to circumstances beyond their personal control (Podsakoff & Organ, 1986). The vignette-based assessments for CCA and CyS reduce this risk through the expert panel participation in development, as well as through testing during the pilot study. All results were carefully interpreted within the cybersecurity context, especially those areas which might be more susceptible to such biases (Verplanken & Orbell, 2003).

This research study was conducted at a single, small private university in the United States. The SETA program has been implemented within the University as a workforce training initiative, which may lend itself to bias. In addition, a related limitation is culture of the participants. As such, additional research will be needed to assess the measures within other countries, especially those with a different culture than exists in the United States, along with replicating the findings with other types of organizations, organization size, organization culture, and varying population demographics.

Delimitations

This study was limited to research participants from a single, higher education university. The sample includes employees (both faculty and staff) who have had no previous formal cybersecurity or information security training while employed by the University. The online version of the SETA program content was limited to delivery through the Blackboard online learning system and all assessments were delivered anonymously via Google Forms.

Definition of Terms

Below is a list that defines the terms and acronyms used in this study.

Cybersecurity - Defined by ACM Joint Task Force on Cybersecurity Education (2017) as a "computing-based discipline involving technology, people, information, and processes to enable assured operations" (para. 2). Cybersecurity is an all-inclusive term often used interchangeably with the term information security, however, it is a subset that focuses on the cyber realm (or cyberspace) (National Institute of Standards & Technology, 2013).

Cybersecurity Countermeasures Awareness (CCA) - Includes employee awareness of security policies, SETA programs, computer monitoring, and computer sanctions (Choi et al., 2013; D'Arcy et al., 2009). CCA can also be described as the state where individuals are aware of their cybersecurity mission within the organization (Katz, 2005; Rezgui & Marks, 2008).

Cybersecurity Skills (CyS) - "Corresponds to an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS in protecting their information technology against damage, unauthorized use, modification, and/or exploitation" (National Initiative for Cybersecurity Careers & Studies, 2014).

Delphi Expert Methodology – This methodology is used in situations where accurate information is unavailable and aims to achieve an informed judgment with consensus on a particular topic (Best, 1974; Brown, 1968). The Delphi methodology has been found to effectively utilize a group communication process to refine measures based on the input of an expert panel (Ramim & Lichvar, 2014).

Identity-based Motivation Theory (IBM) - A theoretical model that focuses on the motivational pull toward identity-congruent action as well as related cognitive procedures. IBM proposes that cognition and action are not separate from contexts but instead, are dynamically shaped by them (Oyserman, 2009).

Information security - Encompasses technical measures, policies, risk management approaches, training, and best practices for the protection of information assets. These means can be used to protect an organization's information systems and information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use (Rezgui & Marks, 2008).

Protection Motivation Theory (PMT) – PMT suggests that past behavior will have a significant influence on the process of accessing threats and on an individuals' ability to cope with the threat (Boer & Seydel, 1996; Limayem & Hirt, 2003; Vance et al., 2012). Protection motivation processes attempt to influence individuals' established practices and typical response.

Security Education, Training, and Awareness Programs (SETA) – Organizational learning used to empower employees by increasing their knowledge and awareness and increasing skillsets (Albrechtsen, 2007).

Selective Attention Theory (SAT) - SAT suggests that information is recognized but quickly forgotten unless it holds personal relevance to the individual (Deutsch & Deutsch, 1963).

Skill - "Combination of ability, knowledge, and experience that enables a person to do something well" (p. 280) (Boyatzis & Kolb, 1991).

Vignettes – Vignettes are "short stories about hypothetical characters in specified circumstances, to whose situation the interviewee is invited to respond" (p. 105) (Finch, 1987).

Summary

This study addressed cybersecurity threats to organizational IS which are due to limited skillsets and naïve cybersecurity practices of employees. Approximately 72% to 95% of the cybersecurity threats and vulnerabilities for organizations have been linked to the naive cybersecurity practices of employees (D'Arcy et al., 2009; IBM Global

Technology Services, 2014). While technical security is crucial within organizations to enhance the security of information systems and to protect data, it is also imperative that emphasis is placed on ways in which employees' naive cybersecurity actions may be mitigated (Al-Omari et al., 2012b; Bowen et al., 2011).

D'Arcy et al. (2009) established that implementation of an organizational SETA program is essential to the mitigation of cybersecurity threats. Prior studies have promoted use of organizational SETA programs but very few have focused on what SETA should include and how it should be delivered to produce the most favorable results. The development of CCA as well as CyS through SETA initiatives is imperative, however, additional research is needed to determine the most valuable program type and delivery method (D'Arcy et al., 2009). Therefore, this study empirically assessed if there are significant differences in CCA along with CyS based on SETA program types and delivery methods.

Chapter 2

Review of the Literature

Introduction

In this chapter, a literature review is presented to provide a synopsis of the relevant literature related to cybersecurity threats, countermeasures awareness, skill and organizational SETA programs as well as to lay the theoretical foundation for this study. According to Hart (1998), the literature review will assist in the discovery of existing knowledge (both historically and in current research) and provide a basis for research question development through identification of areas of concern, interest, and neglect. A quality foundation is critical for any research study, which then allows for a quality research contribution (Levy & Ellis, 2006). This examination is interdisciplinary in nature, involving an extensive search of IS literature using several databases from fields including IS, business, and psychology. From the literature review process, important constructs were identified in the literature domain relating to naïve employee cybersecurity behavior: cybersecurity countermeasures awareness (CCA), cybersecurity skill (CyS), and security education, training, and awareness programs (SETA). A comprehensive study of these areas was conducted to determine the existing knowledge base, research questions, approach, and theoretical foundation for this research study. Furthermore, proposed vignettes for the assessment of CCA and SETA program topics were drafted using literature from this review.

Cybersecurity Threats

Computer networks and information technology solutions have become critical to the everyday operation of today's society, economy, and critical infrastructures (Jang-Jaccard & Nepal, 2014). As organizational reliance on technology increases, cyberattacks become more attractive to attackers and increasingly devastating to organizations (Choo, 2011). Cybersecurity threats and vulnerabilities are causing substantial financial forfeiture, impact to business reputation and continuity, as well as loss of company information assets (D'Arcy et al., 2009; Lebek et al., 2013). The number of cyberattacks continues to escalate because they are cheaper, more convenient, less risky than physical attacks, and are unconstrained by geographic location or distance (Jang-Jaccard & Nepal, 2014). Due to lacking knowledge and skillsets, humans are often considered the most susceptible threat vector for cyberattacks, and therefore, are being targeted with continually evolving threats.

Approximately 72% to 95% of the cybersecurity threats and vulnerabilities for organizations have been linked to the naive cybersecurity practices of employees or contractors (D'Arcy et al., 2009; IBM Global Technology Services, 2014). Of these, most security incidents are attributed to current or former employees of the organization (PricewaterhouseCoopers, 2016). IBM Global Technology Services (2014) found the most prevalent practice to be unsafe Web browsing which can lead to IS compromise via malware. Malware is the leading tool used by cyber-attackers to carry out malicious acts and is known to advance rapidly to capitalize on new approaches to exploit flaws in emerging technologies (Jang-Jaccard & Nepal, 2014). Furthermore, social engineering attacks are on the rise and are "now considered the great security threat to people and organizations" (Algarni, Xu, Chan, & Tian, 2014). Even the most technologically advanced IS security measures can be thwarted by social engineering, which utilizes tactics to trick victims into compromising personal or organizational security defenses through phishing, vishing (voice solicitations), and impersonation (Algarni et al., 2014). While employee awareness of social engineering techniques is important, Kvedar, Nettis, and Fulton (2010) found that even those who classify themselves as aware of these tactics can be fooled. Likewise, an employee with IS knowledge does not necessarily possess the cybersecurity skills required to protect themselves and their organization from threats (Choi et al., 2013). Therefore, expanding knowledge of both countermeasures awareness and skills, as well as SETA program type and delivery method are significant not only to add to the body of knowledge in relation to cybersecurity but also for practitioners who are charged with protecting organization information systems and information assets.

Table 1

Summary of Cybersecurity Threats

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Algarni et al., 2014	Empirical study via survey	78 individuals with social network site accounts	Social engineering	Social engineering is a threat to those with social networking site accounts due to lack of mitigation techniques
Choi et al., 2013	Empirical study via expert reviewed survey	185 respondents from a government transportation agency	Cybersecurity threats, computer self-efficacy, CCA, CyS, computer misuse intention	End-user awareness of monitoring and cybersecurity initiative skill reduced misuse intentions
Choo, 2011	Theoretical		Application of Routine Activity Theory (RAT) to	RAT can be used to reduce opportunities for cybercrime by increasing the risks of

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
			mitigate cybersecurity risk	detection and punishment associated
D'Arcy et al., 2009	Empirical study via survey	269 computer users from eight different companies	User awareness of security countermeasures, perceived certainty, severity of organizational sanctions, and misuse intention	Three practices deter IS misuse: user awareness of security policies, SETA programs, and computer monitoring
Jang-Jaccard & Nepal, 2014	Literature review and synthesis		Cybersecurity vulnerabilities and emerging threats	Mitigation of cybersecurity threats should include both IT and non-IT professionals
Kvedar et al., 2010	Empirical study via vulnerability assessment simulation	Graduate, undergraduate, and high school students	Social engineering	More than 40% failed to perceive social engineering as a threat, and 85% gave the attackers network information
Lebek et al., 2013	Literature review and synthesis		Approaches for employee information security awareness and behavior	Future research should include qualitative studies that focus on factors that influence employees' information security awareness
IBM Global Technology Services, 2014	Empirical study via cyberattack event data	Approximately 1,000 clients from 133 countries	Data breaches	Human error contributed to over 95% of the security events
Pricewaterhouse- Coopers, 2016	Empirical study via survey	Approximately 10,000 business and IT executives	Protection of digital assets and creation of business advantages	Findings show focus on: 1) Adoption of new safeguards for digital business models 2) Implementing threat intelligence and information-sharing programs 3) Securing the potential of the Internet of Things

Motivation Theories

Protection Motivation Theory

Rogers (1975) originally proposed PMT to provide conceptual clarity to the understanding of fear appeals. Maddux and Rogers (1983) later extended PMT to produce a more general theory with an emphasis on the cognitive processes mediating behavioral change. PMT has been used as a framework for influencing and predicting various behaviors such as promoting water conservation, persuading individuals to use less energy, the influence of health education, and increasing preparedness for natural disasters (Boer & Seydel, 1996). Recently, PMT has been applied to the domain of information security and previous work from the organizational perspective has focused on employee compliance with IS security procedures and policies (Vance et al., 2012).

PMT suggests that information about a threat causes a cognitive process in individuals that assessess positive and negative responses (Vance et al., 2012). Therefore, naive cybersecurity actions by the employee are an example of a maladaptive response, while positive cybersecurity actions would be considered an adaptive response. The maladaptive response will invoke threat appraisal factors, which decrease the likelihood of a negative response. The three factors of threat appraisal using PMT are: 1) rewards or benefits, 2) severity of the threat, and 3) the extent to which the individual is perceived to be susceptible to the threat. PMT also includes three coping appraisals: 1) belief in the perceived benefits of the coping action by removing the threat, 2) cost to the individual for implementing the protective behavior, and 3) the degree to which the individual believes it is possible to implement the protective behavior.

PMT has been cited as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Agarwal, Sambamurthy, & Stair, 2000). However, grounded empirical studies have found that basing research on intention to comply with information security policies and procedures to be a limitation (Vance et al., 2012). Furthermore, recent studies found that the relationship between SETA and PMT are not as simple as initially suggested by Vance et al. (2012). Johnston et al. (2015) posit that PMT-grounded IS studies miss the dimension of personal relevance which is critical to ensuring employees are not only aware of cybersecurity risks, but that they realize their personal role in the protection of organizational information assets. Therefore, this research was built upon PMT but sought to adequately measure both CCA and CyS instead of concentrating on intention to comply given that intentions are not the focus of this study.

Table 2

Summary of Protection Motivation Theory

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Agarwal et al., 2000	Empirical study via survey, longitudinal research design	186 undergraduate students	Computer self-efficacy	Greater opportunity for hands-on experience with software package increased aspects of self-efficacy and ease-of-use
Boer & Seydel, 1996	Empirical study via survey	386 women	Health education, information acquisition, intention to participate	Interaction between perceived vulnerability and self-efficacy was the major predictor of intention to participate.
Gundu & Flowerday, 2012	Theoretical		Information security awareness	Information security awareness process to cultivate positive security behaviors. Uses the behavioral intentions model

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Johnston et al., 2015	Empirical study via interviews and expert reviewed survey	559 city government employees in Finland	Compliance intention, personal relevance	Fear appeals should be updated to include persuasive messaging campaigns and highlight personal relevance to increase compliance
Maddux & Rogers, 1983	Empirical study via survey	153 undergraduate students	PMT, self-efficacy expectancy	Provided empirical evidence supporting addition of self-efficacy expectancy as fourth component of PMT
Rogers, 1975	Theoretical		PMT	PMT is proposed. Comprised of three crucial components: 1) magnitude of an event; 2) probability of event occurrence; 3) efficacy of a protective response
Vance et al., 2012	Empirical study via expert reviewed survey	42 graduate students	IS security compliance	Importance of awareness and education efforts for IS security compliance

Identity-Based Motivation

Oyserman (2009) formed a theoretical model known as identity-based motivation (IBM) that focuses on the motivational pull toward identity-congruent action as well as related cognitive procedures. According to Oyserman (2009), for education efforts to be successful, participants must identify with the content. Research studies in healthcare, consumer behavior, and school outcomes have tested the prediction that individuals would be more engaged and invested in the topic if they were able to relate training content to previous experiences, providing context (Oyserman, 2008, 2013; Oyserman & Smith, 2015; Oyserman et al., 2014).

Based on the previous findings of IBM studies, the formation of identity is especially significant for cybersecurity-focused education. An employee who identified with SETA content should possess action and procedural readiness that can be called upon without conscious awareness when threats arise (Oyserman, 2009). IBM proposes that cognition and action are not separate from the context but instead, are dynamically shaped by them (Oyserman, 2009). Due to empirical evidence which points to the importance of personal relevance of content in education and training efforts, the study integrated IBM as a part of the theoretical foundation.

Table 3

Summary of Identity-Based Motivation

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Oyserman, 2008	Empirical study via survey	High school students	Racial-ethnic identity, academic achievement	An identity relevant goal was found to be a predictor of improved academic performance
Oyserman, 2009	Synthesis of previous literature		IBM and action-readiness: consumption, health behaviors and academic performance	Once an identity is formed, action and procedural-readiness can be cued without conscious awareness or systematic processing
Oyserman et al., 2014	Empirical study via survey	Undergraduate students	Experienced difficulty, time investment, and learning outcomes	Results show the interpretation of experienced difficulty matters for learning outcomes
Oyserman & Smith, 2015	Synthesis of previous literature		Dynamic construction, action-readiness, and interpretation of difficulty	People interpret situations in ways that are congruent with currently active identities. When actions feel identity-congruent, the behavior is seen as important and meaningful.

Selective Attention Theory

Attention research has long been a focus of researchers, sparking much debate over the process of selection in the flow of memory storage and information processing. Broadbent (1958) developed one of the prominent foundational models of selective attention theory (SAT) which introduced the use of memory stages as an ordered series. The work proposed that individuals have a tendency to process information from only one part of the environment while excluding other parts. This multistore approach suggested that information is first held in an unanalyzed form in a store of unlimited capacity. Some of this information can then be selected for further processing and then held in a limited capacity, short-term store. Selected information is eventually filed in permanent memory or a long-term store with some form of organization, allowing for retrieval and recall. According to the Broadbent (1958) model, attentional selection occurs early, with rudimentary analysis and processing occurring before information can be entered in short-term memory. Broadbent (1958) concluded that we pay attention to only one channel at a time and that the channel given attention is selected based on physical characteristics of the information coming in (which particular ear the information was coming to, the type of voice, etc.). Since individuals have a limited capacity to process information, this filter was believed to prevent information processing overload. Broadbent (1958) assumed that any messages or information received on an unattended channel were lost at an early stage or processing.

Treisman (1964) agreed that the filtering of messages happens early in the process and that physical characteristics are used. However, empirical evidence from the work of Treisman (1964) proves the findings of Broadbent (1958) to be inadequate, as it does not allow for meaning and relevance to be taken into account by the individual. This led to the suggestion of an updated model that does not include the concept of unattended material per Broadbent (1958) but instead opts to view information from unattended channels as still gathered by the individual and available for processing when the message is deemed relevant.

The order of stores in the original multistore model was soon contested by Deutsch and Deutsch (1963) who put forth an opposing theory of late response selection which assumes perception is an unlimited process that can occur parallel and without the need for selection. According to this approach, selection occurs late in the information processing flow, after full perception, and as information is stored in long-term memory. Deutsch and Deutsch (1963) suggested that multiple channels of information could be recognized by the individual but would be quickly forgotten unless they held personal relevance.

For many years, selection has proven a central question in attention theory with approaches shifting back and forth between early and late selection, as well as on a combination of the two. In addition, the factors of information relevance, cognitive load, and complexity of the response have been thoroughly examined in previous research (Kahneman & Treisman, 1984; Lavie & Tsal, 1994; Von Wright, 1970). While theoretical approaches to selective attention have varied, psychophysical experiments have proven that attention plays a significant role in learning (Yli-Krekola et al., 2009). As proposed by Kahneman (1973), individuals will narrow their attention to information currently believed to be relevant. For this reason, it is important that more is known regarding the role of selective attention in the study of awareness and SETA program effectiveness within the organization.

Table 4

Summary of Selective Attention Theory

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Broadbent, 1958	Traditional		Perception, communication, selective learning, and listening	Developed a model using memory stages as an ordered series. Provided groundwork of selective attention theory
Deutsch & Deutsch, 1963	Traditional		Attention	Proposed late response selection. Assumes perception is an unlimited process that can occur without the need for selection
Kahneman, 1973	Traditional		Attention	Places focus on the role of attention in perception and performance.
Kahneman & Treisman, 1984	Traditional		Attention	Suggest shift from early to late selection was related to shift in the field of attention studies
Lavie & Tsal, 1994	Theoretical		Selection in visual attention, perceptual load	Proposed addition of physical distinctiveness and perceptual load to selective attention factors
Treisman, 1964	Empirical study via laboratory experiment		Selective attention, storage of irrelevant messages	Proves meaning and relevance must be taken into account in SAT
Von Wright, 1970		Undergraduate students	Selection in visual immediate memory	Studied the efficiency of selection from visual immediate memory with focus on the complexity of the response.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Yli-Krekola, Särelä, & Valpola, 2009	Empirical study via experiment	Artificially generated data	Selective attention, learning	Found that selective attention can improve learning. With pre-segmentation, fewer exposures are needed to learn relevant information

Cybersecurity Countermeasures Awareness

Awareness is defined as the extent to which a specific population is cognizant of an innovation and formulates a general perception of what it involves (Dinev & Hu, 2007). Organizational impact from awareness strategies have long been studied in social science, criminal justice, as well as medical behavioral sciences and positively linked to individuals' cognitive development (Dinev & Hu, 2007; Shaw et al., 2009). For awareness to be achieved, an organization or individual must be exposed to the existence of the innovation, while providing information on both how it functions and what its benefits are. Given the level of organizational concern today regarding emerging cybersecurity threats, awareness of the significance of cybersecurity, personal responsibility in protecting organizational data, as well as of recent advances by those with malicious intent is imperative, especially for employees in the context of organizations (Choo, 2011; Shaw et al., 2009).

Straub and Welke (1998) used the term security countermeasures to collectively describe a mix of procedural and technical controls to mitigate IS risk. Building upon previously used security countermeasures definitions, CCA can be said to include employee awareness of security policies, SETA programs, computer monitoring, and computer sanctions (Choi et al., 2013; D'Arcy et al., 2009). CCA can also be described as the state where individuals are aware of their cybersecurity mission within the organization (Katz, 2005; Rezgui & Marks, 2008). Previous studies related to deterrence of naive information security behavior had found positive influence of various security countermeasures (Kankanhalli, Teo, Tan, & Wei, 2003; Lee & Lee, 2002). D'Arcy et al. (2009) extended prior work by focusing on the impact of user awareness of security countermeasures on IS misuse intention. The underlying process through which the security countermeasures of security policy, SETA program, and computer monitoring impacted naive behaviors was explored. However, additional research on countermeasures awareness that specifically focuses on cybersecurity threats is needed to determine the most effective method for organizations to address issues from a human-centric lens.

According to Furnell et al. (1996), the need to promote IS security policy and awareness within the organization requires IS security awareness training. Employees' lack of awareness of threats posed in the cyber realm increases the susceptibility of malicious attacks and organizational losses (Kumar, Mohan, & Holowczak, 2008; Shaw et al., 2009). Consequently, in order for the training program to be considered effective, CCA must be measured and improvement made. Based on this, it can be concluded that the CCA of employees is critical for the mitigation of cybersecurity threats, and therefore, must be assessed and evaluated.

Table 5

Summary of Cybersecurity Countermeasures Awareness

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Choi et al., 2013	Empirical study via expert	185 respondents from a large	Cybersecurity threats and vulnerabilities	End-user awareness of monitoring and cybersecurity initiative

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
	reviewed survey	government transportation agency	utilizing impact of computer self-efficacy, CCA, and CyS on computer misuse intention	skill reduced misuse intentions
Choo, 2011	Theoretical		Application of Routine Activity Theory (RAT) to mitigate cybersecurity risk	RAT can be used to reduce opportunities for cybercrime by increasing the risks of detection and punishment associated
D'Arcy et al., 2009	Empirical study via survey	269 computer users from eight different companies	User awareness of security countermeasures, perceived certainty and severity of organizational sanctions, and misuse intention	Three practices deter IS misuse: user awareness of security policies, SETA programs, and computer monitoring
Dinev & Hu, 2007	Empirical study via survey	339 IS professionals and university students	IS security awareness, protective technologies	Confirmed that technology awareness is a determinant of behavioral intention toward protective technologies
Furnell et al., 1996	Empirical study via survey	Employees (both general users and technical staff) of one European organization	Employee awareness and attitudes toward security	Established that organizational culture is important in determining level and types of security that will be accepted.
Kankanhalli et al., 2003	Empirical study via survey	164 IS managers	IS security deterrent efforts, deterrent severity, and preventative efforts	Developed an integrative model of IS security effectiveness. Greater deterrent efforts and preventive measures were found to lead to enhanced IS security effectiveness
Katz, 2005	Empirical study via survey	University faculty and staff	Information security awareness	Findings indicated that employees need to become more aware of IS security and skilled in using technical security methods

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Kumar et al., 2008	Empirical study via survey	130 university students	Awareness of security measures, attitude, intention to use protective technologies	Attitude plays an important role in shaping users' intention to use protective technologies
Rezgui & Marks, 2008	Empirical study via questionnaire, interview, and observation	45 questionnaire participants and seven interview participants from a higher education university	IS security awareness	Recommendations to establish IS security awareness and an understanding of IS security within the organization
Shaw et al., 2009	Empirical study via laboratory experiment	240 graduate students	Information security awareness	Recommendations for information security awareness training via online delivery method
Straub & Welke, 1998	Empirical study via comparative qualitative interviews	37 managers and professionals from Fortune 500 firms	Mitigation of IS security risk	Identified an approach for IS security risk using a theory-based security program. Includes security risk planning, SETA, and countermeasure analysis

Security Education, Training, and Awareness (SETA) Programs

Stanton et al. (2005) stated that even the best technology efforts intended to address IS security will fail unless the organization’s employees take the proper course of action when approached with a threat. Although technology-oriented safeguards such as firewalls and intrusion detection systems are found in a large number of organizations, focus on human factors in security including awareness and training initiatives has historically lagged behind (Furnell & Clarke, 2012). Previous studies in IS literature have confirmed awareness techniques to be effective in increasing employee security-related knowledge, promoting security-conscious decision-making, and in the prevention of naive IS security behaviors within the organization (C. Anderson & Agarwal, 2010; Puhakainen & Siponen, 2010). While training programs and initiatives exist within many organizations, there appears to be limited number of empirical research to determine what topics should be covered, the most useful method used for delivery, and to what degree these factors play a part in the IS security practice of employees (Talib, Clarke, & Furnell, 2010).

Security education, training, and awareness (SETA) programs can take many forms, but typically focus on raising employee awareness of responsibilities in relation to their organizations' information assets, provide instruction on the consequences of abuse, while also developing the necessary skills to help fulfill these requirements (D'Arcy & Hovav, 2007; Whitman, Townsend, & Alberts, 2001). Regardless of the form, the organizational IS security policy should provide the foundation of the SETA program. Many typical SETA programs seem to focus on memorization and often involve coercion, fear tactics, or perception of external pressures, which have been found to have no influence on employee compliance with organizational IS policies (Kranz & Haeussinger, 2014; Parrish & Nicolas-Rocca, 2012). However, according to Parsons et al. (2014) training and education efforts are more effective if they not only outline what is expected but also provide an understanding of why this is important to the individual or employee.

