Student Information Security Behaviors and Attitudes at a Private Liberal Arts University in the Southeastern United States

Dissertation

Submitted to Northcentral University

Graduate Faculty of the School of Business and Technology Management
in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

ALAN HUGHES

Prescott Valley, Arizona
July 2016

Approval Page

Student Information Security Behaviors and Attitudes
at a Private Liberal Arts University in the Southeastern United States

By

Alan Hughes

Approved by:

_____ _____

Chair: *Dr. Gregory Caicco, Ph.D.* Date

Certified by:

_____ _____

Dean of School: *Dr. Peter Bemski, Ph.D.* Date

Abstract

Information security is of concern to individuals, businesses, organizations, and education institutions. Information security breaches, whether due to external or internal agents, exact a heavy cost on these entities every year. Much of the cost is due to employees and other insiders who willfully or ignorantly violate information security policies. A difference seems to exist between what students know about information security, and what they actually do. Since college students are the employees of the future, it is important that they be educated and trained in correct information security practices. In order to create effective training material, it is necessary to gain an understanding into what students do, and their attitudes toward information security. Previous studies have produced varying and sometimes conflicting findings with regard to student information security attitudes and behaviors. This non-experimental quantitative study employed a cross-sectional approach, with both comparative and correlation analysis, in an effort to identify the factors related to information security attitudes and behaviors of students at ABC University [actual name redacted], a liberal arts university in the Southeastern United States. Graduate and undergraduate students across all majors were surveyed. Data was collected through an online survey instrument that had been used and validated in previous research. The results from 699 valid responses suggested that neither information security attitudes or behaviors were significantly related to academic major (F (12, 1382) = 1.160, p = .307; Wilks' Λ = 0.980, partial η^2 = .010). However, while information security attitudes were slightly related to previous information security training, information security behaviors were significantly related to prior information security training (F (10, 1384) = 1.160, p < .001;

Wilks' $\Lambda = 0.959$, partial $\eta^2 = .021$). Finally, information security attitudes seemed to have a strong predictive power with regard to information security behaviors, with attitudes accounting for 17% of the variance in behaviors. These results suggest that information security training that influences both attitudes and behaviors should be provided for higher education students. The results of this study should be useful in building university classes and training programs to bridge the gap between students' knowledge and their actual behaviors.

Acknowledgements

My greatest love and deepest appreciation go to my family, and particularly my wife, Elaine, who both encouraged me to begin this adventure, and demonstrated extreme patience during long nights and weekends of researching and writing. I dedicate this dissertation to Elaine, and to my children, in appreciation for their continual encouragement and willingness to allow me the time to make this happen. I am indebted to my mother-in-law, Jerry Smith, and my late father-in-law, Ralph Smith, for their encouragement and prayers from the beginning. I am also indebted to my late parents, Von Ray and Florence Hughes, without whose sacrificial investments in my life, I would not be here.

I would like to thank my dissertation committee chair, Dr. Gregory Caicco, who read countless drafts and revisions of this document. The encouragement and feedback he provided during this process has proven to be indispensable. I would also like to thank Dr. Garrett Smiley and Dr. Nari Jeter, who recognized the need for this research, and kept me on track with the methodology, respectively. Many thanks go to my colleagues, administrators, and others who contributed in various ways, including freeing up my time by rearranging teaching schedules and offering timely and constructive advice and encouragement.

Finally, I would like to humbly thank God for providing everything my family has needed during the past several years of this endeavor. Without His guidance and care, this undertaking could not and would not have been accomplished. It is to Him that I owe everything.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

In 2013, 257 U.S. organizations reported losses averaging $7.6 million annually to cyber-crime (Ponemon, 2014). Also in 2013, the FBI informed over 3,000 diverse organizations, large and small, that their information systems had been attacked (Nakashima, 2014). Many information security breaches are precipitated directly or indirectly by organizations' employees (Chen, Ramamurthy, & Wen, 2012; Vance, Siponen, & Pahnila, 2012). IBM's 2013 Cyber Security Intelligence Index reported organizations in the U.S. experienced over 91 million security events, over 16 thousand security attacks, and 109 security incidents from January 1, 2013, through December 31, 2013 (IBM, 2014). While many organizations have security policies and training programs in place, people are often considered the weakest security link in any security scheme (Mitnick, 2002).

People make mistakes, act out of ignorance, or deliberately commit malicious acts that can put their employers at risk of a security breach (Bulgurcu, Cavusoglu, & Benbasat, 2010). The absence of strict organizational monitoring may facilitate individuals engaging in non-compliant security practices such as surfing questionable websites, opening suspicious email attachments, using weak passwords, or sharing credentials (Vance et al., 2012). At least one study has found that people are not typically motivated to adhere to established organizational security policies or procedures, but seem to act according to habits they have formed over years of computer use (Chen et al., 2012). Habit may be an important factor in an individual's information security behaviors (Vance et al., 2012), and recent research suggests that many

individuals develop bad security practices and habits during their college and university years (Lomo-David, Acilar, Chapman, & Shannon, 2011).

College students regularly use technology, including the Internet, in their academic studies (Stanciu & Tinca, 2014), social lives, and in their places of employment (Wright & Drozdenko, 2013; Yoon et al., 2012). Students also use social media (Hamade, 2013; Noel-Levitz, 2013), and may be indiscreet with sensitive information on such sites (Pinchot & Paullet, 2012). University networks often provide open access to faculty and staff employees, students, and parents, but must also protect the university's information and technology assets from cyber-attacks (Marchany, 2014). The explosion of smartphones and other mobile networkable devices has introduced a new security threat to education institutions, as students are heavy users of mobile technology and frequently connect to campus networks with these unsecure devices (Jones & Heinrichs, 2012).

Each of these activities provides opportunities for information security issues, making the information security practices of students of critical import (Mensch & Wilkie, 2011). Upon graduation, students typically enter the workforce as employees (Abel, Deitz, & Su, 2014; Lomo-David et al., 2011; U.S. Department of Education, 2014). Some researchers have suggested that universities, as the "first line of defense" (Mensch & Wilkie, 2011, p. 109), should educate students about information security threats, risks, and responses (Kim, 2014; Lomo-David et al., 2011).

Background

Education breaches in the U.S. in 2013 resulted in a per capita cost of $294 (Ponemon, 2014), resulting in potential "financial liabilities" for breached institutions

(Custer, 2010). Five of the documented higher education information security breaches in 2014 (PrivacyRights.org, 2014) exposed over half a million records, and an industry white paper reported that 47, 60, and 33 data breaches occurred in 2011, 2012, and 2013, respectively (Grama, 2014). The industry white paper also reported that about 36% of the breaches were attributed to hacking or malware, and almost one-third involved unintended disclosure of confidential information (Grama, 2014). Another study indicated almost 15% of college student respondents had been victims of identity theft (Mensch & Wilkie, 2011).