For this reason, socio-technical philosophies are understood to be more valuable, providing a means for employees to easily see how the training materials used can correlate to their day-to-day duties (Kruger & Kearney, 2006; Netteland et al., 2007). Socio-technical philosophies embrace social as well as technical elements for optimal design and use of organizational systems (Davis et al., 2014). Whitman et al. (2001)

found that the most effective way to guarantee the viability of IS security efforts is to ensure employees understand steps being taken and accept necessary precautions. This research will seek to address the lack of theoretically grounded empirical studies related to the design and effectiveness of SETA programs while exploring the differences in CCA and CyS based on the different SETA program types (Ng, Kankanhalli, & Xu, 2009).

Implementation of SETA programs has been found to be beneficial in mitigating cybersecurity threats (D'Arcy et al., 2009; Dhillon, 1999; Whitman, 2004). Furthermore, it is imperative that the most effective delivery method for the specific program type be empirically investigated (Paul, 2014). Both online and face-to-face training delivery methods have their advantages, and in previous research, each has been found to successfully produce a motivated employee who has the skills needed to apply their training to job-related tasks (Gupta et al., 2010). However, there seems to be insufficient research in the field of IS to determine the most successful delivery method as well as the type of program for cybersecurity-focused SETA programs.

Table 6

Summary of Security Education, Training, and Awareness Programs

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
C. Anderson & Agarwal, 2010	Empirical study via survey and experiment	Survey: 594 home computer users, Experiment: 101 computer users	Intention to perform security-related behavior, influence of message queues	Empirical evidence that the level of psychological ownership an individual feels influences security behavior
D'Arcy & Hovav, 2007	Empirical study via survey	Employees from eight organizations and graduate students	IS misuse intention and awareness of security countermeasures	User awareness of security policies, security-awareness programs, and

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
				preventive security software reduce IS misuse intentions
D’Arcy et al., 2009	Empirical study via survey	269 computer users from eight different companies	User awareness of security countermeasures, perceived certainty and severity of organizational sanctions, and misuse intention	Three practices deter IS misuse: user awareness of security policies, SETA programs, and computer monitoring
Davis et al., 2014	Theoretical		Socio-technical systems research expansion	Socio-technical research should be applied to extend conceptualizations of ‘systems’, apply the core ideas to new domains beyond new technologies, and, be used in predictive work.
Dhillon, 1999	Theoretical		Computer fraud, security controls	Organizations should develop a security policy, (technical, formal and informal interventions) to minimize losses from computer fraud
Furnell & Clarke, 2012	Theoretical		Information security awareness, human aspects of security	Recommends human aspects are included in a holistic security strategy alongside the necessary technologies
Gupta et al., 2010	Literature review and synthesis		End-user training methods	Researcher suggested long-term look at the influence of different training methods
Kranz & Haeussinger, 2014	Empirical study via survey	444 employees from various organizations	Motivation to comply with organizational IS security policies	Findings advance understanding of motivational processes underlying security compliant behavior
Kruger & Kearney, 2006	Theoretical		Information security awareness	Development of a prototype model for measuring

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
				organizational information security awareness
Netteland et al., 2007	Empirical study using LMS training completion rates and interviews	Organization employees over a four-year period	Information sharing, workplace training	Information sharing can be a critical factor in the implementation of e-learning initiatives
Ng et al., 2009	Empirical study via survey	134 employees	Computer security behavior	Perceived susceptibility, perceived benefits and self-efficacy are determinants of email related security behavior
Parrish & Nicholas-Rocca, 2012	Theoretical		IS security training, mindfulness	Framework for IS security training that integrates mindfulness into the decision-making process. Encouraged use of scenarios and online training/assessment
Parsons et al., 2014	Empirical study via expert reviewed survey	500 Australian employees	Knowledge of policy and procedures, attitude towards policy and procedures, and behavior	Findings suggest that training and education are more effective if they outline what is expected and provide an understanding of why this is important
Paul, 2014	Empirical study using survey and experiment	160 students	Training methodologies	No differences were found in learning outcomes between face-to-face, e-learning, and mobile learning methods
Puhakainen & Siponen, 2010	Interviews, Empirical study via survey	16 employees	IS security policy compliance	Continuous communication process is required to improve user IS security policy compliance
Stanton et al., 2005	Interviews, Empirical study via expert	49 SMEs and 1167 end users	Information security behavior	Behaviors related to password creation and sharing were found to be generally poor and

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
	reviewed survey			varied across different organization types
Talib et al., 2010	Empirical study via survey	333 computer users	Information security awareness and practices	Knowledge and practice obtained at the workplace was transferred to the home environment. Recommendations for developing all-around individual security culture
Whitman et al., 2001	Standard		Information security threats	Supports the need for information security policy and provides sample structure
Whitman, 2004	Interviews, Empirical study via expert reviewed survey	192 top computing executives	Information security threats	Determined top threats and empirically proved need for policy, awareness, and education in organizations

Cybersecurity Skills

Skills Defined

Boyatzis and Kolb (1991) defined skill as a “combination of ability, knowledge, and experience that enables a person to do something well” (p. 280). Skill is also described as the capability to understand and utilize knowledge, intellectual abilities, and past experiences to perform the best course of action well in a given situation (Choi et al., 2013; Levy, 2005; Torkzadeh & Lee, 2003). Skill acquisition is a learning process and generally adopts three stages of development (J. Anderson, 1982; Fitts, 1964). In the first stage, the individual will receive instruction and information about a skill topic area. At this stage, it is common to rehearse the information required for skill execution, making the facts available in working memory (i.e. acquiring the knowledge) for interpretive procedures (J. Anderson, 1982; Fitts, 1964). With practice, the knowledge is internalized and can be directly applied without interpretive procedures. This gradual process is considered stage two, and the individuals' knowledge increases allowing the connection to be made and transferred to actions or practices (Gravill, Compeau, & Marcolin, 2006). Further learning and experience then lead the individual to stage three, where skills are honed to be both efficient and autonomous (J. Anderson, 1982; Fitts, 1964). Improvements in this stage continue indefinitely, experience positively influencing an individual's actions with the ability to generalize procedures and increase performance occurring throughout the skill development until competency level is achieved when skills are mastered (J. Anderson, 1982; Fitts, 1964; Levy & Ramim, 2015; Marcolin, Compeau, Munro, & Huff, 2000).

Table 7

Summary of Skills Defined

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
J. Anderson, 1982	Theoretical		Acquisition of cognitive skill	Skill acquisition is a learning process that has three stages (e.g., declarative, procedural, & automacity); each requires time for honing
Boyatzis & Kolb, 1991	Development and empirical study via video/audio recorded sessions	236 adults consisting of students, managers, and 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
Choi et al., 2013	Empirical study via expert reviewed survey	185 respondents from a large government transportation agency	Cybersecurity threats, computer self-efficacy, CCA, CyS, computer misuse intention	End-user awareness of monitoring and cybersecurity initiative skill reduced misuse intentions

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Fitts, 1964	Theoretical		Perceptual-motor skill learning	Skill learning is a continuously evolving hierarchical process that with practice over time leads to maximum performance or competency
Gravill et al., 2006	Empirical study via paper survey and controlled experiment	67 volunteers from four large retail, financial, distribution, and consulting organizations	Self-assessed user competence	End-users did accurately self-assess their software knowledge but did improve as experience and understanding of IT increased
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 using computer simulation performed better than those without
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 their perceived ability to use a software package higher than their demonstrated competence level with the same software package
Torkzadeh & Lee, 2003	Empirical study via developed instrument	282 end-users from varying industries with mixed management levels	Perceived end-user computing skills	Identified 12 items for measuring perceived end-user computing skills. Cautioned perceptions do not always correspond to actual skills of the individual

Cybersecurity Skills Defined

The ACM Joint Task Force on Cybersecurity Education (2017) defines cybersecurity as “computing-based discipline involving technology, people, information, and processes to enable assured operations” (para. 2). It involves the creation, operation, analysis, and testing of secure computer systems and is considered an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries (ACM Joint Task Force on Cybersecurity Education, 2017). Accordingly, CyS "corresponds to an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS in protecting their information technology against damage, unauthorized use, modification, and/or exploitation" (National Initiative for Cybersecurity Careers & Studies, 2014).

Skills can be acquired and honed, increasing efficiency and impacting positive action, when adequate education and training initiatives are implemented within the organization (Carruth et al., 2010). Employees must have the proper skillset for effective mitigation of cybersecurity risk. They cannot be held responsible for naive cybersecurity practices if education and training are not provided to develop then improve upon these crucial skills (Lerouge, Newton, & Blanton, 2005; B. Von Solms & Von Solms, 2004). Likewise, employees' skills can be advanced when they are aware and engaged in adequate CCA initiatives (Carruth et al., 2010). Prior studies have failed to evaluate the role of skills in the mitigation of cybersecurity threats (Choi et al., 2013). Therefore, it can be concluded that additional research on CyS is needed due to the vulnerabilities presented by employees with lacking skillsets.

Table 8

Summary of Cybersecurity Skills

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
ACM Joint Task Force on Cybersecurity Education, 2017	Standard		Cybersecurity education	Seek to develop comprehensive curricular guidance in cybersecurity education

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Carruth et al., 2010	Empirical study via quasi-experiment with survey	43 high school students	Awareness and skill	Theory and intervention for promotion of knowledge and skill Acquisition in training/education
Choi et al., 2013	Empirical study via expert reviewed survey	185 respondents from a large government transportation agency	Cybersecurity threats and vulnerabilities utilizing impact of computer self-efficacy, CCA, and CyS on computer misuse intention	End-user awareness of monitoring and cybersecurity initiative skill reduced misuse intentions
Lerouge et al., 2005	Empirical study via mailed surveys	124 IS professionals	IS skillset	A systems analyst position requires a multi-faceted skillset but the skills were not ranked equally in terms of job importance and preferred use
National Initiative for Cybersecurity Careers & Studies, 2014	Standard		Cybersecurity	Glossary of common cybersecurity terminology
B. Von Solms & Von Solms, 2004	Theoretical		IS management	Identifies 10 key aspects for management IS governance plans

Demographics and Cybersecurity

Demographic information such as age, gender, role in the organization, years working at the organization, highest educational level, and years since last attended formal education were collected in this study. According to Sekaran (2006), demographic information can be used to test the representation of the data collection vs. the generalized study population. Furthermore, difference with regard to risk-taking, trust, and privacy-related concerns have been found between the genders, as well as among users of varying ages (Fogel & Nehmad, 2009). Per Mertler and Vannatta (2010), descriptive statistics should be used to summarize based on personal characteristics. Demographic questions were drafted based on the research methods recommendations of Sekaran and Bougie (2013) and special care was taken to ensure the wording was meaningful to the employee, response bias minimized, and that they respect the sensitivity and privacy of the participant (See Appendix D).

Summary of What is Known and Unknown

IS security awareness has become increasingly important in both academic and professional realms. This seems to coincide with organizations becoming more cognizant of their information assets and the importance of protection strategies, as well as the roles of the human factor in cybersecurity risk mitigation. However, previous studies suggested that awareness alone is not enough, but instead awareness strategies must be part of a larger organizational plan to establish and maintain an information security culture (Furnell & Thomson, 2009; Talib et al., 2010). Therefore, expanding knowledge of both CCA and CyS, as well as SETA programs are significant for both researchers and practitioners who are charged with protecting organization information systems and information assets. This study addressed a gap in the current body of knowledge by providing a theoretically grounded empirical study related to the design and effectiveness of SETA program type, along with testing it between the delivery methods.

Chapter 3

Methodology

Overview of Research Design

This research study utilized a mixed method approach following the work of Carlton and Levy (2015), using both qualitative and quantitative research methods. According to Straub (1989), both methods are capable of uncovering the underlying meaning of phenomena in research. Qualitative methods are often used to discover evidence, while quantitative methods allow the researcher to verify the results, consequently improving the integrity of the study findings (Shank, 2006). Qualitative methods required the assistance of SMEs per the Delphi methodology to determine the topics to be covered in the SETA program, to validate and refine the measure of CCA, and to approve the content of the two SETA programs with integrated vignette-based assessments for CCA and CyS. Quantitative methods were then used to deploy two SETA program types via two delivery methods to randomized participants.

For the purposes of this research, two SETA program types were developed: 1) a traditional SETA program that informed the employee of organizational policies, along with actions that should and should not be taken, as well as 2) a socio-technical SETA program that also included explanations of why certain actions may cause difficulties for both the individual and the organization. The SETA programs were delivered via online and face-to-face methods. Pre- and post-assessments were used to determine if there are significant differences in the CCA and CyS of the employee based on delivery method. An expert panel was utilized to ensure the validity of the two SETA programs' content per the Delphi methodology and participants were randomly assigned to the four SETA training sessions (two SETA program types & two delivery methods) as well as to a control group.

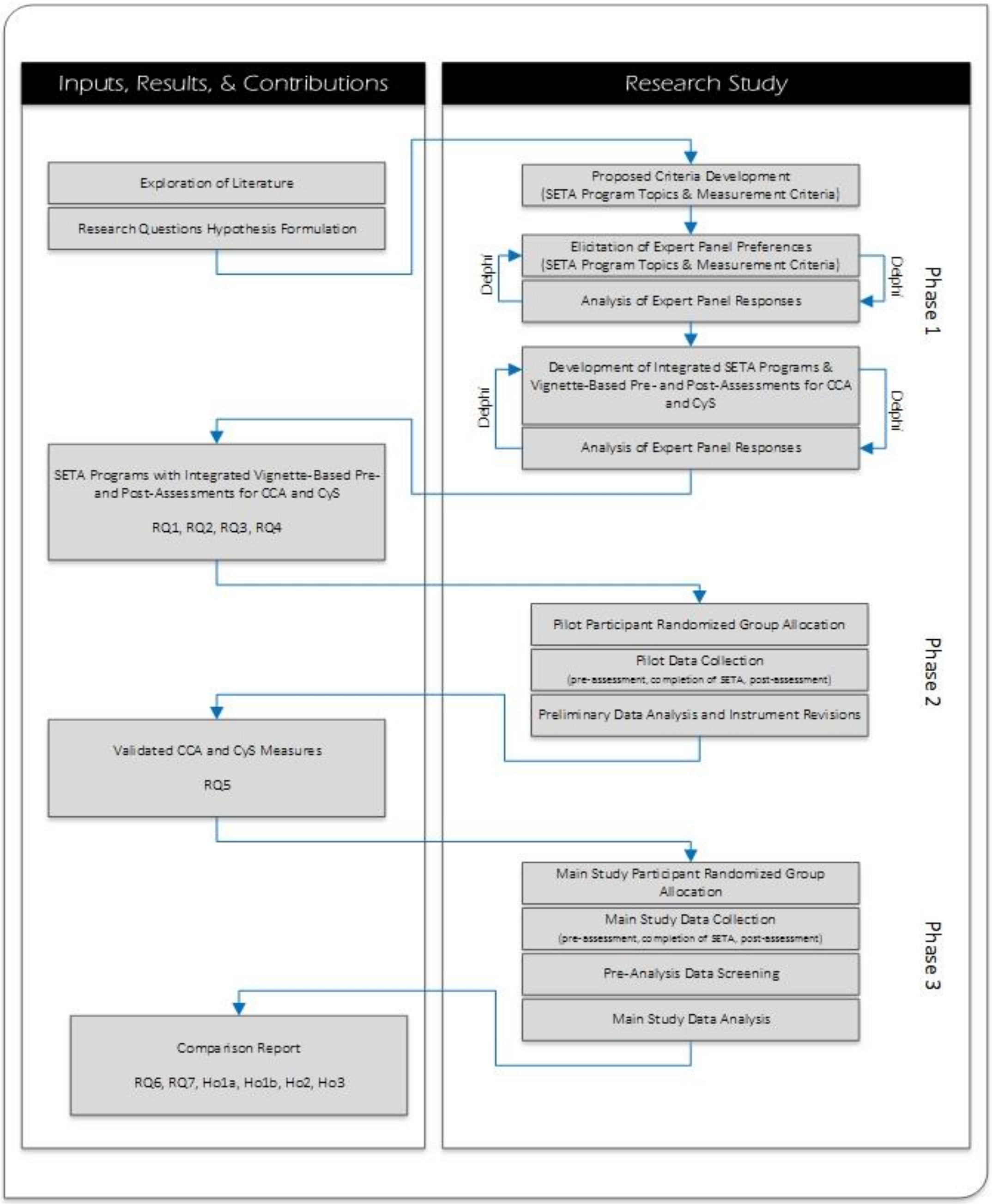

Inputs, Results, & Contributions
Research Study
Exploration of Literature
Research Questions Hypothesis Formulation
Proposed Criteria Development
(SETA Program Topics & Measurement Criteria)
Elicitation of Expert Panel Preferences
(SETA Program Topics & Measurement Criteria)
Analysis of Expert Panel Responses
Delphi
Delphi
Phase 1
Development of Integrated SETA Programs & Vignette-Based Pre- and Post-Assessments for CCA and CyS
Analysis of Expert Panel Responses
Delphi
Delphi
SETA Programs with Integrated Vignette-Based Pre- and Post-Assessments for CCA and CyS
RQ1, RQ2, RQ3, RQ4
Pilot Participant Randomized Group Allocation
Pilot Data Collection
(pre-assessment, completion of SETA, post-assessment)
Preliminary Data Analysis and Instrument Revisions
Phase 2
Validated CCA and CyS Measures
RQ5
Main Study Participant Randomized Group Allocation
Main Study Data Collection
(pre-assessment, completion of SETA, post-assessment)
Pre-Analysis Data Screening
Main Study Data Analysis
Phase 3
Comparison Report
RQ6, RQ7, Ho1a, Ho1b, Ho2, Ho3

Figure 3: Overview of the research design process

The main research question (RQ) that this study addressed is: Are there any significant differences in employees' CCA and CyS between two SETA program types and two SETA delivery methods?

The specific RQs for this research study were:

RQ1: What are the SMEs' approved topics for the two SETA program types using the Delphi methodology?

RQ2: What are the SMEs' approved measurement criteria for CCA using the Delphi methodology?

RQ3: What are the SMEs' approved weights for the three CCA categories (awareness of policy, SETA, & monitoring)?

RQ4: What are the SMEs' approved two SETA programs with integrated vignette-based assessments for CCA and CyS using the Delphi methodology?

RQ5: Are there any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using a pilot group of participants?

RQ6: Are there any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study group of participants?

RQ7a-e: Are there any significant differences between the two SETA program types, and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study participants, when controlled for participants' (a) age, (b) gender, (c) role in the organization, (d) highest

educational level, (e) years working at the organization, and (f) years since last attended formal education?

The specific hypotheses for RQ5 and RQ6 (in null form) are:

Ho1a: There will be no statistically significant mean differences in employee's pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the typical SETA program based on the two delivery methods (face-to-face & online).

Ho1b: There will be no statistically significant mean differences in employee's pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the socio-technical SETA program based on the two delivery methods (face-to-face & online).

Ho2: There will be no statistically significant mean differences on employee's cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) between the two SETA program types (typical & socio-technical).

Ho3: There will be no statistically significant interaction between the two SETA program types and the two delivery methods.

All measures were tested between comparisons for SETA type (typical & socio-technical) and delivery method (face-to-face & online).

Instrument Development

Delphi Methodology

The Delphi methodology has been proven to provide both validity and reliability in situations when there is no source of factual data but a basis for opinion exists (Linstone

& Turoff, 1975, 2002). It was designed to encourage true debate through the use of techniques which allow for anonymity, iteration, and controlled feedback (Gordon & Glenn, 2009). Techniques seek to expose the study to SMEs who often have differing opinions, effectively utilizing a group communication process to refine measures based on the input of the expert panel (Ramim & Lichvar, 2014).

With the Delphi methodology, SMEs from the pertinent discipline were identified and asked to participate in the inquiry (See Appendix E). Experts are specialists or authorities who are qualified to explore answers from a relevant disciplinary perspective and are considered experienced and knowledgeable in the field (Gray & Hovav, 2014). The study was explained to the experts, as was the guarantee of anonymity. According to Clayton (1997), the expert panel size can vary depending on the complexity and the expertise required for consensus on the topic. A panel of 15 to 30 professionals with diverse backgrounds and expertise within the field, as well as varied age and education, is considered best practice for homogeneous populations (Clayton, 1997).

As recommended, during the first phase of the research study a panel of 21 SMEs was gathered to complete the Delphi processes. Each expert possessed skills (i.e., knowledge, experiences, & abilities) in the field of cybersecurity. Engaging those with skillsets and expertise in the area of study allows the group to confirm that the measures are adequate and fully representative of the concept (Sekaran & Bougie, 2013). Consistent with recommendations from Gordon and Glenn (2009), once SMEs agreed to participate, research questions were refined by the researchers and pursued through a number of sequential questionnaires delivered via Web-based methods. In turn, SMEs were asked to provide their judgment as well as feedback on their positions for each of the pieces in need of validation: SETA program topics, the CCA vignette-based assessment, weights for the three CCA categories, and approved SETA program content (See Appendix F). For each of these items, SME feedback was analyzed and synthesized to form the basis of follow-up questionnaires. This process encouraged the participants to reassess their views in light of reasoning presented by others or to refute the position of others when necessary. The Delphi methodology provided for a controlled debate in this manner until consensus on the topic was reached.

Vignette-based Assessment

Siponen and Vance (2010) proposed that an assessment method utilizing hypothetical scenarios is “also known as a vignette or policy capturing method” (p.492). According to Finch (1987), vignettes are “short stories about hypothetical characters in specified circumstances, to whose situation the interviewee is invited to respond” (p. 105). Vignettes request responses on a number of rating scales to measure the dependent variables of interest, allowing for an investigation into the judgment or decision-making processes of the participant (Trevino, 1992).

Traditional survey methods link past behavior with present perceptions, creating the possibility of measurement error (Bachman, Paternoster, & Ward, 1992; Siponen & Vance, 2010). The vignette approach has grown in popularity with the increasing recognition of questionnaire limitations and has been found particularly useful for awareness topics (Hughes & Huby, 2002). Skills are also measured via vignette-based measures in industry and the military. Moreover, vignette-based methods are an established means of assessing antisocial and ethical/unethical behavior (Siponen &

Vance, 2010). Vignette-based methods were employed in 55% of the 174 ethical decision-making articles reviewed by O'Fallon and Butterfield (2005).

Also referred to as scenarios or simulations in previous research, vignettes have been found to be a versatile means of training personnel as they bridge the gap between instruction and practical training (Alexander, 2000). Vignettes have been used in various disciplines to study a range of topics, including emergency management (Alexander, 2000), nursing and medical students (Gould, 1996; Hughes & Huby, 2002; Schigelone & Fitzgerald, 2004), and in the social sciences (Finch, 1987; Wilks, 2004). Gould (1996) popularized the use of vignettes as a part of training and assessment, while their use is now prevalent in fields like human resources and aviation as an integrated piece of organizational learning. Vignettes were first adapted for cybersecurity research by D'Arcy and Hovav (2007) who used the method to measure the intention of users to misuse IS resources in various contexts.

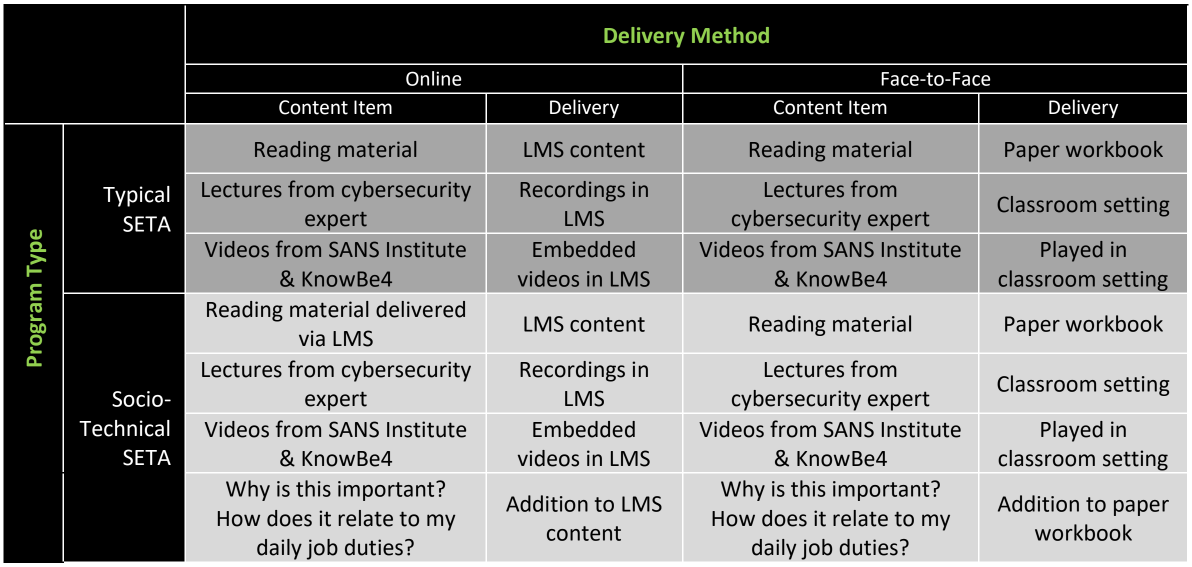
The vignettes must be constructed so that they appear plausible to participants and should present concrete, relatively detailed information concerning the independent variables of interest (Trevino, 1992). The ability to modify the story to be consistent with any research topic, the relaxing nature of the 'story-telling' process, as well as the hypothetical and general nature of the vignette allow for depersonalization that leads to an ease of obtaining information from the participant (Finch, 1987; Schoenberg & Ravdal, 2000). In keeping with previous research, the vignettes for CCA measurement were drafted using anonymized situations validated by cybersecurity experts (Barter & Renold, 1999; Neff, 1979).

Security Education, Training, and Awareness (SETA) Programs

SETA programs are enacted to convey knowledge about organizational IS security risks as well as raise employee awareness of their responsibilities in protecting organizational systems and information assets (Kajzer, D'Arcy, Crowell, Striegel, & Van Bruggen, 2014). According to D'Arcy and Hovav (2007), SETA program topics should be based upon the security policy of the organization. ISO/IEC 27002 standards suggest the following as relevant topics to be covered in IS security policies (ISO/IEC, 2013).

- Access control – data security, data destruction, and encryption
- Confidentiality and information classification
- Physical and environmental security
- End-user-oriented topics, such as:
    - acceptable use of information assets
    - clear desk and clear screen
    - information transfer and storage
    - mobile device security
    - working remotely
    - restrictions on software installations and use (copyright concerns)
- Backup
- Protection from malware and social engineering
- Management of technical vulnerabilities
- Cryptographic controls
- Communication security
- Privacy and protection of personally identifiable information
- Vendor relationships

Based upon these areas, topics for SETA program inclusion were developed and provided to the SMEs for input and revision per the Delphi methodology. After determination of the key topics for inclusion, the SETA program content was developed for delivery via two program types (typical & socio-technical) and two methods (face-to-face & online). Content included reading material, lectures from an expert in the field of cybersecurity, and topic appropriate videos from the SANS Institute and KnowBe4 training curriculums. Each of these content pieces was adapted for both face-to-face and online delivery (See Figure 4). In addition, the socio-technical program type included a facet to provide the participant with more information on why the content is important to them personally as well as identification of how the training materials can correlate to their day-to-day duties.



		Delivery Method			
		Online		Face-to-Face	
		Content Item	Delivery	Content Item	Delivery
Program Type	Typical SETA	Reading material	LMS content	Reading material	Paper workbook
		Lectures from cybersecurity expert	Recordings in LMS	Lectures from cybersecurity expert	Classroom setting
		Videos from SANS Institute & KnowBe4	Embedded videos in LMS	Videos from SANS Institute & KnowBe4	Played in classroom setting
	Socio-Technical SETA	Reading material delivered via LMS	LMS content	Reading material	Paper workbook
		Lectures from cybersecurity expert	Recordings in LMS	Lectures from cybersecurity expert	Classroom setting
		Videos from SANS Institute & KnowBe4	Embedded videos in LMS	Videos from SANS Institute & KnowBe4	Played in classroom setting
		Why is this important? How does it relate to my daily job duties?	Addition to LMS content	Why is this important? How does it relate to my daily job duties?	Addition to paper workbook

Figure 4. SETA program content

Cybersecurity Countermeasures Awareness (CCA)

The measurement instrument for CCA was developed based on the security countermeasures assessments of Hovav and D'Arcy (2012) as well as Vance et al. (2012). Although previous work presented these items in survey format, this study utilized a vignette-based assessment of CCA. Proposed CCA vignettes (See Appendix H) covered awareness of policy, SETA, as well as monitoring and address key, IS security policy topics (Doherty, Anastasakis, & Fulford, 2011; SANS Institute, 2014). The Delphi methodology was used to obtain SME feedback on the adapted vignettes in addition to the weights for the three CCA categories (See Figure 5). The validated vignette-based assessment of CCA was then integrated into the SETA program.

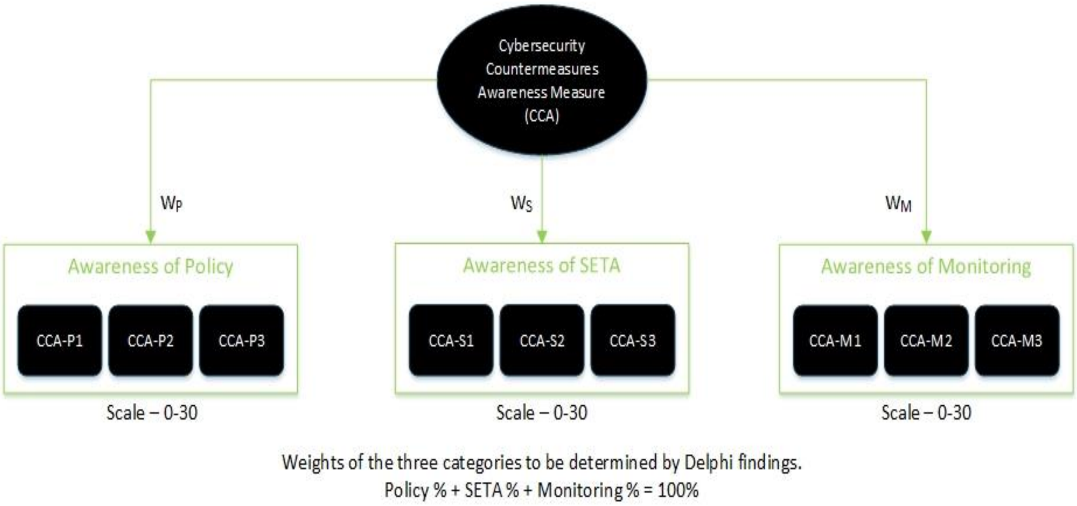

Cybersecurity Countermeasures Awareness Measure (CCA)
WP
WS
WM
Awareness of Policy
CCA-P1
CCA-P2
CCA-P3
Awareness of SETA
CCA-S1
CCA-S2
CCA-S3
Awareness of Monitoring
CCA-M1
CCA-M2
CCA-M3
Scale – 0-30
Scale – 0-30
Scale – 0-30
Weights of the three categories to be determined by Delphi findings.
Policy % + SETA % + Monitoring % = 100%

Figure 5. Research design for weights of CCA categories

Cybersecurity Skills (CyS)

This study measured employees' CyS using nine key cybersecurity skills identified in previously validated research (Carlton & Levy, 2015). Carlton and Levy (2015) utilized the Delphi methodology to gain SMEs input on the top platform independent cybersecurity skills for non-IT professionals. Once the top skills were identified, they were then used to develop both a CyS index and a validated vignette-based iPad assessment application (app), known as MyCyberSkills™ (Carlton, Levy, Ramim, & Terrell, 2015). The MyCyberSkills™ vignette-based assessment app was integrated alongside the CCA measurement tool developed through this research for pre- and post-assessment of the two SETA program types (typical & socio-technical) as well as two delivery methods (face-to-face & online). The MyCyberSkills™ assessment was used as is, requiring no Delphi review since it is has been previously validated in the work of Carlton (2016) (See Appendix I).

Pilot Study

A pilot study was conducted using a sample of 60 employees to verify the validity of the SETA program and the integrated vignette-based assessment instruments. This phase allowed for assurance that the CCA instrument had construct validity, in addition to confirmation that it is internally and externally reliable.

Validity and Reliability

Validity and reliability of a measurement instrument are vital for guarding against inaccurate conclusions in research (Salkind, 2011). Creswell (2002) stated that the reliability and validity of an instrument should provide "an accurate assessment of the variable and enable the researcher to draw inferences to a sample or population" (p. 180). The Delphi methodology employs feedback provided by a diverse set of SMEs through structured processes, which helps to ensure the data collection process is both reliable and valid. Therefore, to ensure validity and reliability, this research study utilized a panel of SMEs to verify the SETA program topics, the measurement criteria for CCA, as well as the weights for the three CCA categories for the hierarchical aggregation.

Validity

Straub, Rai, and Klein (2004) defined valid measures as those that "represent the essence or content upon which the entity or construct is focused" (p. 5). Instrument validity examines the validity of both content and constructs, while confirms that the developed instruments are measuring what they are supposed to be measuring (Levy, 2006; Straub, 1989). Both internal and external validity are key in quality experiment design (Salkind, 2011).

Internal validity refers to the confidence placed in the cause-and-effect relationship and the certainty that an independent variable caused a change in the depending variable (Sekaran, 2006). This research addressed internal validity by ensuring the assignment to each SETA program type and method combination was randomized. A control group was also used to negate the internal validity issues that can be experienced in studies that utilize both a pre- and post-assessment. This control group participated in both the pre- and post-assessment but did not complete either of the two SETA programs. In addition, content validity was facilitated through the use of SMEs via the Delphi methodology. A panel of 21 professionals with diverse backgrounds and expertise within the cybersecurity field served as SMEs. SME responses were used to ensure vignette content captured the research topics in question (Flaskerud, 1979; Gould, 1996). Furthermore, a pilot study was conducted to strengthen the internal validity of the vignette-based assessment. A pilot study is often used when research requires that vignettes be as realistic as possible (Gould, 1996; Hughes & Huby, 2012).

External validity refers to the certainty that any cause-and-effect relationship that is found as part of a research study can then be generalized to other settings, people, and places (Salkind, 2011; Sekaran, 2006). Threats to external validity were addressed by ensuring that all participants received equal treatment during the research process and that the nature of the experience was generalizable to the extent possible. Straub (1989) stated that research findings may be better corroborated with instrument validation. A combination of qualitative and quantitative research methods is recommended, allowing for certainty that the instrument was valid and not obstructing the collection of accurate data.

Reliability

Straub et al. (2004) defined reliability as “the extent to which a variable or set of variables is consistent in what it is intended to measure” (p. 70). Reliability is important because it indicates an unbias instrument that will provide for stable and consistent results upon repeated administrations (Creswell, 2002; Sekaran, 2006). Cronbach’s Alpha is the most commonly used measure to determine the reliability of an instrument (Sekaran, 2006; Straub et al., 2004). The reliability of each construct was assessed using Cronbach’s Alpha per previous research using vignette-based assessment (Hovav & D’Arcy, 2012; Vance et al., 2012; Vance & Siponen, 2012). Cronbach’s Alpha uses a scale from zero to one with a score of one nearing complete reliability (Gefen, Straub, & Boudreau, 2000). The lowest score deemed acceptable is .70, with items scoring below this point either reworded or removed (Sprinthall, 1997).

Population and Sample

This study utilized several sample populations: SMEs to participate in the Delphi methodology used for Phase 1, the pilot study participants required for Phase 2, and finally, main study participants for Phase 3. According to Clayton (1997), the panel size utilized for the Delphi methodology can vary depending on the complexity and the expertise required for consensus on the topic. In accordance with best practices, the SME panel was comprised of 21 professionals with diverse backgrounds and expertise within the cybersecurity field, as well as varying in age and education (Clayton, 1997).

Colleges and universities have been a target for cyber-attacks due to the vast amount of computing power possessed and the open access provided to constituents and the public (Katz, 2005). In fact for some time now, cybersecurity experts have found universities to be organizations with one of the worst environments for IS security (Rezgui & Marks, 2008). This study was conducted using the employee population (both faculty & staff) at a small private university in central Texas, who have received no previous formal cybersecurity training while employed at the University. All employees had the opportunity to complete the SETA program as part of the workforce training initiative. While each of the 320 employees did not complete one of the programs, the response rate was high with 250 participants (or 78.1%), providing an adequate sample of the population. Sekaran and Bougie (2013) indicated that "sample sizes larger than 30 and less than 500 are appropriate for most research" (p. 295). Furthermore, the sample size in multivariate research should be several times (preferably 10 times or more) as large as the number of variables in the study (Sekaran & Bougie, 2013). Based on this recommendation, a sample for the pilot study of 60 employees and the main study sample of 250 employees were deemed sufficient.

Pre-analysis Data Screening

Pre-analysis data screening was conducted to ensure consistency and accuracy of the data. Pre-analysis data screening is the process of detecting and dealing with irregularities or problems with collected data (Levy, 2006). According to Mertler and Vannatta (2010), there are four primary reasons to conduct pre-analysis data screening. First, it is important to ensure the accuracy of the data collected. For the purposes of this study, the risk to accuracy in collected data was mitigated through the use of Web-based collection methods, which accepted only valid responses. The second reason for pre-analysis data screening is to address the risk of respondents submitting the same score for all items (Levy, 2003). Response-set, also known as response bias, is the tendency of respondents to agree with survey instrument statements regardless of content (Winkler, Kanouse, & Ware, 1982). It is important that the data is examined for response-set violations, those instances are evaluated, and violators removed prior to final data analysis as it may represent a threat to validity (Kerlinger & Lee, 2000). These instances were reduced through the use of validated assessment measures using the vignette technique, which eliminated vague or confusing wording. The third reason for pre-analysis data screening is to deal with missing data and ensured that all questions were answered. This risk was addressed with use of a Web-based system that detected missing responses before allowing submission. Finally, the fourth reason for pre-analysis data screening is review for extreme cases or outliers. Mertler and Vannatta (2010) stated that "an outlier can cause a result to be insignificant when, without the outlier, it would have been significant" (p. 29). This risk was mitigated by screening for multivariate outliers using Mahalanobis Distance analysis to determine if such cases should be retained or removed prior to final analysis.

Data Analysis

Selection of the right process for data analysis is crucial (Creswell, 2002). A mixed-method approach was selected for this research, to be conducted in three phases. Analysis of variance (ANOVA), analysis of covariance (ANCOVA), and Spearman Correlation were used to assess the four research questions and three hypotheses. Mertler and Vannatta (2010) stated that the purpose of ANOVA is "to determine group differences when two or more factors create these groups" (p. 90). In order to conduct ANOVA analysis, there must be one dependent variable and more than one independent variable (Mertler & Vannatta, 2010; Terrell, 2012). Terrell (2012) discussed four major assumptions when using ANOVA. First, the sample for the dependent variable should be random. Second, "the scores must be independent of one another" (Terrell, 2012, p.245). Third, the sample or population should be normally distributed (Terrell, 2012). Last, there must be homogeneity of variance; and that "degree of variance within each of the samples should be about the same" (p. 245). According to Mertler and Vannatta (2010), ANCOVA is an extension of ANOVA in that it "adjusts the effects of variables that are related to the dependent variables" (p. 93). The Spearman Correlation is valid for use with ranked data (Mertler & Vannatta, 2010; Terrell, 2012).

RQ/H	Description	Methodology
RQ1	SMEs' approved topics for the two SETA program types	Delphi
RQ2	SMEs' approved measurement criteria for CCA	Delphi
RQ3	SMEs' approved weights for the three CCA areas	Delphi
RQ4	SMEs' approved two SETA programs with integrated vignette-based assessments for CCA and CyS	Delphi
RQ5	Significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using a pilot group of participants	ANOVA
RQ6	Significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study group of participants	ANOVA
RQ7a-e	Significant differences between the two SETA program types, and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study participants, when controlled for participants' (a) age, (b) gender, (c) role in the organization, (d) highest educational level, (e) years working at the organization, and (f) years since last attended formal education	ANCOVA
Ho1a	There will be no statistically significant mean differences in employee's pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the typical SETA program based on the two delivery methods (face-to-face & online).	ANCOVA Spearman Correlations
Ho1b	There will be no statistically significant mean differences in employee's pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the socio-technical SETA program based on the two delivery methods (face-to-face & online).	ANCOVA Spearman Correlations

Ho2	There will be no statistically significant mean differences on employee's cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) between the two SETA program types (typical vs. socio-technical).	ANCOVA Spearman Correlations
Ho3	There will be no statistically significant interaction between the two SETA program types and the two delivery methods.	ANCOVA

Figure 6: Research questions, hypotheses, and methodology

Qualitative data collection methods were used in Phase 1 for the elicitation of SME panel assistance with revision and validation of SETA program topics, weights for the CCA categories, as well as measurement criteria for CCA. The Delphi methodology was used to ensure reliability and validity of the instruments created.

RQ1: What are the SMEs' approved topics for the two SETA program types using the Delphi methodology?

RQ2: What are the SMEs' approved measurement criteria for CCA using the Delphi methodology?

RQ3: What are the SMEs' approved weights for the three CCA categories (awareness of policy, SETA, & monitoring)?

RQ4: What are the SMEs' approved two SETA programs with integrated vignette-based assessments for CCA and CyS using the Delphi methodology?

Phase 2 consisted of a pilot study with randomized participant group allocation into one of two developed SETA program types (typical vs. socio-technical) delivered via two delivery methods (face-to-face & online) as well as to the control group. Pilot data was collected from both a pre- and post-assessment integrated with each SETA program and data analysis performed using ANOVA to ensure validity and reliability. The SETA programs, as well as the CCA instrument, were revised per the preliminary data analysis, addressing RQ5 and providing validated measures for the main study.

RQ5: Are there any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using a pilot group of participants?

The main study was Phase 3 of the research, with participants assigned randomly to two developed SETA program types (typical & socio-technical) delivered via two delivery methods (face-to-face & online) as well as to the control group. Main study data was collected from both a pre- and post-assessment integrated with each SETA program and pre-analysis data screening was completed. Once completed, main study data analysis empirically assessed if there are any significant differences on employees' cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) based on the use of two SETA program types (typical vs. socio-technical) and two SETA delivery methods (face-to-face & online). Pre- and post-analysis scores for each of the four program type and delivery method combinations and for the control group were completed using ANOVA. In addition, ANCOVA was used to compare the groups, while also controlling for a variable that may exert an influence on the dependent variable (Mertler & Vannatta, 2010).

RQ6: Are there any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study group of participants?

RQ7a-e: Are there any significant differences between the two SETA program types, and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study participants, when controlled for participants' (a) age, (b) gender, (c) role in the organization, (d) highest

educational level, (e) years working at the organization, and (f) years since last attended formal education?

The following null hypotheses for RQ5 and RQ6 were tested between comparisons for SETA type (typical & socio-technical) and delivery method (face-to-face & online). Assessment used factorial ANCOVA and Spearman Correlation to assess the statistical significance of each when controlling for participants' (a) age, (b) gender, (c) role in the organization, (d) highest educational level, (e) years working at the organization, and (f) years since last attended formal education. Recommendations for SETA program type and delivery method as a result of data analysis will be provided.

Ho1a: There will be no statistically significant mean differences in employee’s pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the typical SETA program based on the two delivery methods (face-to-face & online).

Ho1b: There will be no statistically significant mean differences in employee’s pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the socio-technical SETA program based on the two delivery methods (face-to-face & online).

Ho2: There will be no statistically significant mean differences on employee’s cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) between the two SETA program types (typical & socio-technical).

Ho3: There will be no statistically significant interaction between the two SETA program types and the two delivery methods.

Resources

This research study required the following resources:

- Expert panel: Phase 1 of the research required an expert panel of 15 to 30 cybersecurity SMEs with diverse backgrounds and expertise within the field, as well as varying in age and education.
- Google Forms: This Web-based tool was used to gather expert panel input as well as for deployment of the CCA and CyS assessments via anonymous methods.
- Web-based learning management system (LMS): Online SETA program content was delivered via the Blackboard Learn LMS although no personally identifiable participant information was collected.
- SETA program content: The following items were used for SETA program content in both the face-to-face and online delivery methods: reading content, lectures provided by an expert in cybersecurity, and topic appropriate videos from SANS Institute and KnowBe4 training curriculums.
- Access to employee population: Approval from the IRB at both Nova Southeastern University and the study site were required to allow faculty and staff participation in the SETA program and related data collection. Site approval from university administration, as well as approval of both IRB committees, were obtained (See Appendices A, B, & C).
- Statistical analysis tool: Following data collection, Statistical Package for the Social Sciences® (SPSS) was used to analyze the data.

Summary

Chapter Three included a description of the research design and methodology for the research study. A mixed method approach was described, using both qualitative and quantitative research methods. The study was implemented in three phases. Phase 1 utilized an SME panel to provide feedback and validation on the SETA program topics, CCA vignette-based assessment, weights for the three CCA categories, and approved SETA program content. Phase 2 consisted of a pilot study with randomized participant group allocation into one of two developed SETA program types (typical & socio-technical) delivered via two delivery methods (face-to-face & online) as well as to the control group. After analysis and revision of study processes based on pilot data, Phase 3 of the research began the main study. Again, participants were assigned randomly to the five groups. Main study data was collected from both a pre- and post-assessment integrated with each SETA program. Pre-analysis data screening, as well as data analysis, was used to address the research questions. Chapter Three concludes with the resources required to complete this research study.

Chapter 4

Results

Overview

This chapter outlines the results of the data analysis for this research study, which utilized a mixed method approach combining an expert panel, developmental research, and quantitative data collection. Details of each of the three phases are presented in the order in which they were conducted. Phase 1 details expert panel data collection using the Delphi methodology, which used SMEs to develop the CCA vignette-based assessment as well as the proposed SETA program content. This phase addressed RQ1, RQ2, RQ3, and RQ4. Phase 2 details the pilot study used to validate the CCA measure, addressing RQ5. This chapter concludes with the details of Phase 3, providing results of the main study, which addressed RQ6 and RQ7 as well as the four hypotheses.

Qualitative Research and Expert Panel (Phase 1)

In Phase 1, a panel of 38 experts with skillsets and expertise in the area of study was targeted. In each of the two Delphi rounds, 21 responses were received representing a 55.2% response rate**.** Descriptive statistics of the expert panel are provided in Table 9. Consistent with recommendations from Gordon and Glenn (2009) as well as Ramim and Lichvar (2014), once SMEs agreed to participate in Phase 1 of the research study, instrument questions were refined and pursued through sequential Delphi rounds delivered via anonymous Web-based methods.

Table 9

Descriptive Statistics of SMEs (N=21)

Demographic Item	Frequency	Percentage
Gender:		
Female	6	28.6%
Male	15	71.4%
Current Employment:		
Academia	6	28.6%
Industry	5	23.8%
Both	10	47.6%
Age:		
20-29 years	1	4.8%
30-39 years	6	28.6%
40-49 years	9	42.9%
50-59 years	5	23.8%
Experience in Information Systems and/or Cybersecurity:		
1-5 years	0	0.0%
6-10 years	2	9.5%
11-15 years	8	38.1%
16-20 years	4	19.0%
20 years or more	7	33.3%
Cybersecurity Certifications:		
0	5	23.8%
1	7	33.3%
2	5	23.8%
3 or more	4	19.0%

In round one, SMEs were asked to provide their judgment as well as feedback on SETA program topics, the CCA vignette-based assessment, and weights for the three CCA categories (awareness of policy, SETA, & monitoring). According to Vernon (2009), the consensus for Delphi studies typically ranges from 55% to 100% agreement, with 70% considered the standard. Agreement percentages for this research study ranged from

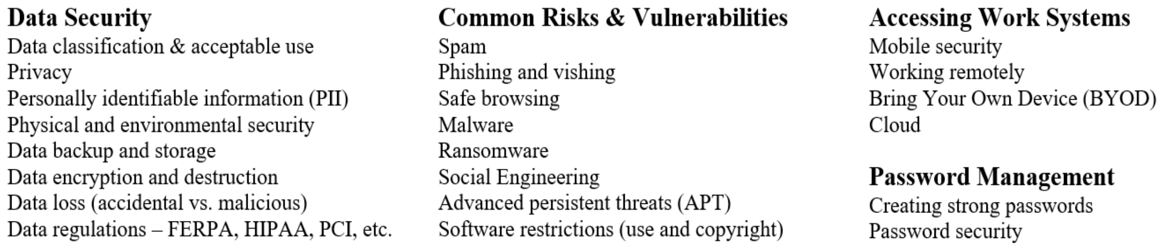
85% to 100% for questions asked of the panel. Given the very high agreement among the SMEs on the instrument questions, no additional cycles were required for round one. In round two, SMEs reviewed the SETA program content for both the typical and socio-technical courses to provide validation. For each of these items, SMEs feedback was analyzed and synthesized to determine that a clear consensus on each topic was provided with no need to proceed with follow-up rounds.

Security Education, Training, and Awareness (SETA) Program Topics

According to D'Arcy and Hovav (2007), SETA program topics should be based upon the security policy of the organization. In round one, SMEs were asked to validate a list of relevant cybersecurity topics based on suggestions in ISO/IEC 27002 standards for IS security policy (ISO/IEC, 2013). SMEs indicated whether the topic was one that should be included in a common organizational SETA program, provided revision of topics when needed, and were encouraged to suggest any additional topics that should be covered in present-day organizational environments. While the experts deemed most of the ISO/IEC 27002 topic suggestions important, the subjects of cryptographic controls and vendor relationships were found to be irrelevant for many organizations. Based on SMEs' feedback, Table 10 provides a list of the topics and subtopics that were determined to be the key foundational items for inclusion in organizational SETA programs. These SMEs' approved topics for the two SETA program types address RQ1.