Many college students' information security practices do not consistently reflect their understanding of risks or their knowledge of available security measures (Slusky & Partow-Navid, 2012). Students may possess or develop bad information security habits such as poor password creation and management, inattention to vulnerabilities, poor email security practices (Mensch & Wilkie, 2011), and disclosure of confidential information on social networking sites (Pinchot & Paullet, 2012). Mobile devices may also be part of the problem as one study found that 83% use a smartphone regularly (Harris, Furnell, & Patten, 2014; Pearson, 2014). Many students ignore the risks associated with smartphones and do not practice good information security on their devices (Jones & Heinrichs, 2012).

Statement of the Problem

University students should be trained in information security practices so they can protect their data and contribute positively to their post-graduation employers by helping ensure information security (Jones & Heinrichs, 2012; Lomo-David et al., 2011). However, the problem is that many students may be lacking comprehensive security

practices, security tools, and proper information security perceptions (Yoon, Hwang &, Kim, 2012) and attitudes (Mensch & Wilkie, 2011; Slusky & Partow-Navid, 2012). The increased student use of mobile devices, combined with students' lax security practices (Slusky & Partow-Navid, 2012) and information security attitudes (Mensch & Wilkie, 2011), seems to make students easy targets for hackers and malware. However, research to date is inconclusive regarding the critical vulnerabilities in their behaviors and technology use (Jones & Heinrichs, 2012; Mensch & Wilkie, 2011; Yoon et al., 2012).

More research was needed on student information security behaviors and influencing factors using larger sample sizes, more diversity, and a greater selection of student majors (Jones & Heinrichs, 2012; Mensch & Wilkie, 2011; Yoon et al., 2012). Existing literature called for studies that analyze the impact of information security training in higher education (Booker, Rebman, & Kitchens, 2009). Calls were also sounded for future research that also included other variables, such as the use of technology tools, password choice, email filters, pop-up blockers (Mensch & Wilkie, 2011), encryption, and anti-virus software (Jones & Heinrichs, 2012).

Purpose of the Study

The purpose of this quantitative correlational and comparative cross-sectional study was to understand the relationship between information security attitudes and practices of higher education students at ABC University, a private liberal arts institution located in the Southeastern United States. Information security attitudes and behaviors were measured with the Student Security Attitudes and Behaviors Survey (Yoon et al., 2012). Information security behaviors included the secure use of passwords, using anti-virus software, and response to phishing emails. Data was collected using an online

survey distributed to 2,445 students with an email link, with a goal of obtaining at least 158 responses to achieve .80 Power using MANOVA F-tests. This was calculated for seven groups, using G*Power, given an effect size of 0.0625, and α error probability of 0.05. This survey employed items previously used by Yoon et al. (2012), which contained demographic and categorical questions as well as 23 items on security behaviors and attitudes. The questionnaire used a 7-point Likert scale for measurement of behaviors and attitudes. Specific behaviors included, but were not limited to, taking deliberate actions to minimize risk of a security breach, following good information security procedures, secure use of smart devices, secure credential management, and use of technology tools such as firewalls, email and browser filters, anti-malware software, and encryption (Mensch & Wilkie, 2011; Yoon et al., 2012). Attitudes included, but were not limited to, perceptions of threats, vulnerabilities, and severity, intentions to actively protect computers and information, perceptions of effectiveness of tools and ability to use security tools, subjective norms, and perception of response costs in implementing information security (Yoon et al., 2012).

Academic major and previous information security training were analyzed to determine whether they predict information security attitudes or behaviors (Knapp & Ferrante, 2012; & Mensch & Wilkie, 2011; Yoon at al., 2012). In addition, information security attitudes were studied to see if they predict behaviors (Mensch & Wilkie, 2011; Yoon et al., 2012). The goal was to conduct further research on a more diverse group of students to help better understand the relationships between these factors and information security attitudes and behaviors (Mensch & Wilkie, 2011; Yoon et al., 2012). The findings of this study provide direction for developing information security training, and

provided information on whether academic major or prior training are predictors of information security attitudes or behaviors. The results also provided data that can be used to construct guidelines for organizations in the development of information security and awareness programs.

Research Questions

The purpose of this quantitative cross-sectional correlational and comparative study was to gather and analyze information security behaviors of students at a liberal arts university in the Southeastern United States. The research questions below offer insight into how the information gathered helped achieve the purpose of the study. The questions are quantitative in nature and were designed to gain critical information from students on their information security behaviors and attitudes.

Q1. Are there differences in students' information security attitudes or behaviors based on academic major?

Q2. Are there differences in students' information security attitudes or behaviors based on hours of information security training?

Q3. Do students' information security attitudes predict their information security behaviors?

Hypotheses

$H1_0$. There are no differences in students' information security attitudes or behaviors based on academic major.

$H1_a$. There are statistically significant differences in students' information security attitudes or behaviors based on academic major.

$H2_0$. There are no differences in students' information security attitudes or behaviors based on hours of information security training.

$H2_a$. There are statistically significant differences in students' information security attitudes or behaviors based on hours of information security training.

$H3_0$. Students' information security attitudes do not predict their information behaviors.

$H3_a$. Students' information security attitudes statistically significantly predict their information behaviors.

Nature of the Study

The research was a quantitative study of the information security behaviors and attitudes of university students. A quantitative approach proved best for this particular study as its goal was to measure actual behaviors and attitudes of university students for statistical analysis. This study sought to determine to what extent students practice certain security behaviors. A qualitative approach might have included observations of and interviews with students, searching for themes concerning information security, and seeking to understand the students' behaviors, which did not fit the purpose of this study. Categorical data items such as major and prior hours of information security training were used to determine whether the significance of their relationships to attitudes and behaviors.

The study included both comparative and correlational components. The comparative component analyzed data to determine whether there were differences in information security attitudes and behaviors between categorical groups. The correlational component analyzed data to determine whether a significant relationship

exists between attitudes and behaviors. The primary variables studied were student information security attitudes and student information security behaviors, as measured by the Student Security Attitudes and Behaviors survey instrument. The relationships between academic major, prior information security training, information security attitudes, and information security behaviors were also analyzed. It is important to note that correlation does not necessarily indicate causation, just that two or more variables are related. Results of correlational studies do provide information for making predictions between the variables. Due to time constraints, an experimental study was not feasible. The study was cross-sectional, as the data was collected at one point in time, rather than over a prolonged time. A longitudinal study might have been useful in determining whether a specific student improved his or her information security behaviors over the course of a university education. However, the goal of this study was to determine where a group of students was at a given point in time so that new information security training could be developed to address items identified by the results of the analysis. Additionally, a longitudinal study was not feasible in a doctoral dissertation situation due to timing, and alignment with course start and end dates.