Table 10

Key foundational SETA programs topics



Data Security
Data classification & acceptable use
Privacy
Personally identifiable information (PII)
Physical and environmental security
Data backup and storage
Data encryption and destruction
Data loss (accidental vs. malicious)
Data regulations – FERPA, HIPAA, PCI, etc.

Common Risks & Vulnerabilities
Spam
Phishing and vishing
Safe browsing
Malware
Ransomware
Social Engineering
Advanced persistent threats (APT)
Software restrictions (use and copyright)

Accessing Work Systems
Mobile security
Working remotely
Bring Your Own Device (BYOD)
Cloud

Password Management
Creating strong passwords
Password security

Measure of Cybersecurity Countermeasures Awareness (CCA)

The measurement instrument for CCA was developed based on the security countermeasures assessments of Hovav and D’Arcy (2012) as well as Vance et al. (2012). Although previous work presented these items in survey format, this study utilized a vignette-based assessment of CCA. The vignettes cover awareness of policy, SETA, as well as monitoring and address key IS security policy topics (Doherty et al., 2011; SANS Institute, 2014). In round one, the Delphi methodology was used to obtain SMEs feedback on several key aspects of the adapted vignettes. Nine vignettes were drafted based on previous empirically validated research studies, with three for each of the three CCA categories (D’Arcy et al., 2009; Hovav & D’Arcy, 2012; Vance et al., 2012). SMEs were asked to review the vignettes to ensure clarity of wording, validity in the context of the policy topic, that the actions provided address the possible outcomes of the vignettes, that the actions measure the cybersecurity countermeasures awareness of the three categories (awareness of policy, SETA, & monitoring) of the individual, and that the scores were assigned appropriately. Based on the feedback from the SMEs, RQ2 was satisfied by completing minor adjustments to clarify vignettes’ wording, to better address possible actions, and to ensure accurate scoring.

In addition to validating key aspects of the CCA vignettes, SMEs were also asked to provide their feedback on the weight of each of the three categories (awareness of policy, SETA, & monitoring), with the sum of the three totaling 100%. Answers across all SMEs were averaged to calculate the weight for each category. Results indicated that the most important category for the overall CCA measure was awareness of the organizational cybersecurity policy, with 41% (St.Dev = 9%). The second most important category for the overall CCA measure was awareness of SETA program content, with 34% (St.Dev = 9%), while awareness of monitoring was considered least important among the three with 25% (St.Dev = 8%). Figure 7 depicts the weights of the three CCA categories with standard deviation, addressing RQ3.

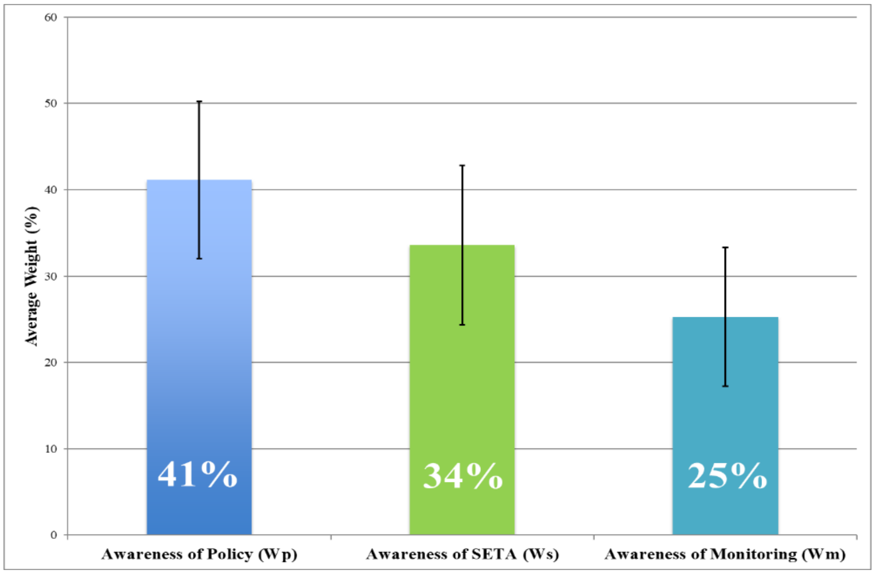


Figure 7. Weights and standard deviation of CCA categories

The SMEs validation of the CCA vignettes and the percentages for each of the three categories provided an empirically validated vignette-based assessment of CCA, allowing each individual the opportunity to demonstrate their level of CCA by responding to nine realistic organizational situations. The sum of the scores for each CCA category was divided by 30, which was the maximum number of points that could be obtained in each CCA category. Finally, the scores for each of the three categories were multiplied by their respective weights and added together to reach the aggregated overall employees' CCA score (Eq. 1). This finalized CCA measure was then integrated into the SETA program as both a pre- and post-assessment.

Eq. 1 $$\text{CCA} = \left(\frac{0.41}{30}\right) \cdot \sum_{3}^{i=1}(P_i) + \left(\frac{0.34}{30}\right) \cdot \sum_{3}^{j=1}(S_j) + \left(\frac{0.25}{30}\right) \cdot \sum_{3}^{k=1}(M_k)$$

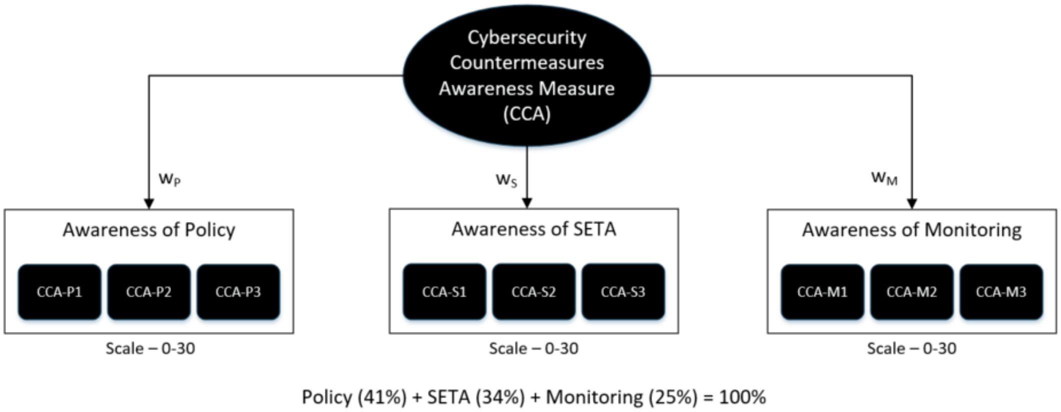


Figure 8. Research design with weights of CCA categories and overall score aggregation

Security Education, Training, and Awareness (SETA) Program Content

Attaining expert opinion on both the typical and socio-technical content before moving forward was imperative given the focus of this study on the two program types. SMEs were provided with a detailed explanation of the typical SETA program, which informs the employee of organizational policies and actions that should or should not be taken. The socio-technical SETA program was also defined as comprising the same basic inclusions in addition to explanations of why certain actions may cause difficulties as well as the potential organizational outcomes associated.

The cybersecurity topics determined important by SMEs in round one for delivery were utilized and content created for the two program types (typical & socio-technical). Delphi round two of this study focused on SMEs validation of the proposed SETA program content. This content included reading material, lectures from an expert in the field of cybersecurity, and topic appropriate videos from the SANS Institute and KnowBe4 training curriculums. SMEs were provided with the opportunity to review material for five of the cybersecurity topics as a representation of the comprehensive content developed. They were asked to verify that the typical training content was what they would expect of an organizational SETA program, to determine if the socio-technical content additions provided the participant with more information on why the content is important to them personally and identification of how the training materials can correlate to their day-to-day duties, and to provide any additional feedback or revision suggestions.

Quantitative Research (Phase 2)

In Phase 2, a group of 60 employees participated in a pilot study to ensure validity and reliability of the CCA measure. Participants were randomly allocated to one of five groups: 1) TypONL (typical program via online delivery); 2) StONL (socio-technical program via online delivery); 3) TypF2F (typical program via face-to-face delivery); 4) StF2F (socio-technical program via face-to-face delivery); and 5) Control (the control group which participated in the pre- and post-assessment but did not experience any of the SETA programs – i.e. no training).

Pilot data was collected from both the pre- and post-assessment, providing both CCA and CyS scores on a scale of 0 to 100 for each individual before and after SETA program completion. The means and standard deviations for both CCA and CyS were calculated for each of the five pilot groups. As demonstrated in Table 11 and Figure 9, the mean

CCA scores for the StONL showed a 10.23% difference in pre- vs. post-assessment scores. This was closely trailed by the StF2F mean difference at 9.25% and the TypF2F mean difference of 9.02%. Additionally, the CCA mean difference between the pre- and post-assessment for the Control group was .11%, suggesting no concern related to validity or reliability of the CCA construct.

Table 11

Means and Standard Deviations for CCA (N=60)

		Pre-Assessment		Post-Assessment		Pre-Post Difference	
Group	**n**	**Mean**	**Standard Deviation**	**Mean**	**Standard Deviation**	**Mean**	**Standard Deviation**
TypF2F	12	84.91%	8.43%	93.92%	10.37%	9.02%	6.16%
StF2F	12	86.08%	7.53%	95.33%	8.26%	9.25%	6.47%
TypONL	12	89.74%	6.29%	95.16%	7.92%	5.41%	4.94%
StONL	12	86.76%	10.10%	96.98%	8.96%	10.23%	7.88%
Control	12	87.04%	4.29%	87.16%	13.35%	0.11%	2.86%

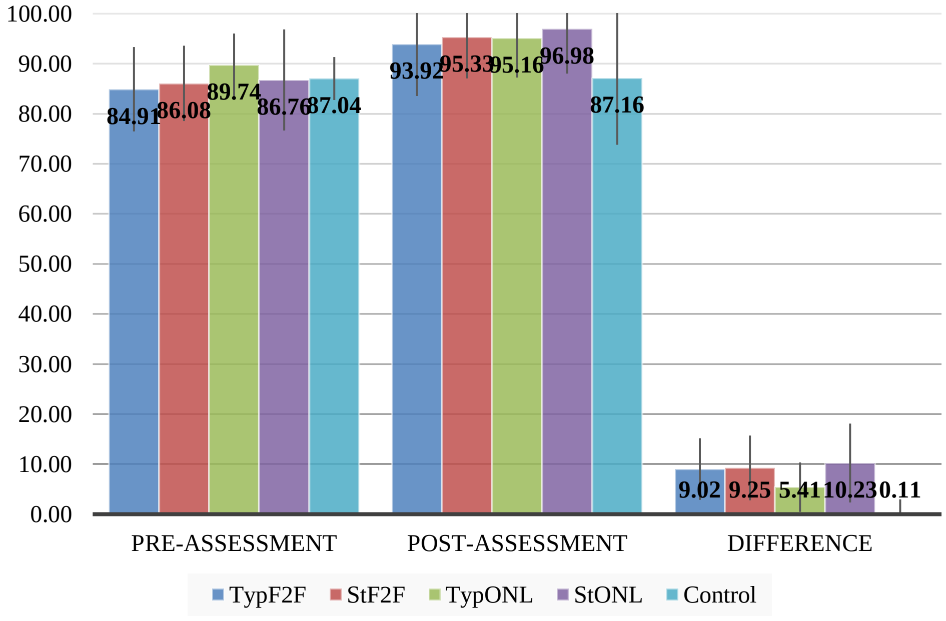


Figure 9. Means and standard deviations for CCA (N=60)

Table 12

Means and Standard Deviations for CyS (N=60)

		Pre-Assessment		Post-Assessment		Pre-Post Difference	
			Standard		Standard		Standard
Group	**n**	**Mean**	**Deviation**	**Mean**	**Deviation**	**Mean**	**Deviation**
TypF2F	12	58.96%	9.74%	71.51%	9.13%	12.55%	8.24%
StF2F	12	59.28%	14.66%	75.19%	9.79%	15.91%	9.47%
TypONL	12	65.54%	6.65%	72.56%	7.37%	7.02%	5.07%
StONL	12	57.66%	11.91%	72.35%	10.72%	14.68%	10.22%
Control	12	60.65%	10.31%	61.83%	7.02%	1.18%	1.33%

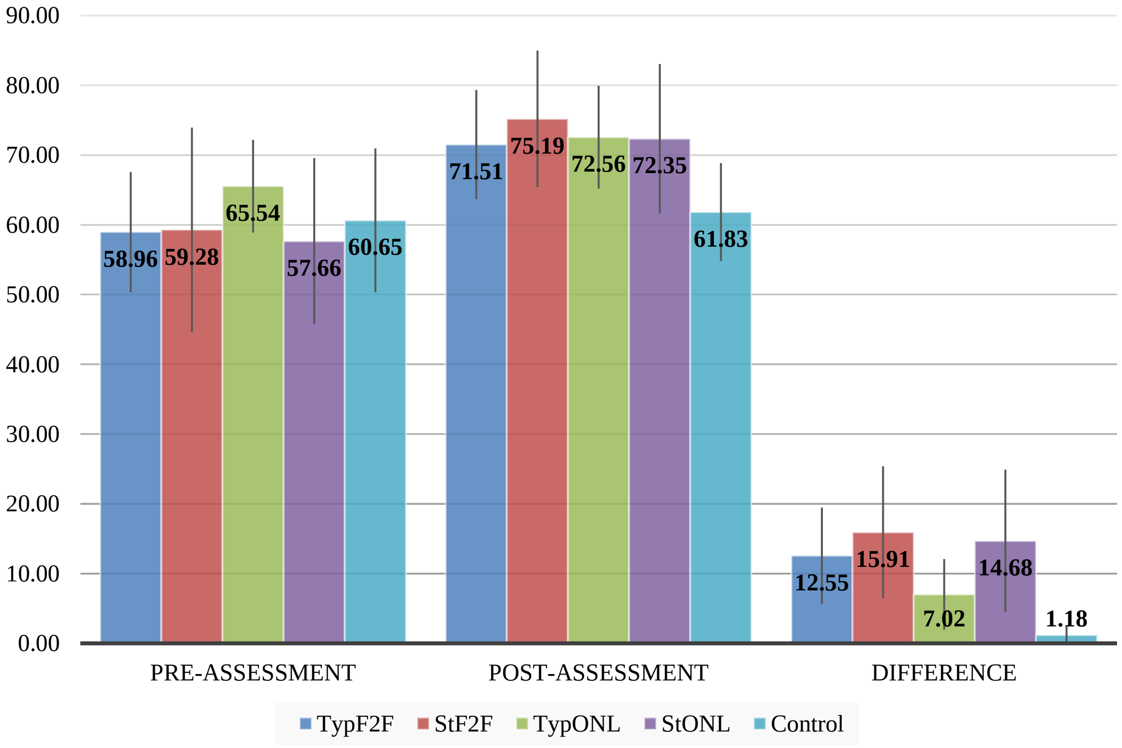


Figure 10. Means and standard deviations for CyS (N=60)

CyS means and standard deviations were also calculated for the pilot group and are provided in Table 12 and Figure 10. Like the CCA results, the CyS outcomes showed a higher difference in the pre- and post-assessment mean score for the socio-technical programs with 14.68% for StONL and 15.91% for StF2F. The mean difference for the typical SETA programs of TypF2F and TypONL calculated at 12.55% and 7.02% respectively. Again, the Control group showed very little change between the pre- and post-assessment with a mean difference of 1.18%.

Furthermore, the ANOVA conducted for the pilot study found a significance below p < 0.001 for both CCA, *F*(1,58) = 16.48, p < 0.001, and CyS, *F*(1,58) = 18.80, p < 0.001, as seen in Table 13. The results suggested there are differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS. The SETA programs, as well as the CCA instrument, were revised per the preliminary data analysis, addressing RQ5 and providing validated measures for the main study.

Table 13

ANOVA Results Between Pilot Study Groups (N=60)

	F	**Sig.**	
CCA Score	16.478	***0.000***	***
CyS Score	18.799	***0.000***	***

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

Quantitative Research (Phase 3)

Pre-Analysis Data Screening

In Phase 3, employees were recruited to participate in the validated SETA program with integrated vignette-based pre- and post-assessment (See Appendix G). As part of a workforce training initiative at a small university in the United States, 320 employees were invited to participate and randomly assigned to one of the five study groups. Responses from 263 individuals were gathered providing an 82.1% response rate. For the purposes of this study, the risk to accuracy in collected data was mitigated through the use of Web-based collection methods, which reduced the opportunity for missing data by ensuring complete responses before allowing submission. However, pre-analysis data screening revealed 13 participants that began the study, but did not complete both the CCA and CyS assessments. These responses were removed to ensure the accuracy of the data collected.

In accordance with Levy (2006), the data set was then reviewed for cases of response-set as well as extreme cases or outliers. CCA and CyS scores were calculated for all completed responses, and the data was imported into Statistical Package for the Social Sciences® (SPSS) version 24 for pre-analysis screening. Analysis included a review for response-set cases to address the risk of respondents submitting the same score for all items, of which no cases were found (Levy, 2003). Furthermore, to ensure accuracy, the data was analyzed for multivariate outliers using Mahalanobis Distance to determine if any responses should be removed prior to final analysis. All responses were found to be within the expected ranges and none were removed, leaving 250 participants who completed both the pre- and post-assessment for analysis. This represents a 78.1% response rate for the study.

Using the CCA and CyS scores, means and standard deviations were calculated for each of the five groups: 1) typical program via online delivery; 2) socio-technical program via online delivery; 3) typical program via face-to-face delivery; 4) socio-technical program via face-to-face delivery; and 5) the control group which participated in the pre- and post-assessment but did not participated in the SETA program.

Demographic Analysis

After completing pre-analysis data screening, pre- and post-assessment responses for 250 participants remained. Of these 133 or 53.2% were completed by females and 117 or 46.8% were completed by males. Analysis of the age of respondents indicated that 167 or 66.8% were 30 to 59 years of age. Given the organizational requirement of a high school degree for employment, the fact that no respondents were found to have less than a high school degree was not surprising. Additionally, 182 or 72.8% of participants responded that they held a bachelor, graduate, or doctoral degree. This is reflective of the environment where the study was performed. Academia lends itself to an elevated percentage of the workforce having higher education degrees due to position requirements or through University initiatives that provide financial support for continuing education efforts. These same initiatives would provide clarification of the high number of respondents who reported their last formal education to be zero to 14 years ago, 139 employees or 55.6%. Finally, after further review, it was determined that the majority of faculty members participating in the study selected the organizational role of trained professional. In conjunction with others who might have selected trained professional as the role that best fits their position, this group accounted for 83 or 33.2% of the respondents. Table 14 presents the demographic details of the population.

Table 14

Descriptive Statistics of the Population (N=250)

Demographic Item	**Frequency**	**Percentage (%)**
Gender		
Male	117	46.8%
Female	133	53.2%
Age		
Under 20	1	0.4%
20 to 29	31	12.4%

30 to 39	44	17.6%
40 to 49	62	24.8%
50 to 59	61	24.4%
60 to 69	42	16.8%
70 or older	9	3.6%
Role in Organization		
Administrative or support staff	96	38.4%
Trained professional	83	33.2%
Skilled laborer	22	9.6%
First level supervisor	16	6.4%
Middle management	24	9.6%
Upper management or executive	9	3.6%
Number of Years Worked at Organization		
Less than 1	34	13.6%
1 to 2	38	15.2%
3 to 5	52	20.8%
6 to 10	45	18.0%
Over 10	81	32.4%
Highest Education Level		
Less than a high school degree	0	0%
High school degree or equivalent (e.g., GED)	38	15.2%
Associate degree, vocational, or technical school	30	12.0%
Bachelor degree (BA, BS, BBA, etc.)	74	29.6%
Graduate degree (MA, MS, MIS, etc.)	56	22.4%
Doctoral degree (Ph.D., MD, JD, DSc, etc.)	52	20.8%
Years Since Last Formal Education		
0-4	57	22.8%
5 to 9	41	16.4%
10 to 14	41	16.4%
15-19	27	10.8%
20-24	25	10.0%
25-29	22	8.8%
30 or more	37	14.8%

Data Analysis

After pre-analysis data screening was completed, the descriptive analysis for the population (N=250) was performed. To answer RQ6, the responses were analyzed to determine if there were any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS. CCA means and standard deviations were calculated for each of the five groups and are represented in Table 15 and Figure 11. Comparable to the pilot study results, the socio-technical programs in the main study provided a higher CCA mean difference with 9.51% for StF2F and 9.81% for StONL. The TypONL, 8.37%, and TypF2F, 8.63%, groups were very close in mean difference for CCA although analysis found them to fall slightly short of the socio-technical programs. The Control group mean difference was 1.08%, which appears to fall within the margin of error representing no valid increase between the pre- and post-assessment measures.

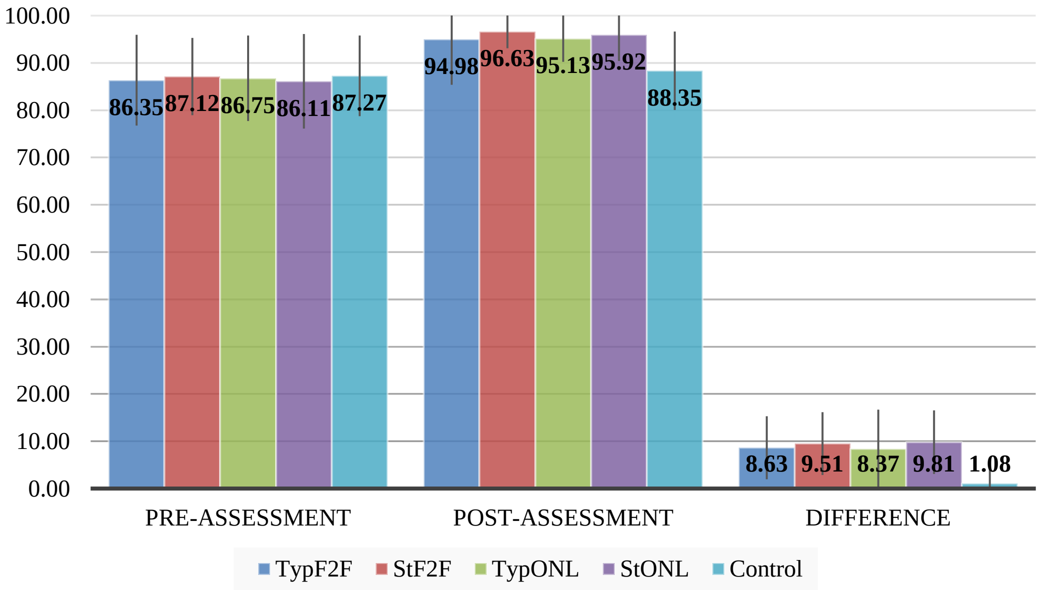


Figure 11. Means and standard deviations for CCA (N=250)

Table 15

Means and Standard Deviations for CCA (N=250)

		Pre-Assessment		Post-Assessment		Pre-Post Difference	
Group	n	Mean	Standard Deviation	Mean	Standard Deviation	Mean	Standard Deviation
TypF2F	50	86.35%	9.60%	94.98%	6.66%	8.63%	6.17%
StF2F	50	87.12%	8.17%	96.63%	3.53%	9.51%	6.64%
TypONL	50	86.75%	9.04%	95.13%	4.89%	8.37%	8.31%
StONL	50	86.11%	10.00%	95.92%	5.52%	9.81%	6.72%
Control	50	87.27%	8.53%	88.35%	8.29%	1.08%	3.84%

A review of the CyS means and standard deviations for each of the five groups, provided in Table 16 and Figure 12, showed a similar Control group outcome with a mean difference of 1.16%. The highest mean difference was for the StF2F group with 14.58%. Participants that completed the StONL program showed an 11.63% difference in CyS, while the TypF2F group had a mean difference of 10.74%. The TypONL group had the least increase in mean CyS with 6.25%.