One obvious threat to validity was the self-reporting nature of the survey. Another threat could be the cross-sectional approach, which assumed that independent and dependent variables were static, while a longitudinal design might have captured changes in behaviors over the duration of the study. However, a cross-sectional study seemed best for this approach, as the goal was to measure student information security behaviors at a point in time. A third threat might have been introduced by collecting survey data from only one institution. Another method of improving validity might have

been to increase the significance level above .05. Enough surveys were received to seek to improve validity by splitting the sample into two groups and comparing and contrasting the resulting analysis on attitudes and behaviors.

Significance of the Study

Mensch and Wilkie (2011) pointed out the gap between students' understanding of information security threats and their actual information security behaviors. More research was needed on student information security behaviors and influencing factors using larger sample sizes, more diversity, and a greater selection of student majors (Jones & Heinrichs, 2012; Mensch & Wilkie, 2011; Yoon et al, 2012). Future research should also include more variables, such as use of technology tools, password choice, email filters, pop-up blockers (Mensch & Wilkie, 2011), encryption, and anti-virus software (Jones & Heinrichs, 2012). Additional research might also include faculty and staff in order to determine their level of security practices and attitudes (Tan & Aguilar, 2012). Further study should also study the reasons students do not secure their computing devices against viruses (Kruck & Teer, 2008). Qualitative studies might reveal more underlying issues in student security behaviors (Mohamed, Karim, & Hussein, 2012). Future research might also study attitudes and behaviors over time, and seek to identify changes that occur and the factors that precipitate those changes (Jones & Heinrichs, 2012). Similar research among large companies might produce more information on corporate employee information security practices (Lomo-David & Shannon, 2009).

The National Institute of Standards and Technology states "The fundamental value of IT security awareness programs is that they set the stage for training by bringing about a change in attitudes which change the organizational culture" (NIST, 1998, p. 15).

Information gathered in this study should prove useful in understanding student security attitudes and behaviors. A primary goal of this study was to provide assistance and information to educators for designing training programs that teach and develop good information security attitudes and behaviors. The results should also help information technology professionals at colleges and universities determine reasonable restrictions that encourage and build good information security habits. Responses to survey questions provided input for targeted training sessions that address those particular areas. The number of students in the population produced a larger sample than was needed, which allowed for validation between randomly selected groups of responses on some tests. Similar results in different groups validated the findings, giving more solid direction on causes of poor student information security behaviors. The findings also helped determine that while information security training is not a predictor of proper security behaviors, it does have a statistically significant relationship. Finally, the results of the study should provide guidance for employers that hire these graduates by informing efforts to build information security awareness and compliance in their organizations.

Definition of Key Terms

Computer Security. Computer security is the set of technologies and procedures that combine to protect information stored on a computer system from attacks of various natures (Yoon & Kim, 2013).

Identity Theft. Identity theft is the use of the identity of another person, living or dead, with or without that person's permission (Council of Australian Governments, 2007).

Information Security Policy. An information security policy (ISP) is set of proscribed procedures and guidelines designed to protect information while individuals/employees access and use that information (Bulgurcu et al., 2010).

Insider. An insider is an employee or other individual who has authorized access to and knowledge of internal information systems of a particular organization (Yaseen & Banda, 2012).

Phishing. Phishing is an attack that employs social engineering and uses fake emails to fool targets into revealing confidential or sensitive information, or to install some form of malicious software on the target's computer (Hong, 2012).

Security Attack. A security attack is an event that analysis proves to be malicious and deliberate, with the goal being theft or destruction of information or information systems (IBM, 2014).

Security Breach. A security breach is a breakdown or defeat of existing security infrastructure allowing an intruder to achieve success (IBM, 2014).

Security Event. A security event is an individual occurrence of some activity on a computer network, system, or device (IBM, 2014).

Security Habit. A security habit is a conditioned information security action developed by repeated practice over time until it becomes automatic (Vance et al., 2012; Yoon, Hwang, & Kim, 2012).

Security Incident. A security incident is an event that requires more study to determine true significance of the event (IBM, 2014).

Summary

United States business and organizations lose millions of dollars annually in over almost 100 million security events and over 16 thousand security attacks (IBM, 2014; Ponemon, 2014). Many of these breaches are caused by employees (Chen et al., 2012; Vance, Siponen, & Pahnila, 2012), who are often referred to as the weakest link in an organization's security infrastructure (Mitnick, 2002). Employees and other insiders make mistakes, sometimes out of ignorance, or may deliberately commit non-compliant acts (Bulgurcu et al., 2010). Many employees act based on habits acquired during years of computer use (Chen at al., 2012; Vance et al., 2012). Many may develop bad information security habits during their college years (Lomo-David et al., 2011). College and university students are heavy users of technology, including the Internet and social media, in several aspects of their lives (Hamade, 2013; Noel-Levitz, 2013; Pinchot & Paullet, 2012; Stanciu & Tinca, 2014; Wright & Drozdenko, 2013; Yoon et al., 2012). Mobile devices have brought new information security challenges to colleges and universities (Jones & Heinrichs, 2012). As higher education graduates are the employees of the future (Abel et al., 2014; Lomo-David et al., 2011; U.S. Department of Education, 2014), universities should take the lead in educating students about information security (Kim, 2014; Lomo-David et al., 2011). However, at present many students to not seem to practice what they already know about information security (Slusky & Partow-Navid, 2012), and may have lax attitudes toward information security (Mensch & Wilkie, 2011; Slusky & Partow-Navid, 2012; Yoon et al., 2012). More research was needed to determine the factors that affect students' information security behaviors and attitudes so

that proper training can be implemented to help prepare them for the workforce (Lomo-David et al., 2011; Mensch & Wilkie, 2011; Yoon et al., 2012).

This correlational and comparative cross-sectional quantitative study sought to identify the security attitudes and behaviors of students at ABC University by analyzing data from students who responded to a survey link distributed via email. An online survey using SurveyMonkey was used to collect data about student security attitudes and practices, including password practices, use of security tools, and handling of sensitive information. The goal of the study was to identify student security practices and attitudes, including the use of technology tools, handling of confidential information, wireless security practices, secure password practices, and perceptions about threats and capabilities. The results of this study should be useful to universities in designing information security training classes and enhancing information technology curricula with the goal of producing students who follow good information security practices.