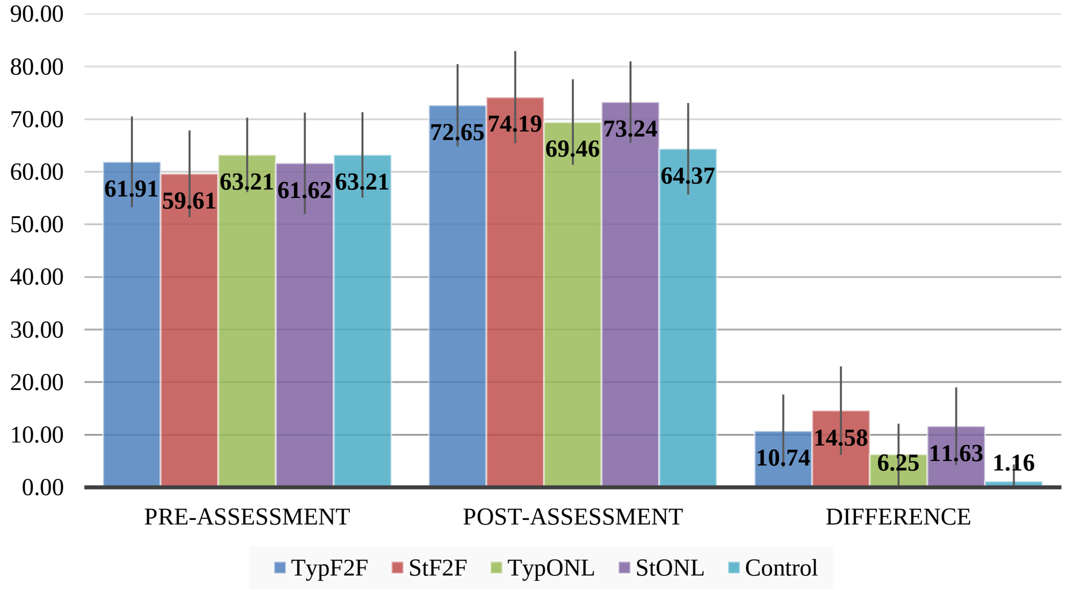


Figure 12. Means and standard deviations for CyS (N=250)

Table 16

Means and Standard Deviations for CyS (N=250)

		Pre-Assessment		Post-Assessment		Pre-Post Difference	
Group	n	Mean	Standard Deviation	Mean	Standard Deviation	Mean	Standard Deviation
TypF2F	50	61.91%	8.62%	72.65%	7.82%	10.74%	6.91%
StF2F	50	59.61%	8.25%	74.19%	8.77%	14.58%	8.42%
TypONL	50	63.21%	7.08%	69.46%	8.14%	6.25%	5.85%
StONL	50	61.62%	9.64%	73.24%	7.75%	11.63%	7.38%
Control	50	63.21%	8.12%	64.37%	8.70%	1.16%	3.18%

In addition to mean and standard deviation analysis, the ANOVA conducted for the main study found a significance below p < 0.001 for both CCA, *F*(1,498) = 111.09, p < 0.001, and CyS, *F*(1,498) = 130.56, p < 0.001, as seen in Table 17. The results indicate that as with the pilot study, main study data analysis also finds differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS.

Table 17

ANOVA Results Between Main Study Groups (N=250)

Variable	F	Sig.	
CCA Score	111.092	***0.000***	***
CyS Score	130.560	***0.000***	***

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

For RQ7, data analysis was completed to determine if there were any significant differences between the two SETA program types, and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study participants, when controlled for participants' (a) age, (b) gender, (c) role in the organization, (d) highest educational level, (e) years working at the organization, and (f) years since last attended formal education. Results of the ANCOVA for each demographic found that gender was not significant for CCA, *F*(1,498) = 0.082, p = 0.774, nor for CyS, *F*(1,498) = 1.786, p = 0.182. While age was not found to be significant for CCA, *F*(6,493) = 1.488, p = 0.180, the result for CyS was significant, *F*(6,493) = 3.169, p = 0.005, suggesting there were differences by age. The ANCOVA conducted for role in the organization was not significant for CCA, *F*(5,494) = 0.771, p = 0.571, or for CyS, *F*(5,494) = 1.046, p = 0.390. The results were similar for years worked at the organization, which was not found to be significant for CCA, *F*(4,495) = 0.753, p = 0.556, nor for CyS, *F*(4,495) = 0.998, p = 0.408. Likewise, years since last formal education was not significant for CCA, *F*(6,493) = 0.590, p = 0.739, or for CyS, *F*(6,493) = 1.896, p = 0.080, although borderline and may require future investigation. The ANCOVA conducted for highest education level was not significant for CCA, *F*(4,495) = 0.986, p = 0.415, however, the result for CyS was significant, *F*(4,495) = 3.047, p = 0.017, suggesting there were differences in CyS based on highest education level of the participant. Table 18 provides an overview of the ANCOVA results.

Table 18

ANCOVA Results for Demographic Items (N=250)

	CCA Score				**CyS Score**				
	df	**Mean Square**	**F**	**Sig.**	**df**	**Mean Square**	**F**	**Sig.**	
Gender	1	0.001	0.082	0.774	1	0.017	1.786	0.182	
Age	6	0.011	1.488	0.180	6	0.029	3.169	***0.005***	**
Role in Organization	5	0.006	0.771	0.571	5	0.01	1.046	0.390	
Years Worked at Organization	4	0.006	0.753	0.556	4	0.009	0.998	0.408	
Highest Education Level	4	0.008	0.986	0.415	4	0.028	3.047	***0.017***	*
Years Since Last Formal Education	6	0.005	0.590	0.739	6	0.018	1.896	0.080	

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

Data analysis continued, addressing the hypotheses for RQ5 and RQ6 beginning with Ho1a: There will be no statistically significant mean differences in employee’s pre- and post-assessment of CCA and CyS for the typical SETA program based on the two delivery methods (face-to-face & online). Spearman Correlation was conducted to assess the differences in CCA and CyS for the face-to-face and online delivery methods of the typical SETA program. Results of the correlations showed, that although significantly different, a weak correlation (r_s= .279, n = 200, p < 0.001).

Additionally, results of the ANCOVA conducted found a significance below p < 0.001 for both CCA, *F*(1,198) = 60.276, p < 0.001, and for CyS, *F*(1,198) = 56.506, p < 0.001. This result is highly significant. Table 19 presents the ANCOVA results for the typical SETA programs, combining both TypONL and TypF2F groups. Data analysis leads to the rejection of Ho1a as statistically significant mean differences are seen between employee's pre- and post-assessment of CCA and CyS for the typical SETA program based on the two delivery methods (face-to-face & online).

Table 19

ANCOVA Results for TypONL and TypF2F (n=200)

	df	**Mean Square Between Groups**	**F**	**Sig.**	
CCA Score	1	0.361	60.276	***0.000***	***
CyS Score	1	0.0361	56.506	***0.000***	***

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

Next, the Spearman Correlation was calculated to assess the differences in CCA and CyS for the face-to-face and online delivery methods of the socio-technical SETA program, addressing Ho1b. Results of the correlations showed a moderate correlation (r_s= 0.437, n = 200, p < 0.001). Furthermore, results of the ANCOVA conducted found a significance below p < 0.001 for both CCA, *F*(1,198) = 89.609, p < 0.001, and for CyS, *F*(1,198) = 115.426, p < 0.001. Similar to the typical SETA program, the result is highly significant. Table 20 presents the ANCOVA results for the socio-technical SETA programs, combining both StONL and StF2F groups. As with Ho1a, data analysis leads to the rejection of Ho1b due to statistically significant mean differences seen between employee's pre- and post-assessment of CCA and CyS for the socio-technical SETA program based on the two delivery methods (face-to-face & online).

Table 20

ANCOVA Results for StONL and StF2F (n=200)

	df	**Mean Square Between Groups**	**F**	**Sig.**	
CCA Score	1	0.467	89.609	***0.000***	***
CyS Score	1	0.859	115.426	***0.000***	***

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

Ho2 stated that there will be no statistically significant mean differences on employee's CCA and CyS between the two SETA program types (typical vs. socio-technical). This hypothesis was also addressed via Spearman Correlation, which assessed the differences in CCA and CyS between the two SETA program types. Results of the correlations showed a weak correlation (r_s= .361, n = 200, p < 0.001). In addition, ANCOVA conducted found a significance below p < 0.001 for both CCA, *F*(1,198) = 89.609, p < 0.001, and for CyS, *F*(1,198) = 115.426, p < 0.001. Again, the result is highly significant. Table 21 presents the ANCOVA results between the two SETA program types. Due to the significance of the ANCOVA results, data analysis leads to the rejection of Ho2 as there are differences are found between the typical and socio-technical program types.

Table 21

ANCOVA Results for Typical and Socio-technical (n=200)

	df	Mean Square Between Groups	F	Sig.	
CCA Score	1	0.825	147.468	***0.000***	***
CyS Score	1	1.167	166.282	***0.000***	***

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

To address Ho3, ANCOVA was used to analyze the interaction between the two SETA program types and the two delivery methods and results are provided in Table 22. Interaction between the two SETA program types and the two delivery methods for the pre-assessment was not significant for CCA, *F*(3,245) = 0.146, p = 0.965, nor for CyS, *F*(3,245) = 0.1.556, p = 0.187. However, interaction between the two SETA program types and the two delivery methods for the post-assessment was found to be significant for both CCA, *F*(3,245) = 15.485, p < 0.001, and for CyS, *F*(3,245) = 11.765, p < 0.001. Ho3 is rejected due to this interaction observed in post-assessment analysis.

Table 22

ANCOVA Results for Pre-Assessment and Post-Assessment Interaction (n=200)

	Pre-Assessment				Post-Assessment				
	df	Mean Square Between Groups	F	Sig.	df	Mean Square Between Groups	F	Sig.	
CCA Scor	3	0.001	0.146	0.965	3	0.056	15.485	***0.000***	***
CyS Score	3	0.011	1.556	0.187	3	0.080	11.765	***0.000***	***

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

Summary

In this chapter, the results of the study were presented with details of each research phase provided in the order performed. A three-phase research approach was used to address the seven research goals and four hypotheses of this study. The first four research goals were successfully addressed by SMEs via the Delphi methodology in Phase 1.

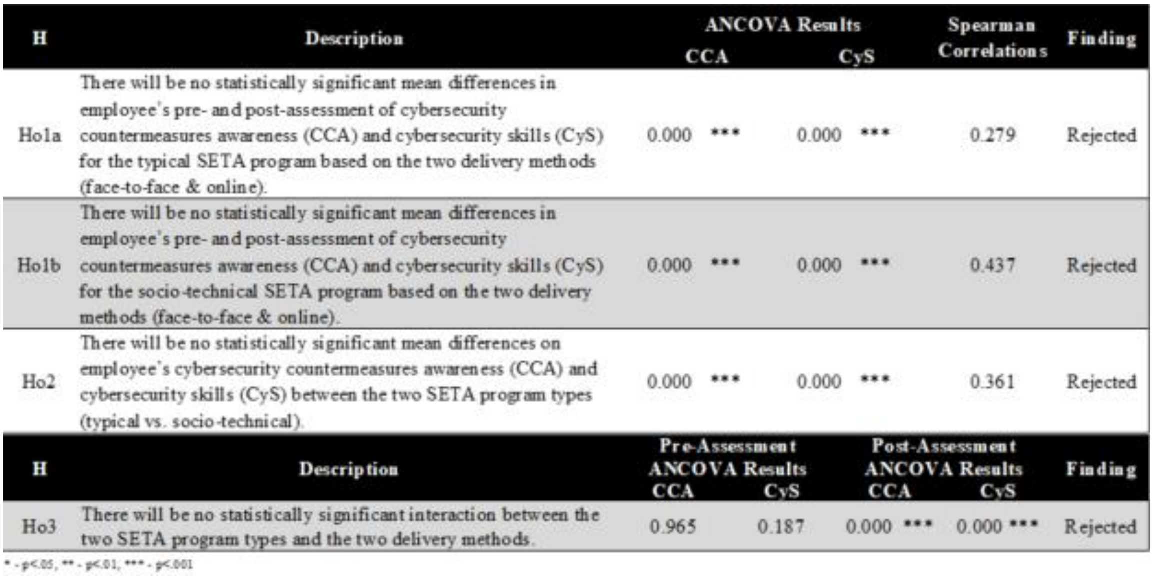
Results included assessment of the SMEs' approved topics for two SETA program types, development and assessment of the SMEs' approved measurement criteria for CCA, determination of SMEs' approved weights for the three CCA categories (awareness of policy, SETA, & monitoring), and development and assessment of the SMEs' approved two SETA programs with integrated vignette-based pre- and post-assessments for CCA and CyS.

The fifth specific goal of this research study was met in Phase 2, using a pilot group of 60 employees who were randomly assigned to one of five groups. The vignette-based pre- and post-assessments of CCA and CyS were used to empirically assess if there were significant differences between the two SETA program types and the two SETA delivery methods, thereby validating the CCA measure. Results were presented in Table 11 and Table 12.

To conclude, Phase 3 was the main study that addressed the two remaining research questions and four hypotheses. In this final research phase, 320 employees were randomly assigned to the five research groups with 250 completing the vignette-based pre-assessment, the prescribed SETA program, and the post-assessment. Means and standard deviations along with ANOVA results were used to empirically assess if there were significant differences in employees' CCA and CyS between the two SETA program types, and the two SETA delivery methods. Goal six was addressed in Table 15, Table 16, and Table 17. Table 18 provides details for goal seven, which analyzed main study data using ANCOVA for any differences when controlling for demographic factors. Lastly, Phase 3 addressed the four research study hypotheses. After data analysis, each null hypothesis was found to be false and was rejected due to empirical findings. Results were presented in Tables 19-22 and are summarized in Table 23.

Table 23

Summary of Hypothesis Analysis



H	Description	ANCOVA Results		Spearman Correlations	Finding
		CCA	CyS		
Ho1a	There will be no statistically significant mean differences in employee's pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the typical SETA program based on the two delivery methods (face-to-face & online).	0.000 ***	0.000 ***	0.279	Rejected
Ho1b	There will be no statistically significant mean differences in employee's pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the socio-technical SETA program based on the two delivery methods (face-to-face & online).	0.000 ***	0.000 ***	0.437	Rejected
Ho2	There will be no statistically significant mean differences on employee's cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) between the two SETA program types (typical vs. socio-technical).	0.000 ***	0.000 ***	0.361	Rejected

H	Description	Pre-Assessment ANCOVA Results		Post-Assessment ANCOVA Results		Finding
		CCA	CyS	CCA	CyS	
Ho3	There will be no statistically significant interaction between the two SETA program types and the two delivery methods.	0.965	0.187	0.000 ***	0.000 ***	Rejected

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

Chapter 5

Conclusions, Discussions, Implications, Recommendations, and Summary

Conclusions

The protection of an organization's IS and information assets from cybersecurity threats is increasingly crucial, especially as businesses become more reliant upon technology for daily business processes (D'Arcy et al., 2009). Employees who lack knowledge and skillsets are seen as a susceptible threat vector for cyber-attacks, and therefore, are being targeted with continually evolving threats (Jang-Jaccard & Nepal, 2014). Therefore, the main goal of this research study was to empirically assess if there are any significant differences on employees' cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) based on the use of two SETA program types (typical & socio-technical) and two SETA delivery methods (face-to-face & online). This study built on previous research by D'Arcy et al. (2009), Levy (2005), Choi et al. (2013), Vance et al. (2012), Oyserman (2009) as well as Dinev et al. (2009), and achieved seven research goals in additional to addressing four hypotheses with empirical evidence.

First, an expert panel was used per the Delphi methodology to develop and validate expert-approved SETA program topics as well as content for the typical and socio-technical programs, and to develop a measure of CCA utilizing validated vignettes for assessment in addition to expert-approved weights of the three CCA categories. Second, the developed measure of CCA was implemented alongside the MyCyberSkills measure validated by the work of Carlton (2016) in both a pre- and post-assessment for a pilot study utilizing 60 employees. The assessments were integrated with the two SETA program types and the two SETA delivery methods, providing a validated CCA measure. In addition, a control group was used to confirm validity and reliability of the study. Lastly, the validated CCA measure developed by this research, accompanied by the validated CyS measure by Carlton (2016), were utilized for the main study. The main study consisted of 250 participants who were randomly assigned to one of five groups: 1) TypONL (typical program via online delivery); 2) StONL (socio-technical program via online delivery); 3) TypF2F (typical program via face-to-face delivery); 4) StF2F (socio-technical program via face-to-face delivery); and 5) Control (the control group which participated in the pre- and post-assessment but did not participate in the SETA program).

Discussions

The first result of this research study was a validated and reliable measure of CCA which adds significantly to the body of knowledge, addressing previous challenges for the determination of SETA program outcomes competency due to dated and limited measures. Due to difficulties with prior construct measures, it was important that further research was conducted to develop and validate a measurement tool to properly assess the CCA level of employees. Furthermore, the second result of this study indicated a significant difference in CyS based on employee age and highest education level. This seems to align with the findings of Carlton (2016) although additional research is needed to investigate the responses for each age group as well as the highest education levels.

Although the employee population had no former cybersecurity-related training while at the University, pre-assessment CCA scores demonstrated a mean of 86.72% with only ten of 250 employees scoring a perfect 100%. Furthermore, the overall mean for the pre-assessment of CyS was 61.91% with no scores of 100%. This demonstrates the need for organizational SETA programs that seek to develop both the CCA and CyS of employees. This study, which focused on two SETA program types (typical vs. socio-technical) via two SETA delivery methods (face-to-face & online), found significant differences in the mean scores for those in socio-typical SETA programs. The face-to-face version of the socio-technical SETA program provided the highest overall return on organizational investment, with a difference between the pre- and post-assessment scores of CCA of 9.51% and CyS of 14.58%. For organizations interested in online SETA program deployment, the socio-technical program via online delivery method provided results that were close to the face-to-face counterpart with a CCA that proved a bit higher mean difference at 9.81% and a CyS mean difference of 11.63%. Of the typical SETA options, the face-to-face delivery method demonstrated the highest empirical results with a CCA mean difference of 8.63% and CyS mean difference of 10.74%. The least responsive program type and delivery method combination proved to be the typical online program, with a CCA mean difference of 8.37% and a CyS mean difference far lower than the other groups at 6.25%.

Based on these empirical results, the benefits of socio-technical SETA programs seem clear. While traditional training has been held in face-to-face format, online methods are increasing in popularity as they have proven to be cost-effective, flexible options for organizations (Dimeff et al., 2009; Salas et al., 2002; Vernadakis et al., 2011). However, this study provides empirical evidence regarding the best program type and delivery method combinations for cybersecurity training specifically.

Implications

The findings of this study contributed substantially to the body of knowledge, providing both researchers and practitioners with additional insight into the development of both the CCA and CyS of employees. The validated measure could be used by organizations who seek to utilize a vignette-based assessment for their workforce instead of self-report methods, which may not provide an accurate depiction of the CCA level of employees. Additionally, knowledge of the implications of utilizing a typical vs. socio-technical SETA program type, whether via face-to-face or online methods, are essential for organizations who are charged with protecting organization IS assets. This study provides empirically validated data regarding the most beneficial SETA program type and delivery method for cybersecurity training, facilitating organization decisions on how to best use resources for training of employees on this critical aspect of daily business. This knowledge will decrease the chance for losses due to naïve employee cybersecurity behaviors and increase organization efficiency.

Recommendations and Future Research

This research study was designed to develop a validated measure of CCA as well as expert-approved SETA program topics and content for organization programs. While the goals of this research were successfully met, there are many areas for future research. First, limitations of this study should be addressed to validate the findings within other countries, especially those with a different culture than exists in the United States. Moreover, the SETA program was implemented within the University as a workforce training initiative, which could lend itself to bias. Further research is required to replicate the findings with other types of organizations, organization size, organization culture, and diverse population demographics. Additionally, more in-depth investigation in into the impact of age and higher education on CyS is warranted based on the findings of this study.

Summary

The research problem that this dissertation study addressed is employees' naive cybersecurity practices, which can lead to organizational hazards including financial implications, impact on business reputation, loss of company information assets, and proprietary information leakage (D'Arcy et al., 2009; Lebek et al., 2013; Vance et al., 2012). Employee practices are a key factor in the mitigation of cybersecurity threats within the organization. The development of cybersecurity countermeasures awareness (CCA) as well as cybersecurity skills (CyS) through SETA initiatives is imperative. However, additional research was needed to determine the most valuable program type and delivery method. Although previous studies have exposed the need for organizational SETA programs, very few have focused on what SETA should encompass and the factors that are most likely to increase success. Therefore, this study contributed to the body of knowledge by empirically assessing if there are significant differences in CCA along with CyS based on the use of two SETA program types (typical vs. socio-technical) and two SETA delivery methods (face-to-face & online).

Development and validation of a measurement tool to properly assess the CyS and CCA level of employees was imperative to this research study due to the limitations of construct measurement in previous research. Qualitative data collection methods were used in Phase 1 for the elicitation of SME panel assistance with revision and validation of SETA program topics, weights for the CCA categories, as well as measurement criteria for CCA. The Delphi methodology was used to ensure reliability and validity of the instruments created.

RQ1: What are the SMEs' approved topics for the two SETA program types using the Delphi methodology?

RQ2: What are the SMEs' approved measurement criteria for CCA using the Delphi methodology?

RQ3: What are the SMEs' approved weights for the three CCA categories (awareness of policy, SETA, & monitoring)?

RQ4: What are the SMEs' approved two SETA programs with integrated vignette-based assessments for CCA and CyS using the Delphi methodology?

Phase 2 consisted of a pilot study with randomized participant group allocation into one of two developed SETA program types (typical & socio-technical) delivered via two delivery methods (face-to-face & online) as well as to the control group. Pilot data was collected from both a pre- and post-assessment integrated with each SETA program and data analysis performed using ANOVA to ensure validity and reliability. The SETA programs and the CCA instrument, were revised per the preliminary data analysis, addressing RQ5 and providing validated measures for the main study.

RQ5: Are there any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using a pilot group of participants?

The main study was Phase 3 of the research, with participants assigned randomly to two developed SETA program types (typical & socio-technical) delivered via two delivery methods (face-to-face & online) as well as to the control group. Main study data was collected from both a pre- and post-assessment integrated with each SETA program, and pre-analysis data screening was completed. This was followed by main study data analysis which empirically assessed if there are any significant differences on employees' CCA and CyS based on the use of two SETA program types (typical vs. socio-technical) and two SETA delivery methods (face-to-face & online). Pre- and post-analysis scores for each of the four program type and delivery method combinations and for the control group were completed using ANOVA. In addition, ANCOVA was used to compare the groups, while also controlling for a variable that may exert an influence on the dependent variable (Mertler & Vannatta, 2010).

RQ6: Are there any significant differences between the two SETA program types and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study group of participants?

RQ7a-e: Are there any significant differences between the two SETA program types, and the two SETA delivery methods based on the vignette-based pre- and post-assessments of CCA and CyS using the main study participants, when controlled for participants' (a) age, (b) gender, (c) role in the organization, (d) highest educational level, (e) years working at the organization, and (f) years since last attended formal education?

The following null hypotheses for RQ5 and RQ6 were tested between comparisons for SETA type (typical & socio-technical) and delivery method (face-to-face & online).

Assessment used factorial ANCOVA and Spearman Correlation to assess the statistical significance of each when controlling for participants' (a) age, (b) gender, (c) role in the organization, (d) highest educational level, (e) years working at the organization, and (f) years since last attended formal education. Recommendations for SETA program type and delivery method as a result of data analysis were provided.

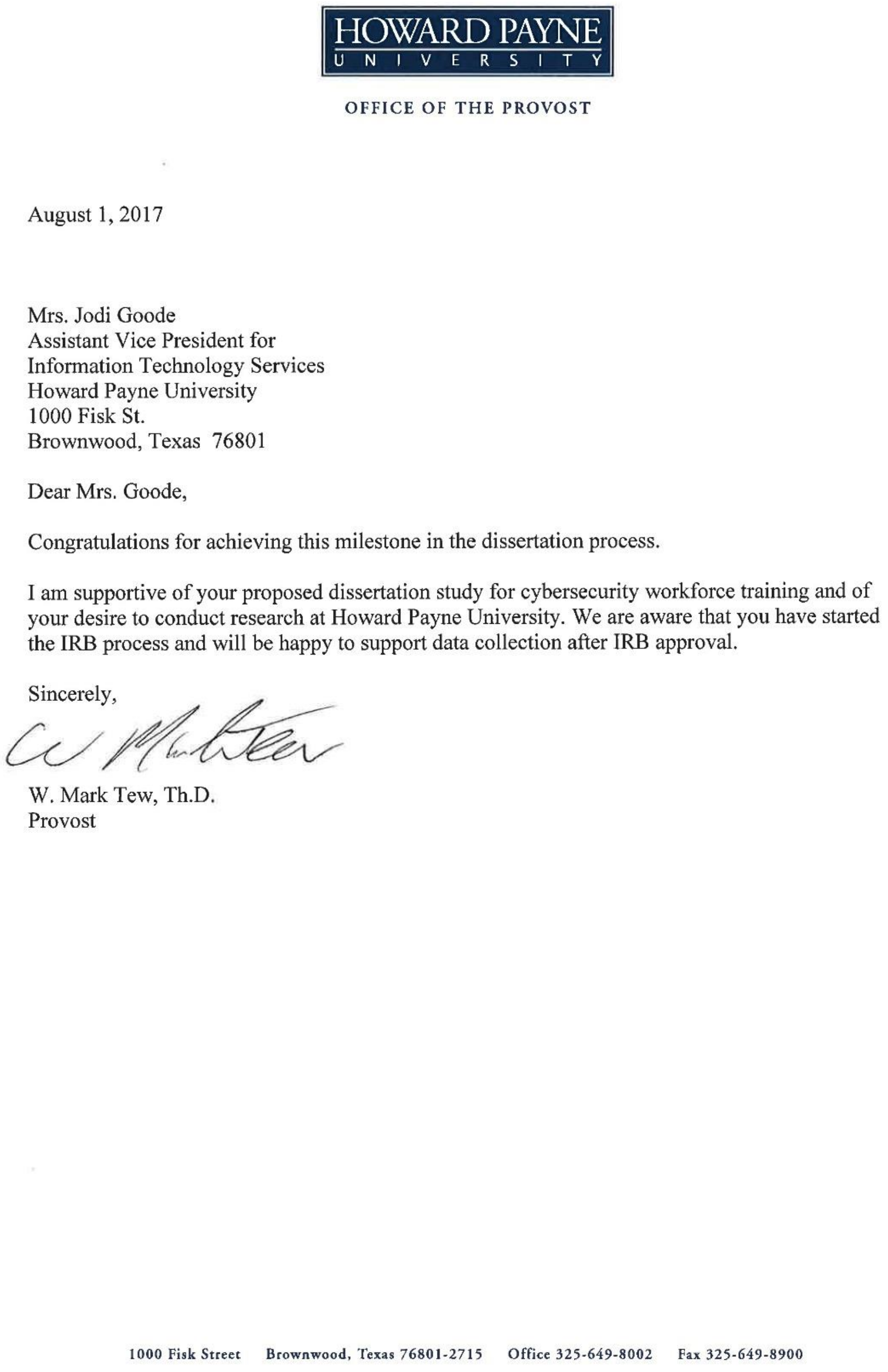
Ho1a: There will be no statistically significant mean differences in employee’s pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the typical SETA program based on the two delivery methods (face-to-face & online).