Chapter 2: Literature Review

The purpose of this correlational and comparative non-experimental cross-sectional quantitative study was to identify and understand key information security behaviors and attitudes of higher education students at ABC University, a private liberal arts institution located in the Southeastern United States. The organization of the literature review begins with a description of the cost of information security breaches in organizations, individual information security behaviors and the theories that attempt to explain those behaviors. Research on institutional security policies, employee security behaviors, and organizational security controls describes the efforts organizations have made to develop policies governing the use of technology and information, employees' tendencies toward non-compliant information security behaviors, and the technological controls implemented to enforce security policies and improve employee compliance. An exploration of higher education information security controls demonstrates the difference between the more controlled business world and the less controlled higher education environment. Recent literature on student behaviors, attitudes, and factors affecting those behaviors and attitudes, gives insight into what students do with regard to information security, and to some degree, why they do what they do.

Documentation

Existing research literature was located via Northcentral University's online library, primarily using EBSCOHost and ProQuest search engines, as they produced the better results. Keyword phrases such as 'student security practices,' 'student security behaviors,' 'corporate security policies,' 'student information security attitudes,' 'higher education information security,' 'student mobile device use,' 'bluetooth security,'

‘mobile device security,’ ‘student smartphone security,’ and ‘student wireless security’ produced useful results. Variations on the above themes filled out the research findings with regard to literature on the discussion topics. Primary research helped form a sufficient starting point, and led to secondary research of appropriate supporting material. Many of the articles discovered by initial searches provided a number of useful references in their respective bibliographies.

Information Security Breach Impact

Many U.S. organizations, including small businesses, experience information security breaches that can result in a loss of money, confidential data, and reputation (Ponemon, 2015; IBM, 2013). A major breach may result in financial and reputational losses (IBM, 2013; Ponemon, 2015). In 2014, the cost of a security breach in the U.S. was $201 per record exposed, and the average data breach cost was $5.85 million in a survey of 257 U.S. companies (Ponemon, 2014). A study by IBM found that a moderate disruption could cost an organization almost $500,000 (IBM, 2013). Small businesses are not immune to cybercrime, with attacks against them increasing 31% in 2012 (Symantec, 2013). A survey of 4,000 Australian businesses, of which 82.3% were small businesses, reported threats such as malicious software, wireless Internet vulnerabilities, compromised websites, phishing and spear phishing, online fraud, denial of service (DoS) attacks, unauthorized access, and cloud computing risks as potential causes of disruptions (Hutchings, 2012, p. 2-4). Neither are education institutions safe from the attacks of cyber criminals or the actions of insiders, but may actually be more likely to experience an information security breach than some other organization types (Garrison & Ncube, 2011).

In 2014, a number of information security breaches occurred, and in just five of those breaches, over half a million records were exposed (PrivacyRights.org, 2014). Over one-third of the 140 reported education breaches between 2011 and 2013 were the result of malware attacks or hacking attacks (Grama, 2014). A similar study found that most education breaches might not be the result of insider actions, but of hackers (Garrison & Ncube, 2011). Nearly another one-third of education institution breaches resulted in unintentional disclosure of confidential information (Grama, 2014). Identity theft also seems to be a problem among students, with almost 15% of surveyed higher education students reporting their identities had been stolen (Mensch & Wilkie, 2011). However, these statistics are from a small sample size, and may not be generalizable. Another study found that students may be somewhat informed in general about identity theft risks, but at the same time may be lacking in specific knowledge, which seems to contribute to their inability to take appropriate identity protection measures (Seda, 2014). This may indicate a need for more specific training to help reduce the risk of identity theft victimization (Seda, 2014).

Many breaches are the result of deliberate or negligent actions on the part of employees (PWC, 2015; Lomo-David et al., 2011), who may have formed their security habits as college students (Lomo-David et al., 2011). The future employees of businesses and other organizations are today's students who may carry their technology practices into their professions (Stanciu & Tinca, 2014). A number of factors may combine to influence student security behaviors (Mensch & Wilkie, 2011; Yoon et al., 2012; Wright & Drozdenko, 2013). Among these factors are students' attitudes toward information security (Mensch & Wilkie, 2011), behavioral intentions and habits (Yoon et al., 2012),

and potential monetary gain (Wright & Drozdenko, 2013). A student's perception of his or her ability to employ a given security mechanism may also be a predictor of student information security behaviors (Yoon et al., 2012).

Individual Security Behaviors and Attitudes

Many organizational information security incidents are due to negligent or malicious information security practices on the part of employees or other insiders (Vance et al., 2012; Ponemon, 2012). Much of the extant literature identifies people as often being the weakest link in information security (Bulgurcu et al., 2010; Chen et al., 2012; Mensch & Wilkie, 2011). In some situations, people may deliberately carry out malicious acts, either directly committing or indirectly facilitating a security breach (D'Arcy, Herath, & Shoss, 2014). In other situations, employees may carry out non-malicious security violations in order to get their jobs done. They may also not perceive the risk to be great enough to go to the trouble to comply with policy (Guo, Yuan, Archer, & Connelly, 2011). For instance, some employees may synchronize their smart devices to make their work lives easier and more "convenient" (p. 35), and may contribute toward greater productivity (Chigona, Robertson, & Mimbi, 2012).

External threats can create security issues for organizations, but many security issues result from insiders' deliberate non-compliant actions or mistakes (Ponemon, 2012). Insiders are not under the same time constraints as external agents, and may cause more damage than their external counterparts cause (Hua & Bapna, 2013). Internal attackers use their knowledge of internal procedures and protections may render standard threat protections ineffective (Hua & Bapna, 2013). Organizations are increasingly taking disciplinary action against employees for breaching existing security policy

(Doherty, Anastasakis, & Fulford, 2011), as non-compliance may create a high level of risk for the organization (Ponemon, 2012). However, the stresses of the security policies themselves can contribute to non-compliance (D'Arcy et al., 2014). Additionally, employees may care more about getting their jobs done than security, and extra effort to comply may influence whether the employee follows or circumvents policy (Guo et al., 2011).

Negligence may also be another factor in non-compliance, as some employees may seek to do their work with as little additional effort as possible, following security policy only when it does not create an additional burden for them (Wall, 2013). In a 2012 study, 39% of responding companies blamed insider negligence for data breaches (Ponemon, 2012). Adding to the insider threat are well-meaning employees who may unwittingly create risk by exposing information, lazy employees who are seeking the easiest way to get by, and overachievers, who put successful task completion ahead of security (Wall, 2013). Public-facing employees may sometimes be deceived into leaking information to social engineers, while other employees may assume a whistleblower mantle and leak information deliberately (Wall, 2013).

In addition to and in contrast with negligence, motives such as financial pressure, greed, and revenge for perceived injustice may prompt deliberate malicious behavior resulting in a security breach (Wright & Drozdenko, 2013). One study found that financial concerns weighed heavily on a person's intent to commit unethical information technology acts (Chatterjee, Sarker, & Valacich, 2015). Another study considered the aspect of injustice and retribution, and suggested that an organization should take into account how the organization's own environment, including interaction with supervisors,

might motivate an individual to deliberately commit an act of computer abuse (Willison & Warkentin, 2013). Individuals may sometimes fail to comply with security policies because they are not motivated to do so, a major factor in non-compliance (Chen et al., 2012). A lack of or reduced consequences for non-compliance may create an atmosphere conducive to lax information security behavior (Chatterjee et al., 2015; Chen et al., 2012). On the other hand, employees may sometimes view information security requirements as an obstruction that they must figure a way around (Ahmad, Maynard, & Park, 2014).

The results of one study indicated that users may make "subjective judgments" (p. 584) depending on their perception of the importance of a given set of data, and the difficulty of complying with requirements (Sun, Ahluwalia, & Koong, 2011). Another study suggested that knowledge of the organization's information policies might not lead to good information security decisions (Parsons, Young, Butavicius, McCormac, Pattinson, & Jerram, 2015). Another article suggested that an individual who encounters a situation in which he or she is tempted to violate information security policy makes such a subjective judgment based on two internal forces and one external force (Qing, Zhengchuan, Dinev, & Hong, 2011). The internal forces are the person's measure of self-control and his or her moral beliefs, while the external force is the person's perception of severity of consequences (Qing et al., 2011). Various emotions may also be a part of an individual's decision to violate information security policy, and the concept was explored in a study on what the authors labelled the "'emote opportunity model of computer abuse" (Baskerville, Park, & Kim, 2014, p. 166).

A perceived lower likelihood of detection may also contribute to a person's

decision to undertake the unethical use of information technology (Chatterjee et al., 2015). In addition, different ethical definitions may apply in different cultures (Fleischmann, Robbins, & Wallace, 2011). A person's view of the ethics of a given action may also vary depending on whether the organization has a policy in place prohibiting the action (Whitman & Zafar, 2014). Employees with strongly held religious beliefs may also strongly object to unethical practices (Mohamed et al., 2012).

Individuals may tend to be more compliant with security policies when they know their activities are being monitored (Chen et al., 2012), and when an atmosphere of expected compliance exists (Cavallari, 2011). A study on positive and negative management examples suggested that management should monitor employees to be sure they are conforming to right information behaviors (Taylor & Robinson, 2014). A contrasting study suggested that "organizations should involve employees in the development and implementation of monitoring schemes so that feedbacks on security policy compliance could help foster a positive security culture" (Chen, Ramamurthy, & Wen, 2015, p. 17). People may also be more compliant with security policy requirements based on peer or role model influence to comply (Ifinedo, 2014).

Individuals may also be more policy-compliant when they perceive that the consequences for non-compliant behavior will be severe, certain, and timely (Chen et al., 2012; Yoon & Kim, 2013). In contrast, one study investigated the influence of factors specific to a company that in turn have an effect on decisions employees make with regard to information security (Parsons et al., 2015). The results seemed to indicate that "organizations with high consequence penalties were more likely to have good organizational information security culture than those with low-consequence penalties"

(Parsons et al., 2015, p. 124). However, even though the results indicated serious penalties for non-compliance may result in a higher knowledge of the organization's "policies and procedures" (p. 124), they also indicated that the knowledge might not have a significant effect on employee information security decision-making (Parsons et al., 2015).

It is important that organizations do not rush to judgment in an instance of non-compliance, but should ensure their security policy is problem-focused, rather than individual-focused (Wall, 2013, p. 121). People may be motivated to take action to avoid threats if they are convinced the threats exist, are likely to occur, and the consequences of non-action will be severe (Liang & Xue, 2010). The perceived severity of consequences may provide the impetus for U.S. users to implement information security threat protection measures (Hovav & D'Arcy, 2012). Indeed, it may be that communications that combine the ideas of protection and punishment could have a positive synergistic effect on employee information security behaviors (Johnston, Warkentin, & Siponen, 2015).

Researchers at the University of Florida found that pharmacy students activated more secure social media settings after an orientation which discussed the potential negative effects of "unprofessional postings" (Williams, Feild, & James, 2011, p. 5). The training addressed the potential impressions of such postings on future faculty and future employer perceptions of potential students and employees, respectively (Williams et al., 2011). In spite of various training and communications about security, employees may sometimes use neutralizing reasons to justify non-compliance (Siponen & Vance, 2010). Neutralizing behaviors include denial of responsibility and injury, claiming the non-

compliant action was necessary, and claiming a higher loyalty was involved (Siponen & Vance, 2010).

Organizational norms, or what an individual believes others may think or expect concerning security policy compliance, do not always positively affect an individual's intention to comply with security policy (Yoon & Kim, 2013). Supporting Yoon's findings, Cox (2012) suggested that subjective norms might have a significant effect on an individual's information security intentions (Cox, 2012). In contrast, another study found that social influence could have slightly more impact than the stronger predictors of self-efficacy and response efficacy on an employee's compliance intentions (Johnston & Warkentin, 2010). The latter study also found that social influence might affect behavioral intent more than an individual's intention to comply (Johnston & Warkentin, 2010). However, Johnson and Warkentin's 2010 study was limited by time constraints, instrument size, and participants, all of which may limit generalizability of the study to universities or other similarly decentralized IT governance environments (Johnston & Warkentin, 2010).

A feeling of moral obligation to comply can have a significant positive effect on compliance with policy, and perceived expectations of organization management may affect an individual's sense of moral obligation significantly (Yoon & Kim, 2013). This could be especially the case with ethical or religious individuals (Mohamed et al., 2012). Mohamed et al. (2012) also suggested that employers consider training to develop "individuals through spiritual and religious values" (p. 338). Agreeing with that premise, one study suggested that consideration of "moral beliefs" should be included in "any IS deterrence model" (D'Arcy & Herath, 2011, p. 654). However, security policies do not

appear to directly create a sense of moral obligation to comply, but may indirectly affect this sense of duty by positively affecting organizational norms (Yoon & Kim, 2013). An organizational culture that expects compliance may positively affect employee attitudes toward compliance (Cavallari, 2011). Programs that help employees see the value of an information security policy to his or her daily work may be helpful in encouraging security policy compliance (AlHogail, 2015). Additionally, altruism may be positively related to ethical computer practices (Chiang & Lee, 2011), as it is positively related to compliant behavior in general (Pugmire, 1978). Researchers in a study of employee computer abuse suggested that "end users are not consistent in their behavioral intentions to comply with recommendations to protect their informational as the degree of relationship between attitudes and behaviors sets" (Johnston & Warkentin, 2010, p. 562). Understanding the interrelationships of these factors should help organizations plot a course of action (Yoon & Kim, 2013) concerning security training. Another study suggested the importance of habit in information security behaviors (Yoon et al., 2012).