Ho1b: There will be no statistically significant mean differences in employee’s pre- and post-assessment of cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) for the socio-technical SETA program based on the two delivery methods (face-to-face & online).

Ho2: There will be no statistically significant mean differences on employee’s cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) between the two SETA program types (typical & socio-technical).

In conclusion, this research study made several contributions to the body of knowledge, providing empirical evidence related to the most effective SETA program type and delivery method for cybersecurity specific training, which will be equally beneficial to researchers and practitioners. The value of socio-technical SETA programs was evident from the main study findings. In addition, expert-approved SETA program topics were provided and a validated CCA measure created which can be used by those seeking a reliable vignette-based assessment as a part of SETA program deployment.

Appendix A



HOWARD PAYNE
UNIVERSITY

OFFICE OF THE PROVOST

August 1, 2017

Mrs. Jodi Goode
Assistant Vice President for
Information Technology Services
Howard Payne University
1000 Fisk St.
Brownwood, Texas 76801

Dear Mrs. Goode,

Congratulations for achieving this milestone in the dissertation process.

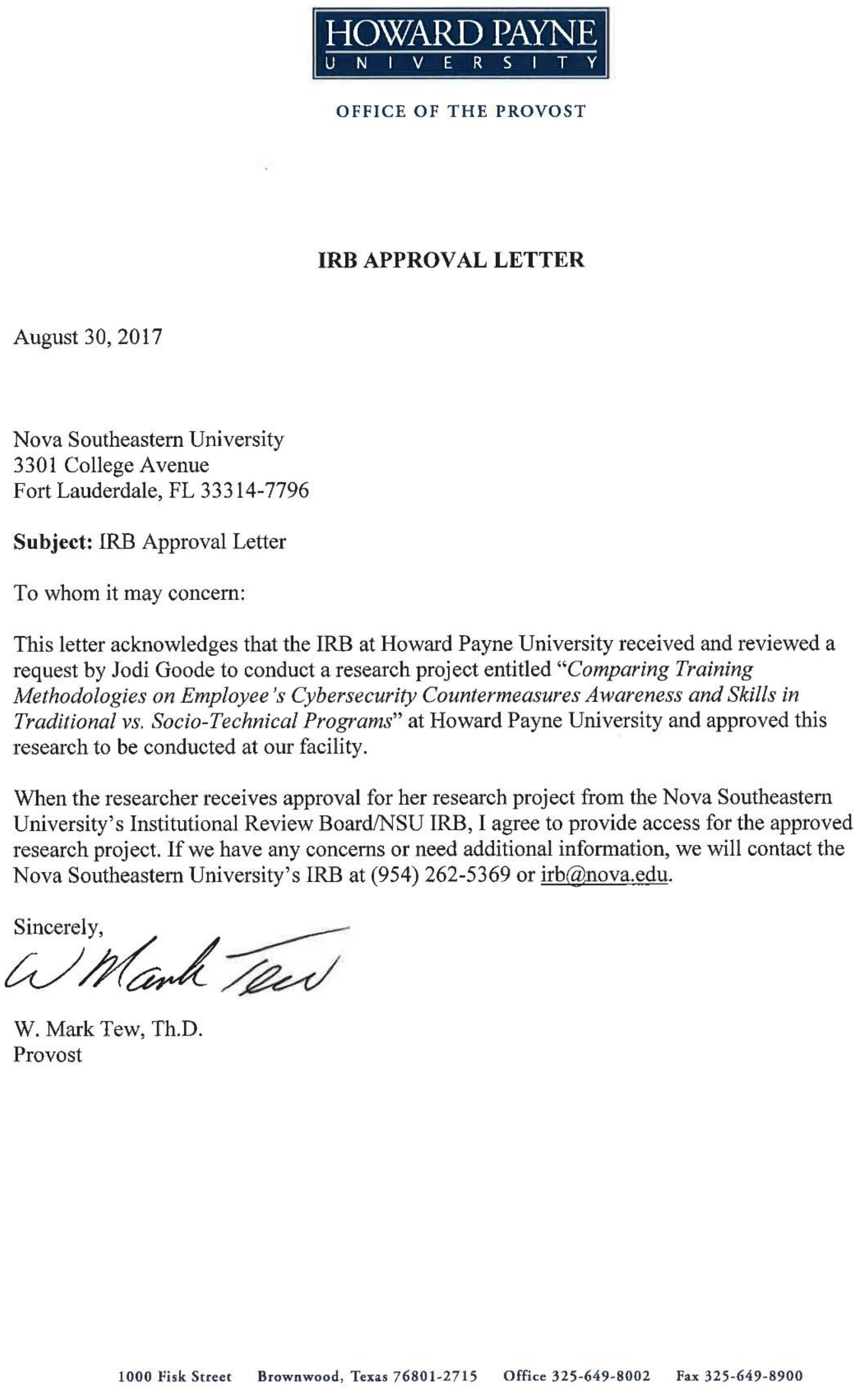
I am supportive of your proposed dissertation study for cybersecurity workforce training and of your desire to conduct research at Howard Payne University. We are aware that you have started the IRB process and will be happy to support data collection after IRB approval.

Sincerely,

W. Mark Tew, Th.D.
Provost

1000 Fisk Street Brownwood, Texas 76801-2715 Office 325-649-8002 Fax 325-649-8900

Appendix B



HOWARD PAYNE
UNIVERSITY

OFFICE OF THE PROVOST

IRB APPROVAL LETTER

August 30, 2017

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

Subject: IRB Approval Letter

To whom it may concern:

This letter acknowledges that the IRB at Howard Payne University received and reviewed a request by Jodi Goode to conduct a research project entitled "*Comparing Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs*" at Howard Payne University and approved this research to be conducted at our facility.

When the researcher receives approval for 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.

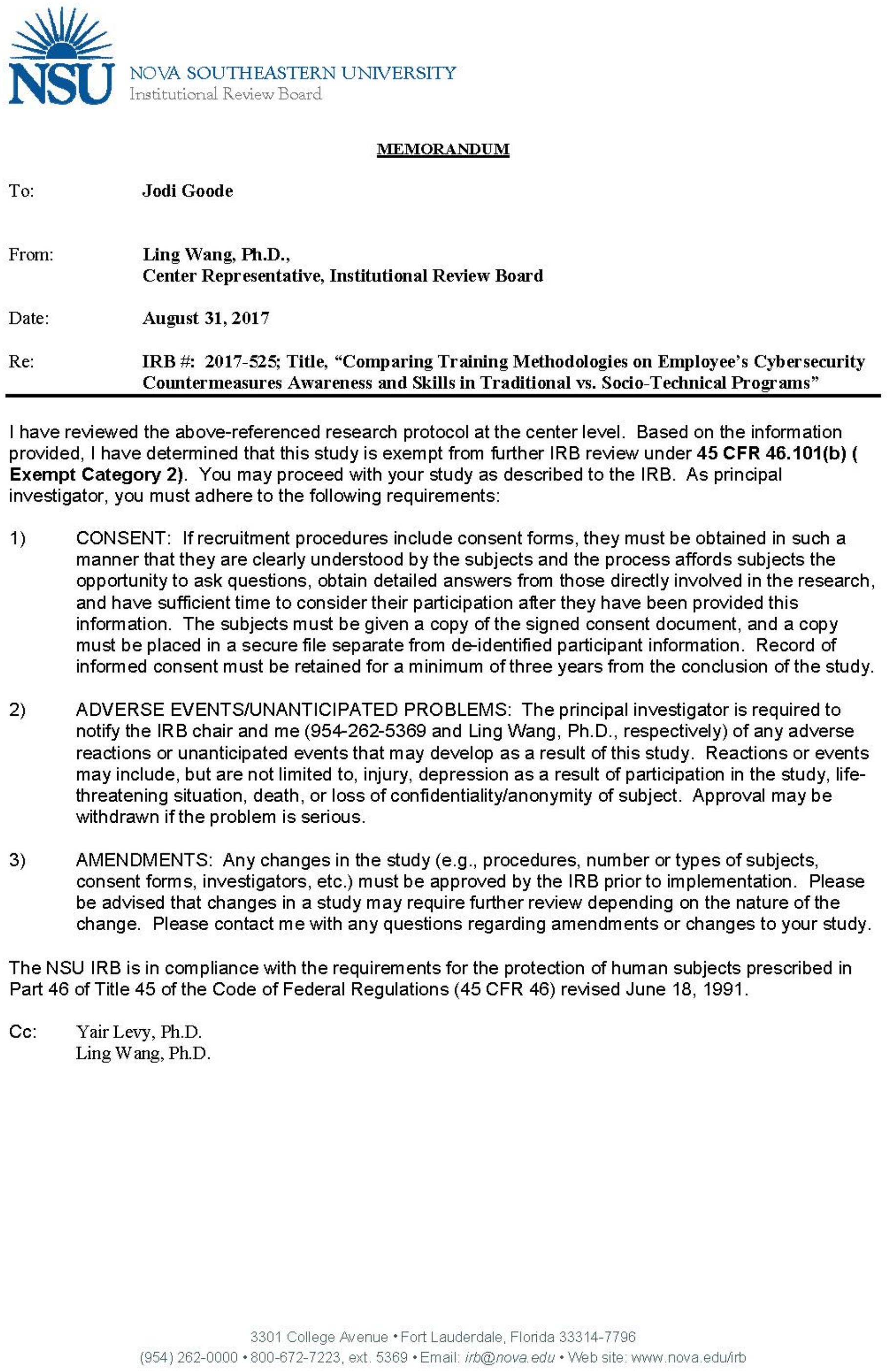
Sincerely,

W Mark Tew

W. Mark Tew, Th.D.
Provost

1000 Fisk Street   Brownwood, Texas 76801-2715   Office 325-649-8002   Fax 325-649-8900

Appendix C



NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Jodi Goode**

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

Date: **August 31, 2017**

Re: **IRB #: 2017-525; Title, "Comparing Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt Category 2)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-0000 • 800-672-7223, ext. 5369 • Email: *irb@nova.edu* • Web site: www.nova.edu/irb

Appendix D

Demographic Questions

1. What is your gender?
    a. Female
    b. Male

2. Age (Enter in years):

3. What is the highest level of education you have completed?
    a. Elementary School
    b. Middle School
    c. High School
    d. College Degree
    e. Graduate Degree
    f. Other

4. Select the number of years since your last formal education.
    a. 0-4
    b. 5-9
    c. 10-14
    d. 15-19
    e. 20-24
    f. 25-29
    g. 30 or more

5. Select the option that best describes your role within the organization.
    a. Full-time employee
    b. Part-time employee
    c. First level supervisor
    d. Middle management
    e. Upper management

6. Number of years worked in the organization:
    a. Less than 1
    b. 1-2
    c. 3-5
    d. 6-10
    e. Over 10

Appendix E

Expert Panel Recruitment Email

Dear Information Systems and Cybersecurity Experts,

I would like to request your assistance in providing expert feedback on several pieces of 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, working under the supervision of Professor Yair Levy. My research deals with cybersecurity training for employees and the potential impact that different program types (online vs. face-to-face) or delivery methods (typical vs. socio-technical) might have on cybersecurity countermeasures awareness and skills.

With your help, I seek to develop a measure of cybersecurity countermeasures awareness as well as a validated security education, training, and awareness (SETA) program. The program will be delivered via four treatments: typical program via online delivery; socio-technical program via online delivery; typical program via face-to-face delivery; socio-technical program via face-to-face delivery. Both the typical and socio-technical SETA programs will be based on the same cybersecurity topics. However, while the typical SETA program will inform the employee of organizational policies and actions that should and should not be taken, the socio-technical SETA program will also include explanations of why certain actions may cause difficulties and the potential organizational outcomes associated.

The information provided will be used for this research study in aggregated form and no personally identifiable information (PII) will be collected. As an expert participant, you agree to keep all information regarding this research confidential and to refrain from disclosing any details related to subsequent study surveys or the material contained within them. Input for each item below will be gathered anonymously, synthesized, and then follow-up round(s) of questions may be sent to help reach consensus amongst the panel as needed.

1) Approved topics for the two SETA program types (typical & socio-technical).
2) Approved vignettes for measuring cybersecurity countermeasures awareness.
3) Approved weights for the three cybersecurity countermeasures awareness categories (awareness of policy, SETA, & monitoring).
4) Approved content of the two SETA program types (typical & socio-technical) in the two delivery methods (online & face-to-face).

If you are willing to participate on this expert panel, maintain a high level of confidentiality, and non-disclosure as it pertains items, *please click here to start the evaluation*.

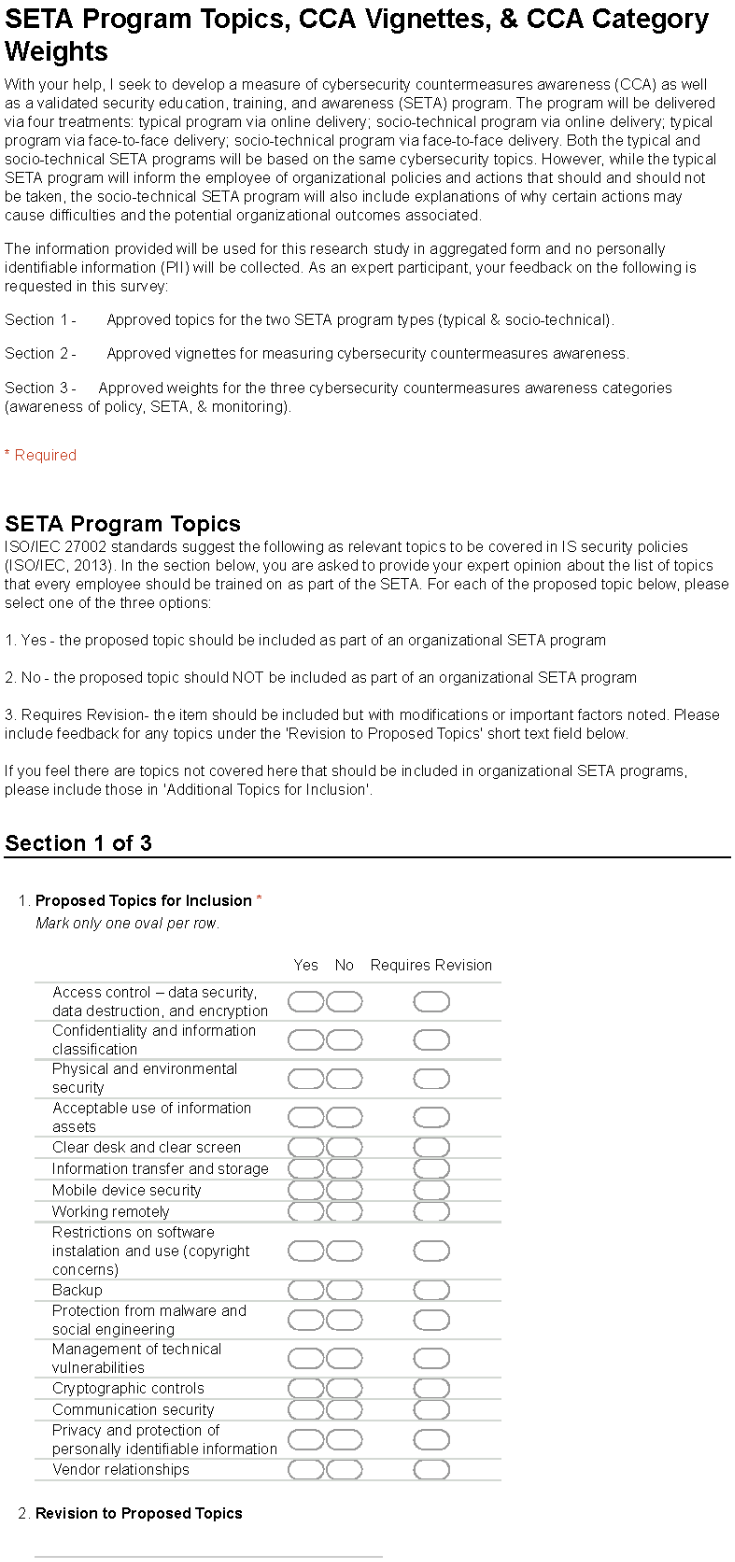
Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. If you would like to receive the findings of the study, please indicate it with your reply to this email and I will be happy to provide you with information about the academic research publication(s)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

Regards,

Jodi Goode, Ph.D. Candidate
E-mail: jp1587@mynsu.nova.edu
Information Systems and Cybersecurity

Appendix F

Expert Panel Survey



SETA Program Topics, CCA Vignettes, & CCA Category Weights

With your help, I seek to develop a measure of cybersecurity countermeasures awareness (CCA) as well as a validated security education, training, and awareness (SETA) program. The program will be delivered via four treatments: typical program via online delivery; socio-technical program via online delivery; typical program via face-to-face delivery; socio-technical program via face-to-face delivery. Both the typical and socio-technical SETA programs will be based on the same cybersecurity topics. However, while the typical SETA program will inform the employee of organizational policies and actions that should and should not be taken, the socio-technical SETA program will also include explanations of why certain actions may cause difficulties and the potential organizational outcomes associated.

The information provided will be used for this research study in aggregated form and no personally identifiable information (PII) will be collected. As an expert participant, your feedback on the following is requested in this survey:

Section 1 - Approved topics for the two SETA program types (typical & socio-technical).

Section 2 - Approved vignettes for measuring cybersecurity countermeasures awareness.

Section 3 - Approved weights for the three cybersecurity countermeasures awareness categories (awareness of policy, SETA, & monitoring).

* Required

SETA Program Topics

ISO/IEC 27002 standards suggest the following as relevant topics to be covered in IS security policies (ISO/IEC, 2013). In the section below, you are asked to provide your expert opinion about the list of topics that every employee should be trained on as part of the SETA. For each of the proposed topic below, please select one of the three options:

1. Yes - the proposed topic should be included as part of an organizational SETA program

2. No - the proposed topic should NOT be included as part of an organizational SETA program

3. Requires Revision- the item should be included but with modifications or important factors noted. Please include feedback for any topics under the 'Revision to Proposed Topics' short text field below.

If you feel there are topics not covered here that should be included in organizational SETA programs, please include those in 'Additional Topics for Inclusion'.

Section 1 of 3

1. **Proposed Topics for Inclusion** *

Mark only one oval per row.

	Yes	No	Requires Revision
Access control – data security, data destruction, and encryption	○	○	○
Confidentiality and information classification	○	○	○
Physical and environmental security	○	○	○
Acceptable use of information assets	○	○	○
Clear desk and clear screen	○	○	○
Information transfer and storage	○	○	○
Mobile device security	○	○	○
Working remotely	○	○	○
Restrictions on software instalation and use (copyright concerns)	○	○	○
Backup	○	○	○
Protection from malware and social engineering	○	○	○
Management of technical vulnerabilities	○	○	○
Cryptographic controls	○	○	○
Communication security	○	○	○
Privacy and protection of personally identifiable information	○	○	○
Vendor relationships	○	○	○

2. **Revision to Proposed Topics**

3.

4.

5. **Additional Topics for Inclusion**

6.

7.

Vignette-Based Measurement of Cybersecurity Countermeasures Awareness (CCA)

Previous research has defined cybersecurity countermeasures awareness (CCA) as the state where individuals are aware of their cybersecurity mission within the organization. CCA includes three categories: employee awareness of security policies, SETA programs, and computer monitoring.

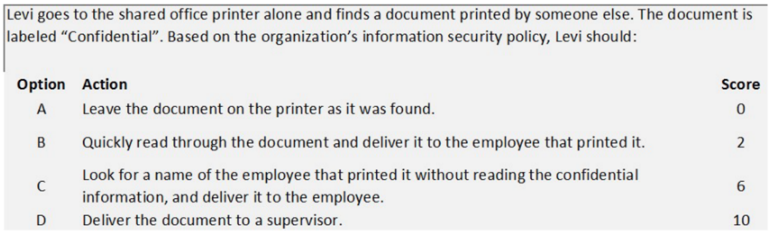
The proposed vignettes below have been developed based on prior empirical research and seek to assess the CCA of the employee. Each will cover one of the three categories of CCA and address key IS security policy topics. Please review each of the vignettes and answer the questions below regarding clarity of wording, validity, and scoring.

Section 2 of 2

CCA Category - Policy

Please answer the following questions for each of the vignettes created to address the policy category.

CCA-P1



Levi goes to the shared office printer alone and finds a document printed by someone else. The document is labeled "Confidential". Based on the organization's information security policy, Levi should:

Option	Action	Score
A	Leave the document on the printer as it was found.	0
B	Quickly read through the document and deliver it to the employee that printed it.	2
C	Look for a name of the employee that printed it without reading the confidential information, and deliver it to the employee.	6
D	Deliver the document to a supervisor.	10

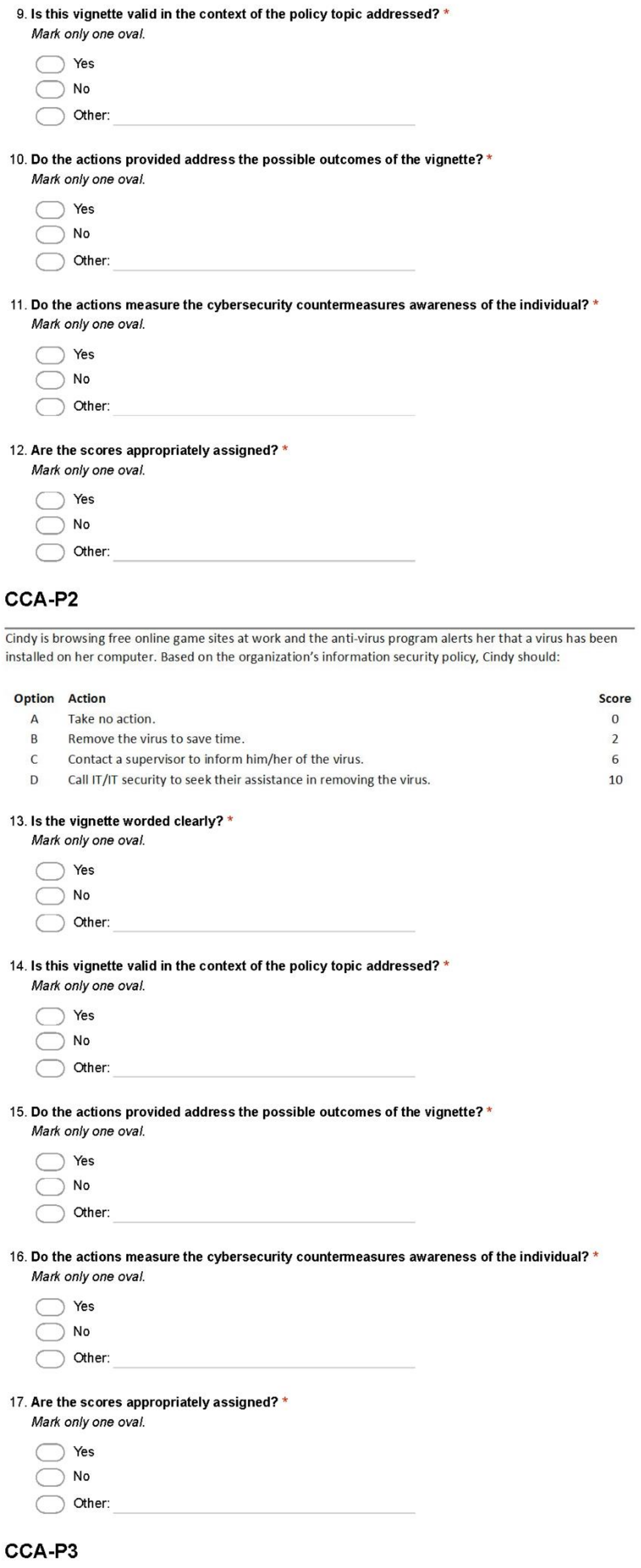
8. **Is the vignette worded clearly?** *

Mark only one oval.