Habitual actions or behaviors are those that individuals perform automatically due to frequent repetition (Polites & Karahanna, 2013; Vance et al., 2012). With regard to information security policies and behaviors, habit may be a significant factor in individuals' actions (Vance et al., 2012; Yoon et al., 2012). Aarts and Dijksterhuis (2000) described habits as "goal-directed automatic behaviors" (p. 60), or mental links between goals and actions, paired by repeated performance on a frequent basis. The results of their study supported the link to cognitive processes related to habit, or automatic behavior, rather than defining habit as merely conditioned response to a stimulus (Aarts & Dijksterhuis, 2000). Habit, however, is not to be confused with

reasoned responses, which do require more involvement of the individual's cognitive processes (Ajzen, 1991). It is possible that bad habits can be overcome and reversed by alerting people to their own behavior (Vitak, Crouse, & LaRose, 2011). The alert should be quickly reinforced by emphasizing the damage they are doing to their careers, as well as to the organization (Vitak et al., 2011).

Individuals are often considered the weakest security link in any organization, due to non-compliant behaviors that may be based on a variety of reasons (Mitnick, 2002). Much research is available on employee security behaviors based on the Theory of Planned Behavior, the Theory of Reasoned Action, Behavioral Intention, and others (Yoon et al., 2012). More research should better inform organizations in the value of information security training and determining courses of action to provide improved information security programs (Lomo-David & Shannon, 2009; Okenyi & Owens, 2007).

Organizational Security Actions

Businesses and other organizations often deploy various technologies that combine to protect a network primarily from external threats (Doherty et al., 2011). Employers and other organizations may implement tools such as intrusion detection systems and secure network protocols to prevent attacks (Yoon & Kim, 2013; Herath & Rao, 2009). However, many intrusion detection systems, while potentially assisting in the detection of possible intrusions, require manual intervention and decision-making (Barrios, 2013). Concerning internal threats, if employees discover their employers are monitoring their information technology activities, the result may be reduced morale and self-worth among the employees (Ciocchetti, 2011). In a study of employee computer abuse, the authors pointed out that leaving information security to end users may be a

dangerous course of action (Johnston & Warkentin, 2010). In addition to technical solutions, some organizations put policies and procedures in place in attempts to counter bad information security behavior by employees, and to encourage proper information security practices (Chen et al., 2012). At least one study suggested formulating and adopting acceptable use policies as potentially the best strategy for dealing with users' information security behaviors (Doherty et al., 2011). Organizations may also benefit from balancing their approaches to information security between "technical, management, and human aspects" (Singh, Gupta, & Ojha, 2014, p. 661).

Acceptable use policies set the limits for use of computers and other information technology resources by defining permissible and non-permissible employee actions (Doherty et al., 2011). The presence of a corporate social media policy may be more effective in inhibiting some computer and network use activities than monitoring processes (Trinkle, Crossler, & Warkentin, 2014). Protection of information resources is especially important to organizations driven by knowledge or data acquisition and storage (Doherty et al., 2011). Properly written acceptable use policies should create a user awareness of security threats, as well as acceptable and unacceptable uses of information and information technology (Doherty et al., 2011). Information security policies define management's information security expectations, including the consequences of employee non-compliance (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). This, however, may become more complicated when two or more companies intertwine their networks, creating insiders from outsiders (Franqueira, van Cleeff, van Eck, & Wieringa, 2013). The bring-your-own-device movement may create additional policy needs for organizations, in addition to complexities associated with various legislative and

regulatory requirements (McLellan, Sherer, & Fedeles, 2015).

In a study limited by scope and sample, Knapp and Ferrante (2012) found that organizations might be able to improve their security postures by creating security awareness in employees, and maintaining and enforcing information security policies (Knapp & Ferrante, 2012). In addition, organizations must focus on developing high-quality information security awareness, including the ability to manage and measure an information security program (Hall, Sarkani, & Mazzuchi, 2011). However, concerning enforcement, a different study recommended avoiding a rush to judgment for an employee's first-time offense (Wall, 2013), as some employees may not be aware of all of the various security policies in their organizations (Crossler, Long, Loraas, & Trinkle, 2014). Creating an atmosphere of compliance may also positively affect employee attitudes toward compliance (Cavallari, 2011; Ifinedo, 2014). One author suggested that the rapid rate of movement toward an information-driven culture has created a need for users who know how to interact with information in a secure manner (Astakhova, 2014). Another article focused on morals, values, and habits as potential influencers of security awareness and actions. The authors suggested that organizations "remove obstacles on the path to establishing the new habit" (Pfleeger, Sasse, & Furnham, 2014, p. 504) in order to assist users in creating new habits. Security tools, policies, and procedures can create obstacles for users, and organizations should focus on removing obstacles to form "keystone habits" (Pfleeger et al., 2014, p. 504). This may be accomplished by making employees aware of security breaches to communicate policy and procedure information during a breach or incident (Pfleeger et al., 2014). Information security might also be improved by using fear appeals that impress individuals with a greater appreciation for

the potential damage resulting from a security threat (Boss, Galletta, Benjamin, Moody, & Polak, 2016; Son, 2011). Fear appeals should also convey a sense of vulnerability to individuals in a way that potential perceived benefits of security violations are neutralized (Boss et al., 2016). The goal of fear appeal programs in a larger information security program is to motivate an individual toward protection of assets, and not to reject informational warnings (Boss et al., 2016).

Moody and Siponen (2013) recommended that employers recruit and hire "highly motivated and committed employees in each work role" while at the same time educating employees on the "negative implications of personal use of the Internet for the organization" (Moody & Siponen, 2013, p. 332). Others have suggested that companies should invest more in protection from insider threats than external threats (Hua & Bapna, 2013). Prislan suggested that companies ask users to sign confidentiality agreements that stipulate the threats and risks to their organizations' information assets, and the employees' responsibility to abide by the agreements (Prislan, 2014). To make employees more aware of management expectations regarding information security, organizations often develop and implement information security awareness training programs (Kim, 2014).

Information Security Awareness Training

Information security awareness training informs employees of expectations and security threats, and encourages employees to form good security practices (Olusegun & Ithnin, 2013; Wolf, Haworth, & Pietron, 2011). Employees may not know how they can or should contribute to the organizations information security goals (Singh et al., 2014). Information security awareness training that builds an awareness of threats and avoidance

measures may motivate employees to avoid IT security threats (Liang & Xue, 2010). A later study confirmed this finding, suggesting that Security, Education, and Awareness Training (SETA) programs may be effective in encouraging an information security culture (Chen et al., 2015). In contrast, another study found that countermeasures that addressed rationale may be effective in reducing non-compliant actions seen by employees as means to various ends (Hedström, Karlsson, & Kolkowska, 2013). A study on mobile device security threats suggested that organizations provide required training and find ways to incentivize employees to learn to protect themselves and their assets from information security theft (Tu, Turel, Yuan, & Archer, 2015). This may become more critical as graduating students believe they should be able to use either their own devices or company devices at any time, for any purpose (Cisco, 2011).

In some cases, security practices have improved with intervening security practice reminders over time (Wolf et al., 2011). One study suggested that information technology workers attend periodic training that focused on the organization's specific "threats, vulnerabilities, rules" concerning information security (Prislan, 2014). Delivery methods of information security awareness training include online courses, instructor-led training classes, simulations, games, posters, newsletters, and others (Abawajy, 2014). In one study, about one-third of the participants preferred text-based delivery of training, while over half the participants preferred video training (Abawajy, 2014). Game-based delivery, however, fared very well in the study, producing improvements with each round of testing (Abawajy, 2014). A study on how awareness and communications affect information security suggested that frequent communication about information security might have positive results (Mishra, Caputo, Leone, Kohun, & Draus, 2014). The study

further suggested that "training with work related examples would be useful in understanding the depth and reach of the controls" (Mishra et al., 2014, p. 145).

Education in good information security practices may be necessary to provide the level of information security behavior that is critical to most organizations (Bulgurcu et al., 2010; Yoon et al., 2012). It is also important to know that there seem to be different perspectives in an organization's information security program, and employees may not always have the same perspective as management (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2012). Employees tend to act based on ingrained habits in performing their daily tasks, and these habits are not always compliant with organizational information security policies (Vance et al., 2012). Habits are actions repeated on a continuous basis, and at least one study has stated that security habits strongly affect university students' information security intentions (Yoon et al., 2012).

Habitual actions or behaviors are automatically due to frequent repetition (Vance et al., 2012; Polites & Karahanna, 2013). With regard to information security policies and behaviors, habit may be a significant factor in an individual's actions (Vance et al., 2012; Yoon et al., 2012). In an oft-cited study, Aarts and Dijksterhuis (2000) described habits as "goal-directed automatic behaviors" (p. 60), or mental links between goals and actions, paired by repeated performance on a frequent basis (Aarts & Dijksterhuis, 2000). The results of their study supported the link to cognitive processes related to habit, or automatic behavior, rather than defining habit as mere conditioned response to a stimulus (Aarts & Dijksterhuis, 2000). Habit, however, is not to be confused with reasoned responses, which do require more involvement of the individual's cognitive processes (Ajzen, 1991).

Moral obligation may strongly affect an individual's intentions and attitudes toward computer security policy compliance (Yoon & Kim, 2013). Similarly, another study found that employees may be more compliant with security policies when they believe their compliance positively affects their coworkers (Ifinedo, 2014). However, if an individual is unaware that certain actions, such as sharing a password with another individual, is unethical behavior, they may not consider it wrong (Myrry et al., 2009). This may make information security awareness training more critical in developing right security behaviors among employees (Bulgurcu et al., 2010; Olusegun & Ithnin, 2013; Wolf et al., 2011).

On the other hand, Yoon et al. (2012) suggested that it might be more important to train students in actual information security practices rather than just awareness (Yoon et al., 2012). Another contradicting study suggested that self-control may be more effective in information security behaviors than training, and recommended that employers consider self-control screening to improve their information security postures (Hu, West, & Smarandescu, 2015). A study of deterrence theory in information security suggested that research should consider several moderating variables, including self-control and moral beliefs (D'Arcy & Herath, 2011). Another study suggested found that ethics instruction for university junior and senior students could have a significant positive effect on students' perceptions about ethical security breaches (Morgan & Neal, 2011).

The National Institute for Standards and Technology (2003) states that a goal of security awareness programs is to "change behavior or reinforce good security practices" (NIST, 2003, p. 8). Security awareness training seeks to teach proper skills and change

individual behaviors related to information security (NIST, 2003). Information security awareness training should use appropriate educational methods and focus on activities that help employees respond in a systematic way when working with information (Puhakainen & Siponen, 2010). This recommendation is supported by another study that suggested training in actual information security practices to improve security behaviors (Yoon et al., 2012). In addition, training and communication should be an ongoing part of an organization's normal activities (Puhakainen & Siponen, 2010; Yoon et al., 2012).

A study limited to undergraduate students suggested that negatively framed messages might have a positive behavioral influence on individuals' information security technology adoption (Shropshire, Warkentin, & Johnston, 2010). In fact, perception of risk levels may increase when more than one negative message is processed at one time (Marcelo, Laroche, Odile, & Eggert, 2012). The combination of these factors in a training program is intended to prepare individuals for potential security events so that they respond with the proper actions (Wolf et al., 2011), with the goal of reducing the organization's vulnerability to threats. Further, D'Arcy and Herath (2011), based on their findings in an analysis of the literature, stated "Given the strong theoretical and empirical support for moral beliefs as a moderator in deterrence theory, we consider its inclusion essential in any IS deterrence model" (D'Arcy & Herath, 2011, p. 654). An alternative method of teaching information security involves using "Hackademic Challenges" which require students to learn how to perform various information security attacks, with the goal of clarifying the basic need for information security in all systems (Papanikolaou, Vlachos, Venieris, Ilioudis, Papapanagiotou, & Stasinopoulos, 2013, p. 330). Some researchers have suggested that information security awareness training should be

delivered to university students to educate them on threats, risks, and proper responses (Kim, 2014; Lomo-David et al., 2011), and "build proper security habits" (Yoon et al., 2012, p. 412). According to one article, "Any successful security program requires strong policy, communication to all users, education about potential threats and vulnerabilities, and regular reinforcement of policy to maximize user awareness and compliance" (Chenoweth, Minch, & Tabor, 2010, p. 137).

Some studies point to the importance of information security awareness training for improving security behaviors (Knapp & Ferrante, 2012). Other studies point to training in actual security actions as a way to better practices (Yoon et al., 2012). More research is needed on more diverse samples to help ascertain the effectiveness of information security awareness programs (Knapp & Ferrante, 2012). An important need, and a goal of this study, is to identify the impact of prior information security training on subsequent student information security behaviors.