○ Yes

○ No

○ Other:



9. **Is this vignette valid in the context of the policy topic addressed?** *

Mark only one oval.

○ Yes

○ No

○ Other: ____________________

10. **Do the actions provided address the possible outcomes of the vignette?** *

Mark only one oval.

○ Yes

○ No

○ Other: ____________________

11. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *

Mark only one oval.

○ Yes

○ No

○ Other: ____________________

12. **Are the scores appropriately assigned?** *

Mark only one oval.

○ Yes

○ No

○ Other: ____________________

CCA-P2

Cindy is browsing free online game sites at work and the anti-virus program alerts her that a virus has been installed on her computer. Based on the organization's information security policy, Cindy should:

Option	Action	Score
A	Take no action.	0
B	Remove the virus to save time.	2
C	Contact a supervisor to inform him/her of the virus.	6
D	Call IT/IT security to seek their assistance in removing the virus.	10

13. **Is the vignette worded clearly?** *

Mark only one oval.

○ Yes

○ No

○ Other: ____________________

14. **Is this vignette valid in the context of the policy topic addressed?** *

Mark only one oval.

○ Yes

○ No

○ Other: ____________________

15. **Do the actions provided address the possible outcomes of the vignette?** *

Mark only one oval.

○ Yes

○ No

○ Other: ____________________

16. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *

Mark only one oval.

○ Yes

○ No

○ Other: ____________________

17. **Are the scores appropriately assigned?** *

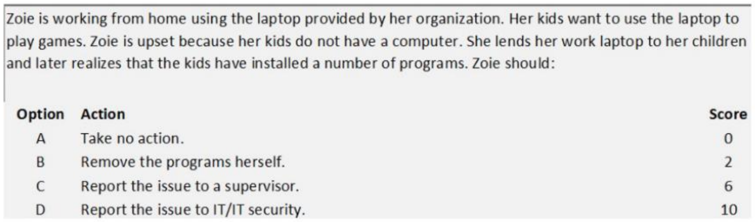
Mark only one oval.

○ Yes

○ No

○ Other: ____________________

CCA-P3



Zoie is working from home using the laptop provided by her organization. Her kids want to use the laptop to play games. Zoie is upset because her kids do not have a computer. She lends her work laptop to her children and later realizes that the kids have installed a number of programs. Zoie should:

Option	Action	Score
A	Take no action.	0
B	Remove the programs herself.	2
C	Report the issue to a supervisor.	6
D	Report the issue to IT/IT security.	10

18. **Is the vignette worded clearly?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

19. **Is this vignette valid in the context of the policy topic addressed?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

20. **Do the actions provided address the possible outcomes of the vignette?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

21. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

22. **Are the scores appropriately assigned?** *

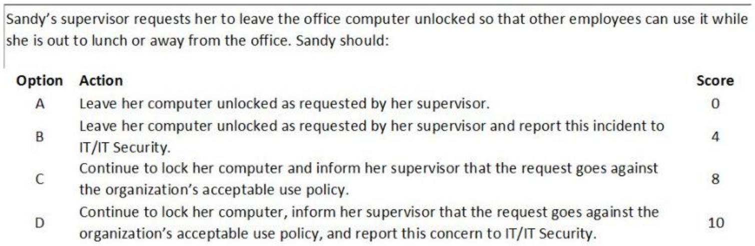
Mark only one oval.

○ Yes
○ No
○ Other: ____________________

CCA Category - Awareness of SETA

Please answer the following questions for each of the vignettes created to address the awareness of SETA category.

CCA-S1



Sandy's supervisor requests her to leave the office computer unlocked so that other employees can use it while she is out to lunch or away from the office. Sandy should:

Option	Action	Score
A	Leave her computer unlocked as requested by her supervisor.	0
B	Leave her computer unlocked as requested by her supervisor and report this incident to IT/IT Security.	4
C	Continue to lock her computer and inform her supervisor that the request goes against the organization's acceptable use policy.	8
D	Continue to lock her computer, inform her supervisor that the request goes against the organization's acceptable use policy, and report this concern to IT/IT Security.	10

23. **Is the vignette worded clearly?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

24. **Is this vignette valid in the context of the policy topic addressed?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

25. **Do the actions provided address the possible outcomes of the vignette?** *

Mark only one oval.

○ Yes
○ No
○ Other: ______________________________

26. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *

Mark only one oval.

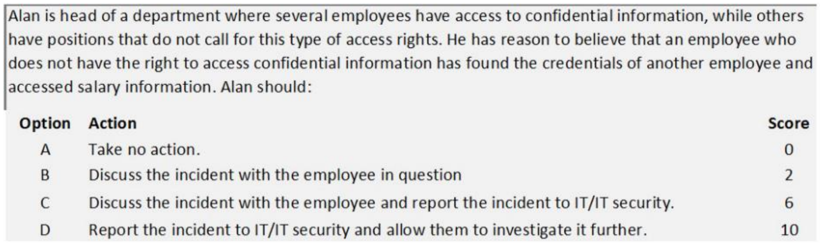
○ Yes
○ No
○ Other: ______________________________

27. **Are the scores appropriately assigned?** *

Mark only one oval.

○ Yes
○ No
○ Other: ______________________________

CCA-S2



Alan is head of a department where several employees have access to confidential information, while others have positions that do not call for this type of access rights. He has reason to believe that an employee who does not have the right to access confidential information has found the credentials of another employee and accessed salary information. Alan should:

Option	Action	Score
A	Take no action.	0
B	Discuss the incident with the employee in question	2
C	Discuss the incident with the employee and report the incident to IT/IT security.	6
D	Report the incident to IT/IT security and allow them to investigate it further.	10

28. **Is the vignette worded clearly?** *

Mark only one oval.

○ Yes
○ No
○ Other: ______________________________

29. **Is this vignette valid in the context of the policy topic addressed?** *

Mark only one oval.

○ Yes
○ No
○ Other: ______________________________

30. **Do the actions provided address the possible outcomes of the vignette?** *

Mark only one oval.

○ Yes
○ No
○ Other: ______________________________

31. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *

Mark only one oval.

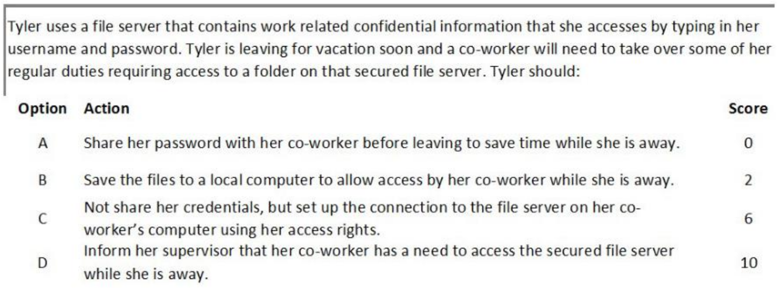
○ Yes
○ No
○ Other: ______________________________

32. **Are the scores appropriately assigned?** *

Mark only one oval.

○ Yes
○ No
○ Other: ______________________________

CCA-S3



Tyler uses a file server that contains work related confidential information that she accesses by typing in her username and password. Tyler is leaving for vacation soon and a co-worker will need to take over some of her regular duties requiring access to a folder on that secured file server. Tyler should:

Option	Action	Score
A	Share her password with her co-worker before leaving to save time while she is away.	0
B	Save the files to a local computer to allow access by her co-worker while she is away.	2
C	Not share her credentials, but set up the connection to the file server on her co-worker's computer using her access rights.	6
D	Inform her supervisor that her co-worker has a need to access the secured file server while she is away.	10

33. **Is the vignette worded clearly?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

34. **Is this vignette valid in the context of the policy topic addressed?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

35. **Do the actions provided address the possible outcomes of the vignette?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

36. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

37. **Are the scores appropriately assigned?** *

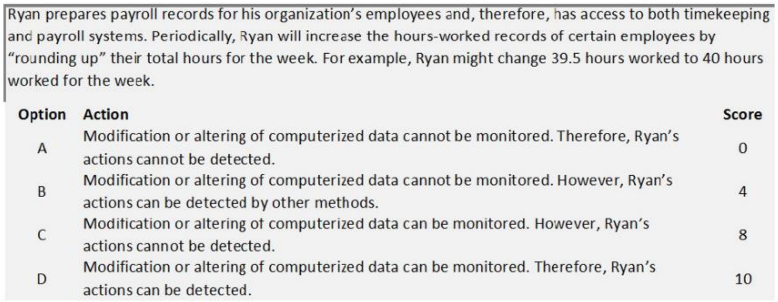
Mark only one oval.

○ Yes
○ No
○ Other: ____________________

CCA Category - Monitoring

Please answer the following questions for each of the vignettes created to address the monitoring category.

CCA-M1



Ryan prepares payroll records for his organization's employees and, therefore, has access to both timekeeping and payroll systems. Periodically, Ryan will increase the hours-worked records of certain employees by "rounding up" their total hours for the week. For example, Ryan might change 39.5 hours worked to 40 hours worked for the week.

Option	Action	Score
A	Modification or altering of computerized data cannot be monitored. Therefore, Ryan's actions cannot be detected.	0
B	Modification or altering of computerized data cannot be monitored. However, Ryan's actions can be detected by other methods.	4
C	Modification or altering of computerized data can be monitored. However, Ryan's actions cannot be detected.	8
D	Modification or altering of computerized data can be monitored. Therefore, Ryan's actions can be detected.	10

38. **Is the vignette worded clearly?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

39. **Is this vignette valid in the context of the policy topic addressed?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

40. **Do the actions provided address the possible outcomes of the vignette?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

41. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *

Mark only one oval.

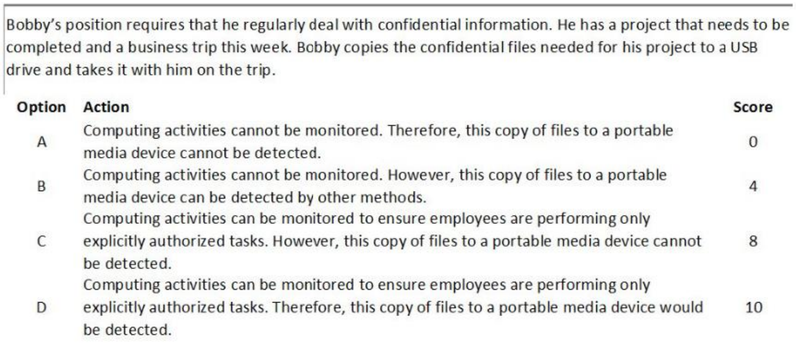
○ Yes
○ No
○ Other: ____________________

42. **Are the scores appropriately assigned?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

CCA-M2



Bobby's position requires that he regularly deal with confidential information. He has a project that needs to be completed and a business trip this week. Bobby copies the confidential files needed for his project to a USB drive and takes it with him on the trip.

Option	Action	Score
A	Computing activities cannot be monitored. Therefore, this copy of files to a portable media device cannot be detected.	0
B	Computing activities cannot be monitored. However, this copy of files to a portable media device can be detected by other methods.	4
C	Computing activities can be monitored to ensure employees are performing only explicitly authorized tasks. However, this copy of files to a portable media device cannot be detected.	8
D	Computing activities can be monitored to ensure employees are performing only explicitly authorized tasks. Therefore, this copy of files to a portable media device would be detected.	10

43. **Is the vignette worded clearly?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

44. **Is this vignette valid in the context of the policy topic addressed?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

45. **Do the actions provided address the possible outcomes of the vignette?** *

Mark only one oval.

○ Yes
○ No
○ Other: ____________________

46. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *

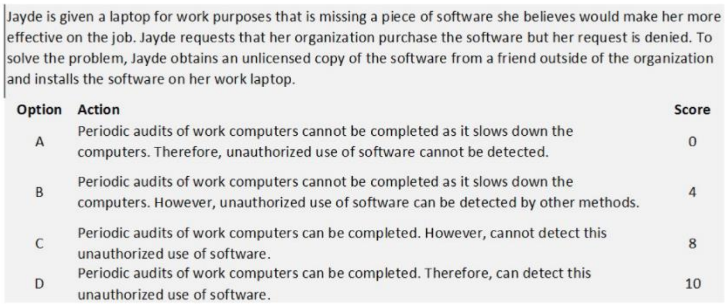
Mark only one oval.

○ Yes
○ No
○ Other: ____________________

47. **Are the scores appropriately assigned?** *
Mark only one oval.

○ Yes
○ No
○ Other: ______________________

CCA-M3



Jayde is given a laptop for work purposes that is missing a piece of software she believes would make her more effective on the job. Jayde requests that her organization purchase the software but her request is denied. To solve the problem, Jayde obtains an unlicensed copy of the software from a friend outside of the organization and installs the software on her work laptop.

Option	Action	Score
A	Periodic audits of work computers cannot be completed as it slows down the computers. Therefore, unauthorized use of software cannot be detected.	0
B	Periodic audits of work computers cannot be completed as it slows down the computers. However, unauthorized use of software can be detected by other methods.	4
C	Periodic audits of work computers can be completed. However, cannot detect this unauthorized use of software.	8
D	Periodic audits of work computers can be completed. Therefore, can detect this unauthorized use of software.	10

48. **Is the vignette worded clearly?** *
Mark only one oval.

○ Yes
○ No
○ Other: ______________________

49. **Is this vignette valid in the context of the policy topic addressed?** *
Mark only one oval.

○ Yes
○ No
○ Other: ______________________

50. **Do the actions provided address the possible outcomes of the vignette?** *
Mark only one oval.

○ Yes
○ No
○ Other: ______________________

51. **Do the actions measure the cybersecurity countermeasures awareness of the individual?** *
Mark only one oval.

○ Yes
○ No
○ Other: ______________________

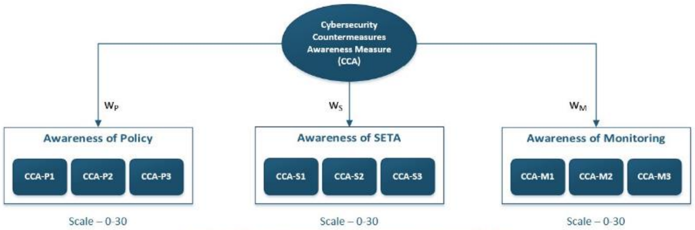
52. **Are the scores appropriately assigned?** *
Mark only one oval.

○ Yes
○ No
○ Other: ______________________

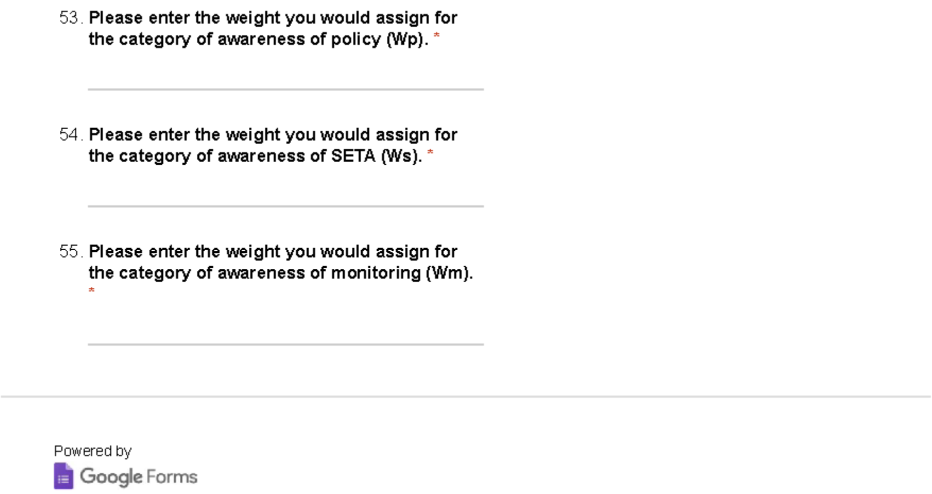
Weights for Three CCA Categories

Please answer the questions below to assist in determining the weights for each of the three categories of Cybersecurity Countermeasures Awareness (CCA). Keep in mind that the three percentages provided below should equal 100%.

Section 3 of 3



Weights of the three categories to be determined by Delphi findings.
Policy % + SETA % + Monitoring % = 100%



53. **Please enter the weight you would assign for the category of awareness of policy (Wp).** *

54. **Please enter the weight you would assign for the category of awareness of SETA (Ws).** *

55. **Please enter the weight you would assign for the category of awareness of monitoring (Wm).** *

Appendix G

Research Study Recruitment Email

Faculty & Staff,

With cyber threats constantly developing and increasing in sophistication, cybersecurity training is now important for organizations. This fall, a cybersecurity training program will be offered to all employees with the goal of increasing awareness of cyber threats facing us as a University, discussing organizational policies and procedures, and ultimately helping you better understand the role you play in keeping data secure.

You are encouraged not only to complete the training course materials but to also participate in the anonymous pre- and post-assessment. The assessment will take approximately 45 minutes to complete and will gather absolutely no personal information. I am currently 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. The data gathered from the pre- and post-assessments will be used in a generalized manner as part of my research study, which seeks to determine the most successful cybersecurity training method within the organization.

If you are willing to participate, please reply to this email and you will be contacted with additional details on how to access the pre- and post-assessments. You must be 18 years of age or older.

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

Warmest Regards,
Jodi Goode, Ph.D. Candidate
Email: jp1587@mynsu.nova.edu
Information System and Cybersecurity

Appendix H

Proposed Cybersecurity Countermeasures Awareness Vignettes

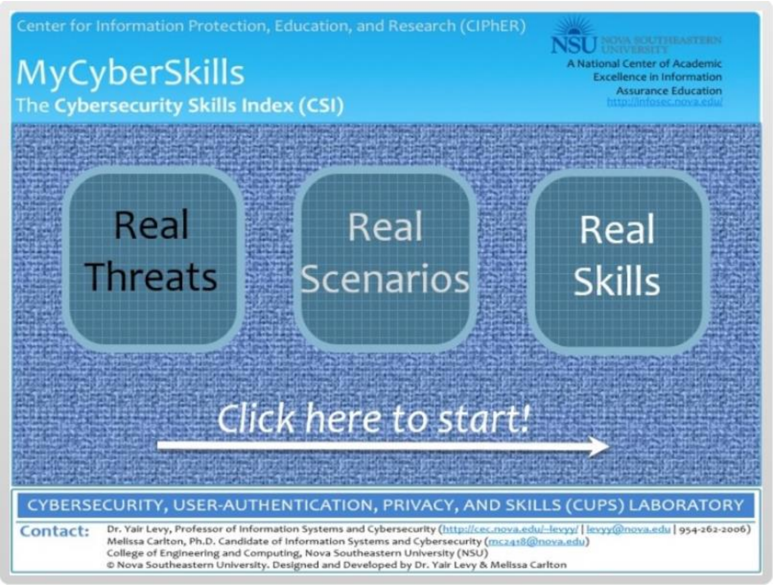
	CCA Measure	*Vignette*			*Policy Topic*	*Adapted From*
Policy	CCA-P1	Levi goes to the shared office printer alone and finds a document printed by someone else. The document is labeled "Confidential". Based on the organization's information security policy, Levi should:			Disclosure of information Doherty et al. (2011)	Vance et al. (2012)
		Option	**Action**	**Score**		
		A	Leave the document on the printer as it was found.	0	Acceptable Use Policy SANS Institute (2014)	
		B	Quickly read through the document and deliver it to the employee that printed it.	2		
		C	Look for a name of the employee that printed it without reading the confidential information, and deliver it to the employee.	6		
		D	Deliver the document to a supervisor.	10		
	CCA-P2	Cindy is browsing free online game sites at work and the anti-virus program alerts her that a virus has been installed on her computer. Based on the organization's information security policy, Cindy should:			Prevention of viruses and worms Doherty et al. (2011)	Vance et al. (2012)
		Option	**Action**	**Score**		
		A	Take no action.	0	Acceptable Use Policy SANS Institute (2014)	
		B	Remove the virus to save time.	2		
		C	Contact a supervisor to inform him/her of the virus.	6		
		D	Call IT/IT security to seek their assistance in removing the virus.	10		
	CCA-P3	Zoie is working from home using the laptop provided by her organization. Her kids want to use the laptop to play games. Zoie is upset because her kids do not have a computer. She lends her work laptop to her children and later realizes that the kids have installed a number of programs. Zoie should:			Mobile computing Doherty et al. (2011)	Vance et al. (2012)
		Option	**Action**	**Score**		
		A	Take no action.	0	Acceptable Use Policy SANS Institute (2014)	
		B	Remove the programs herself.	2		
		C	Report the issue to a supervisor.	6		
		D	Report the issue to IT/IT security.	10		
SETA	CCA-S1	Sandy's supervisor requests her to leave the office computer unlocked so that other employees can use it while she is out to lunch or away from the office. Sandy should:			User access management Doherty et al. (2011)	Vance et al. (2012)
		Option	**Action**	**Score**		
		A	Leave her computer unlocked as requested by her supervisor.	0		
		B	Leave her computer unlocked as requested by her supervisor and report this incident to IT/IT Security.	4	Acceptable Use Policy SANS Institute (2014)	

		C	Continue to lock her computer and inform her supervisor that the request goes against the organization's acceptable use policy.	8		
		D	Continue to lock her computer, inform her supervisor that the request goes against the organization's acceptable use policy, and report this concern to IT/IT Security.	10		
	CCA-S2		Alan is head of a department where several employees have access to confidential information, while others have positions that do not call for this type of access rights. He has reason to believe that an employee who does not have the right to access confidential information has found the credentials of another employee and accessed salary information. Alan should:		Violations and breaches Doherty et al. (2011)	Hovav and D'Arcy (2012)
		Option	**Action**	**Score**		
		A	Take no action.	0	Acceptable Use Policy SANS Institute (2014)	
		B	Discuss the incident with the employee in question	2		
		C	Discuss the incident with the employee and report the incident to IT/IT security.	6		
		D	Report the incident to IT/IT security and allow them to investigate it further.	10		
	CCA-S3		Tyler uses a file server that contains work-related confidential information that she accesses by typing in her username and password. Tyler is leaving for vacation soon and a co-worker will need to take over some of her regular duties requiring access to a folder on that secured file server. Tyler should:		User access management Doherty et al. (2011)	Vance et al. (2012)
		Option	**Action**	**Score**		
		A	Share her password with her co-worker before leaving to save time while she is away.	0	Password Protection Policy SANS Institute (2014)	
		B	Save the files to a local computer to allow access by her co-worker while she is away.	2		
		C	Not share her credentials, but set up the connection to the file server on her co-worker's computer using her access rights.	6		
		D	Inform her supervisor that her co-worker has a need to access the secured file server while she is away.	10		
Monitoring	CCA-M1		Ryan prepares payroll records for his organization's employees and, therefore, has access to both timekeeping and payroll systems. Periodically, Ryan will increase the hours-worked records of certain employees by "rounding up" their total hours for the week. For example, Ryan might change 39.5 hours worked to 40 hours worked for the week.		User access management Doherty et al. (2011)	Hovav and D'Arcy (2012)
		Option	**Action**	**Score**		
		A	Modification or altering of computerized data cannot be monitored. Therefore, Ryan's actions cannot be detected.	0	Ethics Policy SANS Institute (2014)	
		B	Modification or altering of computerized data cannot be monitored. However, Ryan's actions can be detected by other methods.	4		
		C	Modification or altering of computerized data can be monitored. However, Ryan's actions cannot be detected.	8		
		D	Modification or altering of computerized data can be monitored. Therefore, Ryan's actions can be detected.	10		
	CCA-M2		Bobby's position requires that he regularly deal with confidential information. He has a project that needs to be completed and a business trip this week. Bobby copies the confidential files needed for his project to a USB drive and takes it with him on the trip.		Physical security of infrastructure and information resources Doherty et al. (2011)	Vance et al. (2012); Hovav and D'Arcy (2012)
		Option	**Action**	**Score**		

	A	Computing activities cannot be monitored. Therefore, this copy of files to a portable media device cannot be detected.	0		
	B	Computing activities cannot be monitored. However, this copy of files to a portable media device can be detected by other methods.	4	Acceptable Use Policy SANS Institute (2014)	
	C	Computing activities can be monitored to ensure employees are performing only explicitly authorized tasks. However, this copy of files to a portable media device cannot be detected.	8		
	D	Computing activities can be monitored to ensure employees are performing only explicitly authorized tasks. Therefore, this copy of files to a portable media device would be detected.	10		
CCA-M3	Jayde is given a laptop for work purposes that is missing a piece of software she believes would make her more effective on the job. Jayde requests that her organization purchase the software but her request is denied. To solve the problem, Jayde obtains an unlicensed copy of the software from a friend outside of the organization and installs the software on her work laptop.			Software development and maintenance Doherty et al. (2011)	Hovav and D'Arcy (2012)
	Option	**Action**	**Score**		
	A	Periodic audits of work computers cannot be completed as it slows down the computers. Therefore, unauthorized use of software cannot be detected.	0	Acceptable Use Policy SANS Institute (2014)	
	B	Periodic audits of work computers cannot be completed as it slows down the computers. However, unauthorized use of software can be detected by other methods.	4		
	C	Periodic audits of work computers can be completed. However, cannot detect this unauthorized use of the software.	8		
	D	Periodic audits of work computers can be completed. Therefore, can detect this unauthorized use of the software.	10		

Appendix I

MyCyberSkills Assessment Example Screens



Center for Information Protection, Education, and Research (CIPhER)

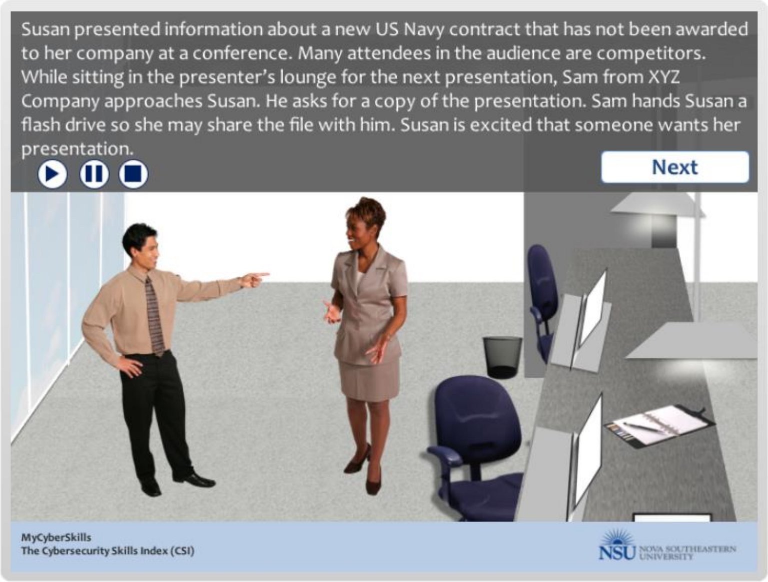
MyCyberSkills

The Cybersecurity Skills Index (CSI)

NSU NOVA SOUTHEASTERN UNIVERSITY
A National Center of Academic Excellence in Information Assurance Education
http://infosec.nova.edu/
Real Threats
Real Scenarios
Real Skills
Click here to start!

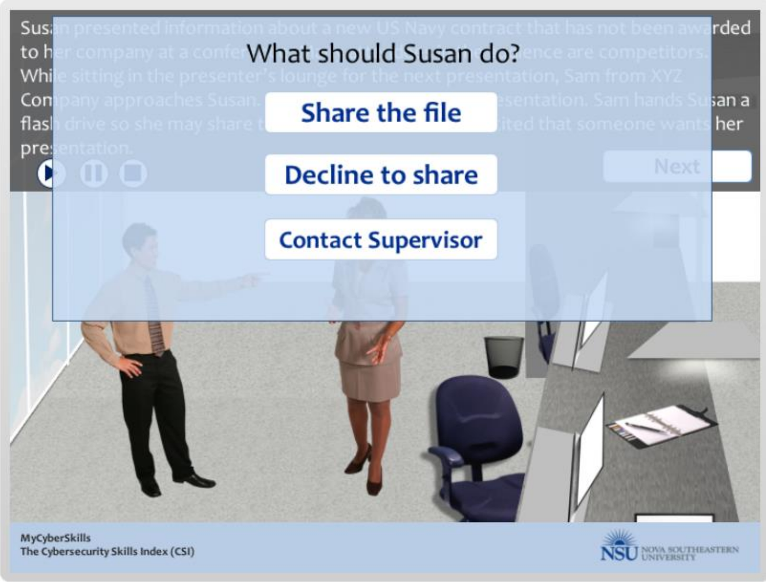
CYBERSECURITY, USER-AUTHENTICATION, PRIVACY, AND SKILLS (CUPS) LABORATORY

Contact: Dr. Yair Levy, Professor of Information Systems and Cybersecurity (http://cec.nova.edu/~levyy/ | levyy@nova.edu | 954-262-2006)
Melissa Carlton, Ph.D. Candidate of Information Systems and Cybersecurity (mc2418@nova.edu)
College of Engineering and Computing, Nova Southeastern University (NSU)
© Nova Southeastern University. Designed and Developed by Dr. Yair Levy & Melissa Carlton



Susan presented information about a new US Navy contract that has not been awarded to her company at a conference. Many attendees in the audience are competitors. While sitting in the presenter's lounge for the next presentation, Sam from XYZ Company approaches Susan. He asks for a copy of the presentation. Sam hands Susan a flash drive so she may share the file with him. Susan is excited that someone wants her presentation.

Next
MyCyberSkills
The Cybersecurity Skills Index (CSI)
NSU NOVA SOUTHEASTERN UNIVERSITY



Susan presented information about a new US Navy contract that has not been awarded to her company at a confer ence are competitors. While sitting in the presenter's lounge for the next presentation, Sam from XYZ Company approaches Susan. esentation. Sam hands Susan a flash drive so she may share t ited that someone wants her presentation.

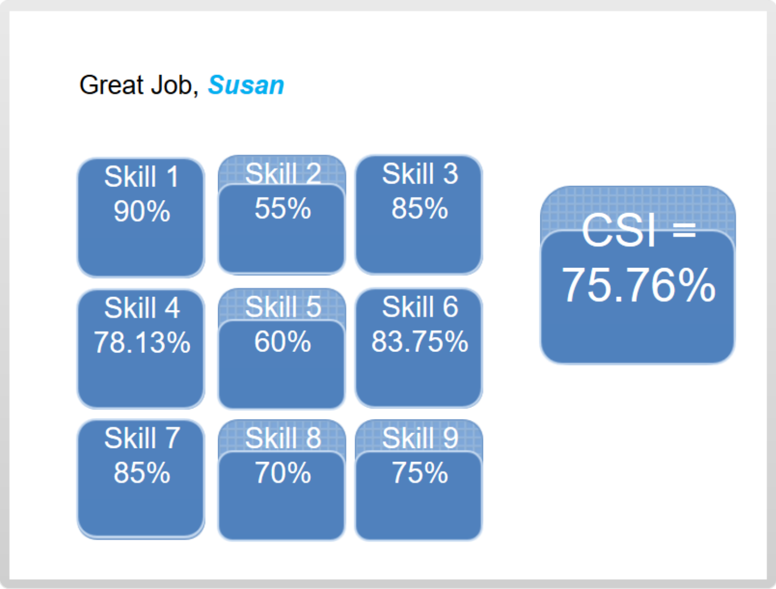
What should Susan do?

Share the file

Decline to share

Contact Supervisor

Next
MyCyberSkills
The Cybersecurity Skills Index (CSI)
NSU NOVA SOUTHEASTERN UNIVERSITY



Great Job, ***Susan***

Skill 1 90%	Skill 2 55%	Skill 3 85%
Skill 4 78.13%	Skill 5 60%	Skill 6 83.75%
Skill 7 85%	Skill 8 70%	Skill 9 75%

CSI = 75.76%

References

Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 2*(4), 1-12.

ACM Joint Task Force on Cybersecurity Education. (2017). Defining Cybersecurity. Retrieved June 2, 2018, from https://cybered.hosting.acm.org/

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). Research report: The evolving relationship between general and specific computer self-efficacy - An empirical assessment. *Information Systems Research, 11*(4), 418-430.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012a). Information security policy compliance: The role of information security awareness. *18th Americas Conference on Information Security*, Seattle, WA.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012b). Security policy compliance: User acceptance perspective. *45th Hawaii International Conference on System Science*, Maui, HI.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

Alexander, D. (2000). Scenario methodology for teaching principles of emergency management. *Disaster Prevention and Management: An International Journal, 9*(2), 89-97.

Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). Social engineering in social networking sites: How good becomes evil. *Pacific Asia Conference on Information Systems*, Chengdu, China.

Anderson, C., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *Management Information Systems Quarterly, 34*(3), 613-643.

Anderson, J. (1982). Acquisition of cognitive skill. *The Psychological Review, 89*(4), 369-406.

Arbaugh, J., Bangert, A., & Cleveland-Innes, M. (2010). Subject matter effects and the community of inquiry (CoI) framework: An exploratory study. *The Internet and Higher Education, 13*(1), 37-44.

Arbaugh, J., DeArmond, S., & Rau, B. (2013). New uses for existing tools? A call to study on-line management instruction and instructors. *Academy of Management Learning & Education, 12*(4), 635-655.

Arbaugh, J., Desai, A., Rau, B., & Sridhar, B. (2010). A review of research on online and blended learning in the management disciplines: 1994–2009. *Organization Management Journal, 7*(1), 39-55.

Bachman, R., Paternoster, R., & Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law and Society Review*, 343-372.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. New York: Freeman.

Barter, C., & Renold, E. (1999). The use of vignettes in qualitative research. *Social Research Updates, 25*(9), 1-6.

Best, R. J. (1974). An experiment in delphi estimation in marketing decision making. *Journal of Marketing Research*, 448-452.

Boer, H., & Seydel, E. R. (1996). Protection motivation theory *Predicting Health Behavior: Research & Practice with Social Cognition Models* (pp. 95-120). Buckingham, PA: Open University Press.

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. *International Conference on Technologies for Homeland Security*, Waltham, MA.

Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology, 11*(3-4), 279-295.

Broadbent, D. E. (1958). *Perception and communication*. London: Pergamon.

Brown, B. B. (1968). *Delphi process: A methodology used for the elicitation of opinions of experts*. Santa Monica, CA: The Rand Corporation.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly, 34*(3), 523-548.

Callister, R. R., & Love, M. S. (2016). A comparison of learning outcomes in skills-based courses: Online versus face-to-face formats. *Decision Sciences Journal of Innovative Education, 14*(2), 243-256.

Carlton, M. (2016). *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills* (Doctoral dissertation), Nova Southeastern University, Proquest Dissertations Publishing. (10240271)

Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills of non-IT professionals. *IEEE SoutheastCon Conference*, Fort Lauderdale, FL.

Carlton, M., Levy, Y., Ramim, M., & Terrell, S. (2015). Development of the MyCyberSkills iPad app: A scenarios-based, hands-on measure of non-IT professional' cybersecurity skills. *Pre-ICIS Workshop on Information Security and Privacy*, Fort Worth, TX.

Carruth, A. K., Pryor, S., Cormier, C., Bateman, A., Matzke, B., & Gilmore, K. (2010). Evaluation of a school-based train-the-trainer intervention program to teach first aid and risk reduction among high school students. *The Journal of School Health, 80*(9), 453-460.

Cheng, B., Wang, M., Yang, S. J., & Peng, J. (2011). Acceptance of competency-based workplace e-learning systems: Effects of individual and peer learning support. *Computers & Education, 57*(1), 1317-1333.

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. *Pre-International Conference of Information Systems on Information Security & Privacy*, Milan, Italy.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Clark, R. E. (1994). Media will never influence learning. *Educational Technology Research & Development, 42*(2), 21-29.

Clayton, M. J. (1997). Delphi: A technique to harness expert opinion for critical decision-making tasks in education. *Educational Psychology, 17*(4), 373-386.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *Management Information Systems Quarterly, 19*(2), 189-211.

Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative*. Upper Saddle River, NJ: Merrill Prentice Hall.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

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.

Davis, M. C., Challenger, R., Jayewardene, D. N., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics, 45*(2), 171-180.

Deutsch, J. A., & Deutsch, D. (1963). Attention: Some theoretical considerations. *The Psychological Review, 70*(1), 80.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security, 7*(4), 171-175.

Dimeff, L. A., Koerner, K., Woodcock, E. A., Beadnell, B., Brown, M. Z., Skutch, J. M., . . . Harned, M. S. (2009). Which training method works best? A randomized controlled trial comparing three methods of training clinicians in dialectical behavior therapy skills. *Behaviour Research & Therapy, 47*(11), 921-930.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 23.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*(3), 201-209.

Faux, T. L., & Black-Hughes, C. (2000). A comparison of using the Internet versus lectures to teach social work history. *Journal of Research on Social Work Practice, 10*(4), 454-466.

Finch, J. (1987). The vignette technique in survey research. *Sociology*, 105-114.

Fitts, P. M. (1964). Perceptual-motor skill learning *Categories for Human Learning*. New York, NY: Academic Press.

Flaskerud, J. H. (1979). Use of vignettes to elicit responses toward broad concepts. *Nursing Research, 28*(4), 210-211.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(1), 983-988.

Furnell, S., Gaunt, P., Holben, R., Sanders, P., Stockel, C., & Warren, M. (1996). Assessing staff attitudes towards information security in a European healthcare establishment. *Journal of Medical Informatics, 21*(2), 105-112.

Furnell, S., & Thomson, K.-L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security, 2009*(2), 5-10.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(1), 7.

Gordon, T., & Glenn, J. (2009). *Futures research methodology*.

Gould, D. (1996). Using vignettes to collect data for nursing research studies: How valid are the findings? *International Journal of Clinical Nursing, 5*(4), 207-212.

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

Gray, P., & Hovav, A. (2008). From hindsight to foresight: Applying futures research techniques in information systems. *Communications of the Association for Information Systems, 22*(1), 12.

Gray, P., & Hovav, A. (2014). Using scenarios to understand the frontiers of IS. *Information Systems Frontiers, 16*(3), 337-345.

Gundu, T., & Flowerday, S. (2012). The enemy within: A behavioural intention model and an information security awareness process. *Information Security for South Africa Conference*, Grahamstown, South Africa.

Gupta, S., Bostrom, R. P., & Huber, M. (2010). End-user training methods: What we know, need to know. *Communications of the ACM, 41*(4), 9-39.

Hall, K., Mero, N., & Cheramie, R. (2017). Reflecting on performance feedback: The effect of counterfactual thinking on individual learning. *77th Annual Meeting of the Academy of Management*, Atlanta, GA.

Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination*: Sage.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US 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. *Journal of the Association for Information Systems, 34*(50), 893-912.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, 35-49.

Hughes, R., & Huby, M. (2002). The application of vignettes in social and nursing research. *Advanced Nursing, 37*(4), 382-386.

Hughes, R., & Huby, M. (2012). The construction and interpretation of vignettes in social research. *Social Work and Social Sciences Review, 11*(1), 36-51.

IBM Global Technology Services. (2014). IBM security services 2014 cyber security intelligence index. Retrieved July 25, 2015, from http://www-03.ibm.com/security/services/2014-cyber-security-intelligence-index-infographic/

ISO/IEC. (2013). ISO/IEC 27002. *2013 Information technology- Security techniques - Code of practice for information security controls.* Retrieved July 1, 2016, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer & System Sciences, 80*(5), 973-993.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Management Information Systems Quarterly, 34*(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *Management Information Systems Quarterly, 39*(1), 113-134.

Kahneman, D. (1973). *Attention and effort* (Vol. 1063). Cliffs, New Jersey: Prentice-Hall Englewood.

Kahneman, D., & Treisman, A. (1984). *Changing views of attention and automaticity*. New York: Academic Press.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security, 43*(2), 64-76.

Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. *Communications of the ACM, 34*(2), 43-48.

Kerlinger, F., & Lee, H. (2000). *Foundations of behavioral research*. Holt, NY: Harcourt College Publishers.

Kraiger, K., & Ford, J. K. (2006). The expanding role of workplace training: Themes and trends influencing training research and practice. *Historical perspectives in Industrial & Organizational Psychology*, 281-309.

Kranz, J., & Haeussinger, F. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. *International Conference on Information Systems*, Auckland, Australia.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 46*(1), 254-264.

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.

Lavie, N., & Tsal, Y. (1994). Perceptual load as a major determinant of the locus of selection in visual attention. *Attention, Perception, & Psychophysics, 56*(2), 183-197.

Lebek, B., Uffen, J., Neumann, M., & Hohler, B. (2013). Towards a needs assessment process model for security, education, training and awareness programs: An action design research study. *European Conference on Information Systems*, Utrecht, The Netherlands.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 57-63.

Lerouge, C., Newton, S., & Blanton, J. E. (2005). Exploring the systems analyst skill set: Perceptions, preferences, age, and gender. *Journal of Computer Information Systems, 45*(3).

Levy, Y. (2003). A study of learners' perceived value and satisfaction for implied effectiveness of online learning systems. *Dissertation Abstracts International, A65*(03), 1014-1344.

Levy, Y. (2005). A case study of management skills comparison in online and on-campus MBA programs. *International Journal of Information & Communication Technology Education, 1*(3), 1-20.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishers.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science, 9*, 181-212.

Levy, Y., & Ramim, M. M. (2015). The effect of competence-based simulations on management skills enhancements in e-learning courses. *Interdisciplinary Journal of e-Skills & Lifelong Learning, 11*, 179-190.

Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems, 4*(1), 65-95.

Linstone, H. A., & Turoff, M. (1975). *The Delphi method: Techniques and applications* (Vol. 29): Addison-Wesley Reading, MA.

Linstone, H. A., & Turoff, M. (2002). *The Delphi method: Techniques and applications* (Vol. 18): Addison-Wesley Publishing Company, Advanced Book Program.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Experimental Social Psychology, 19*(5), 469-479.

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.

McLaren, C. H. (2004). A comparison of student persistence and performance in online and classroom business statistics experiences. *Decision Sciences Journal of Innovative Education, 2*(1), 1-10.

Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods: Practical application and interpretation*. Los Angeles, CA: Pyrczak.

National Initiative for Cybersecurity Careers & Studies. (2014). Cyber glossary. Retrieved June 15, 2015, from https://niccs.us-cert.gov/awareness/cybersecurity-101

National Institute of Standards & Technology. (2013). Glossary of key information security terms. Retrieved July 22, 2015, from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Neff, J. A. (1979). Interactional versus hypothetical others: The use of vignettes in attitude research. *Sociology & Social Research, 64*(1), 105-125.

Netteland, G., Wasson, B., & Morch, A. I. (2007). E-learning in a large organization: A study of the critical role of information sharing. *Journal of Workplace Learning, 19*(6), 392-411.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

O'Fallon, M. J., & Butterfield, K. D. (2005). A review of the empirical ethical decision-making literature: 1996–2003. *Journal of Business Ethics, 59*(4), 375-413.

Orvis, K. A., Fisher, S. L., & Wasserman, M. E. (2009). Power to the people: Using learner control to improve trainee reactions and learning in web-based instructional environments. *The Journal of Applied Psychology, 94*(4), 960.

Oyserman, D. (2008). Possible selves: Identity-based motivation and school success. *Self-Processes, Learning, & Enabling Human Potential*, 269-288.

Oyserman, D. (2009). Identity-based motivation: Implications for action-readiness, procedural-readiness, and consumer behavior. *Journal of Consumer Psychology, 19*(3), 276-279.

Oyserman, D. (2013). Not just any path: Implications of identity-based motivation for disparities in school outcomes. *Economics of Education Review, 33*, 179-190.

Oyserman, D., & Smith, G. (2015). Just not worth my time? Experienced difficulty and time investment. *Social Cognition, 33*(2), 85-103.

Oyserman, D., Smith, G., & Elmore, K. (2014). Identity-based motivation: Implications for health and health disparities. *Journal of Social Issues, 70*(2), 206-225.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Hawaii International Conference on System Sciences*, Waikoloa, HI.

Park, J. H., & Wentling, T. (2007). Factors associated with transfer of training in workplace e-learning. *Journal of Workplace Learning, 19*(5), 311-329.

Parlamis, J. D., & Mitchell, L. D. (2014). Teaching negotiations in the new millennium: Evidence-based recommendations for online course delivery. *Negotiation Journal, 30*(1), 93-113.

Parrish, J. L., & Nicolas-Rocca, S. (2012). Toward better decisions with respect to is security: Integrating mindfulness into IS security training. *Pre-ICIS Workshop on Information Security & Privacy*, Orlando, FL.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176.

Paul, T. V. (2014). An evaluation of the effectiveness of e-learning, mobile learning, and instructor-led training in organizational training and development. *Journal of Human Resource & Adult Learning, 10*(2), 1-13.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *The Journal of Management, 12*(4), 531-544.

Ponemon Institute. (2015). Cost of Cyber Crime Study. Retrieved September 12, 2016, from http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/

PricewaterhouseCoopers. (2016). The Global State of Information Security® Survey 2016. Retrieved March 1, 2016, from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Management Information Systems Quarterly, 34*(4), 757-778.

Putri, F. F., & Hovav, A. (2014). Employees compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. *European Conference on Information Systems*, Tel Aviv, Israel.

Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Journal of Applied Knowledge Management, 2*(1), 122-136.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7–8), 241-253.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

Rhee, H. S., Ryu, Y., & Kim, C.-T. (2005). I am fine but you are not: Optimistic bias and illusion of control on information security. *International Conference on Information Systems*, Omaha, NE.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Ross, C. (2006). Training nurses and technologists for trauma surgery. *Journal of Trauma Nursing, 13*(4), 193-195.

Salas, E., Kosarzycki, M. P., Burke, C. S., Fiore, S. M., & Stone, D. L. (2002). Emerging themes in distance learning research and practice: Some food for thought. *International Journal of Management Reviews, 4*(2), 135-153.

Salkind, N. J. (2011). *Exploring research*. Upper Saddle River, NJ: Prentice Hall

SANS Institute. (2014). Information Security Policy Templates. Retrieved May 22, 2015, from https://www.sans.org/security-resources/policies/

Schigelone, A. S., & Fitzgerald, J. T. (2004). Development and utilization of vignettes in assessing medical students' support of older and younger patients' medical decisions. *Evaluation and the Health Professions, 27*(3), 265-284.

Schoenberg, N. E., & Ravdal, H. (2000). Using vignettes in awareness and attitudinal research. *International Journal of Social Research Methodology, 3*(1), 63-74.

Sekaran, U. (2006). *Research methods for business: A skill building approach*. Hoboken, New Jersey: John Wiley & Sons.

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill building approach*: John Wiley & Sons.

Shank, G. (2006). Six alternatives to mixed methods in qualitative research. *Journal of Qualitative Research in Psychology, 3*(4), 346-356.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *Management Information Systems Quarterly, 34*(3), 487.

Sitzmann, T., & Ely, K. (2010). Sometimes you need a reminder: The effects of prompting self-regulation on regulatory processes, learning, and attrition. *The Journal of Applied Psychology, 95*(1), 132.

Smith, G., Heindel, A., & Torres-Ayala, A. T. (2008). E-learning commodity or community: Disciplinary differences between online courses. *The Internet and Higher Education, 11*(3), 152-159.

Spears, J. L. (2006). The effects of user participation in identifying information security risk in business processes. *Computer Personnel Research Conference*, Pomona, CA.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *Management Information Systems Quarterly, 34*(3), 503-522.

Sprinthall, R. (1997). Basic statistical analysis. Boston, MA: Allyn and Bacon.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Straub, D. W. (1989). Validating instruments in MIS research. *Management Information Systems Quarterly, 13*(2), 147-169.

Straub, D. W., Rai, A., & Klein, R. (2004). Measuring firm performance at the network level: A nomology of the business impact of digital supply networks. *Journal of Management Information Systems, 21*(1), 83-114.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly, 22*(2), 441-470.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *International Conference on Availability, Reliability, and Security*, Krakowska Akademia, Poland.

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

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.

Treisman, A. (1960). Contextual cues in selective listening. *Quarterly Journal of Experimental Psychology, 12*(4), 242-248.

Treisman, A. (1964). Monitoring and storage of irrelevant messages in selective attention. *Journal of Verbal Learning & Verbal Behavior, 3*(6), 449-459.

Trevino, L. K. (1992). Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly, 2*(02), 121-136.

Vance, A., Anderson, B., Kirwan, C., & 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*, 679-722.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(4), 190-198.

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational & End User Computing, 24*(1), 21-41.

Vernadakis, N., Antoniou, P., Giannousi, M., Zetou, E., & Kioumourtzoglou, E. (2011). Comparing hybrid learning with traditional approaches on learning the Microsoft Office Power Point 2003 program in tertiary education. *Computers & Education, 56*(1), 188-199.

Vernon, W. (2009). The Delphi technique: A review. *International Journal of Therapy and Rehabilitation, 16*(2), 69-76.

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.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Von Wright, J. M. (1970). On selection in visual immediate memory. *Journal of Acta Psychologica, 33*, 280-292.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57.

Whitman, M. E., Townsend, A. M., & Alberts, R. J. (2001). Information systems security and the need for policy. *Information Security Management, 24*, 9-18.

Wilks, T. (2004). The use of vignettes in qualitative research into social work values. *Journal of Qualitative Social Work, 3*(1), 78-87.

Winkler, J. D., Kanouse, D. E., & Ware, J. E. (1982). Controlling for acquiescence response set in scale development. *Applied Psychology, 67*(5), 555-583.

Yli-Krekola, A., Särelä, J., & Valpola, H. (2009). Selective attention improves learning. *International Conference on Artificial Neural Networks*, Limassol, Cyprus.