Education Institution Information Security

Institutions of higher learning, including U.S. institutions, are not immune to information security breaches, with threats growing over the past several years and security incidents creating increased cost (Custer, 2010). This at a time when some researchers have said that information security is more critical than ever (Silic & Back, 2014). In 2010, U.S. educational institutions reported 65 security incidents resulting in 1.6 million exposed records (Collins, Sainato, & Khey, 2011). The probability of unintended information disclosure at an educational institution is 35% (Collins et al., 2011), and the average cost of an education institution data breach is about $210,000 (Custer, 2010). The mobile device phenomenon among students and employees has

increased the risk level in higher education, creating security problems for information technology professionals (Patten & Harris, 2013). Almost 70% of these professionals have reported having no ability to identify the vulnerabilities created by mobile devices (Tenable-Security, 2012). The majority of students may not lock their devices, whether phones or PDAs, either electronically (Jones & Chin, 2015) or physically (Whipple, Allgood, & Larue, 2012). This may be tied to their lack of understanding of specific information security risks (Seda, 2014), or laxness toward information security (Mensch & Wilkie, 2011).

Higher education information security professionals have been deploying technology-based security solutions for many years (Grajek & EDUCAUSE, 2014). Network and security administrators have implemented firewalls, malware detection systems, and intrusion detection/prevention systems to protect their respective institutions' information systems (Grajek et al., 2014). The need to protect confidential student information and comply with existing security regulations, along with the potential for non-compliance penalties, has now focused attention on risk management, including processes and people, the latter being cited often as the weakest link in information security (Bulgurcu et al., 2010; Chen et al., 2012; Mensch & Wilkie, 2011).

Though Grajek et al. (2014) reported risk management as a high priority in higher education, a study published by the SANS Institute reported that only 45% of respondents had implemented formal procedures for assessing risk with respect to critical assets and business impact (Marchany, 2014). Indeed, one study suggested of research institutions suggested that implementation of given security measures was based on governmental or other agencies' regulatory requirements rather than risk analysis results (de Albuquerque

& dos Santos, 2015). This may be of concern, as the Family Educational and Privacy Act (FERPA) addresses student record security and ties federal funding to FERPA compliance (Marchany, 2014; U.S. Department of Education FERPA Web Site, 2015). All of this may be even more complicated for online higher education institutions (Asllani, 2012).

There may be a "high expectation" of privacy students may have concerning information they disclose to faculty (Harris & Dalton, 2014). One study suggested that teachers should make students aware of the reasons they are collecting certain private information, such as pictures, phone numbers, and home addresses, and collect as little private information as possible (Yang & Wang, 2014). University security professionals may also be concerned with Payment Card Industry (PCI) regulations, as payment systems are a critical part of a university's assets (Marchany, 2014). Over 60% of survey respondents identified state legislation on data breach notification as an important concern (Marchany, 2014). The need for openness on university networks is in conflict with the need for securing the data stored on those networks (Marchany, 2014).

Student Security Behaviors and Attitudes

A discrepancy appears to exist between students' security attitudes and their behaviors (Mensch & Wilkie, 2011). Students educated about security risks may not always act in their personal lives on what they have been taught in the classroom, which may be no more effective than what they have learned about security from popular media sources (Rudman, 2014). Some researchers believe people form their information security habits as college and university students as they interact with university networks and information (Lomo-David et al., 2011). Further, some believe that students carry

those habits into the workplace after graduation (Lomo-David et al., 2011). For example, students seem to use weak passwords or share credentials with others (Lomo-David et al., 2011; Teer et al., 2007). Students may carry out their employment responsibilities using the same insecure practices they developed in college, potentially exposing their employing organizations to risk of security breaches (Lomo-David et al., 2011). This may be supported by the findings of a study that compared information security behaviors of information technology (IT) professionals to the behaviors of students. The IT professionals did not report good information security practices, which may suggest that information security practices do not naturally develop with time and experience (Harris et al., 2014). This study only used a small sample of IT professionals, which may be a limiting factor in generalizability of its findings.

Complicating the risk, mobile devices are popular among students, with smartphones being a popular method of accessing campus resources, potentially putting campus networks and information at risk (Jones & Heinrichs, 2012). Students may be unaware of security measures available for their smartphones, and fail to avoid risky Internet security behaviors (Jones & Heinrichs, 2012). One study suggested that if smartphone users were more network literate, they would likely have a higher level of concern about mobile device security and mobile phone viruses in particular (Jang, Chang, & Tsai, 2014). The failure to take proper precautions and avoid risky smartphone or other mobile device actions, if continued in the workplace, may prove to be a problem for future employers (Patten & Harris, 2013; Ruhnka & Loopesko, 2013). In contrast to mobile device behavior, students appear to be more conscientious about portable storage devices, such as flash drives. In fact, students may be more security conscious in this

area than faculty (Knott & Steube, 2012a).

Over 80% of students surveyed by Cisco believe the lines between personal and work-provided devices are disappearing, and believe they should be able to use either at any time, for either purpose (Cisco, 2011). Further, 56% of student respondents stated they would pass up a job offer or violate the policy if a potential employer's policy prohibits social media access (Cisco, 2011). Finally, 64% of surveyed students indicated social media policies were important enough to inquire about, and 24% indicated social media policies would be prominent in a decision to accept or decline a job offer (Cisco, 2011). Indeed, one study demonstrated that firms who allow the use of personal devices might be more desirable to potential employees. The study also suggested that students may "have strong expectations that future employers will permit them to use personal devices on job" (Weeger, Wang, & Gewald, 2015, p. 7).

This bring-your-own-device (BYOD) model is of concern to security administrators (Patten & Harris, 2013), as it can reduce the effectiveness of centralized security controls (Ruhnka & Loopesko, 2013). The ability for these devices to remotely connect to an enterprise's network escalates the risk of data theft and cyber attacks (Garba, Armarego, Murray, & Kenworthy, 2015). This can be troubling for healthcare organizations, as governmental rules and regulations, such as the HIPPA's Privacy Rule and Security Rule, may conflict with the concept of employees using mobile devices to access Electronic Protected Health Information (Terry, 2015). One author recommended that employers require employees to agree to allow "remote erasure" (p. 90) of lost or stolen personal devices used to access company systems (Fisher & Allen, 2015). A U.S. Computer Emergency Readiness Team (CERT) paper, going a step further, recommends

never crossing between work and personal domains with mobile devices or storage (Walters, 2012).

Security credentials. Although criticized much for their lack of true security, passwords are the best-known and most available authentication technique (Reno, 2013). A study at King Saud University Hospital indicated 34% of the nursing staff allowed fellow workers to know their passwords (Albarrak, 2011). An oft-cited study of student security behaviors reported that 53% of the responding students admitted to intentionally sharing their passwords (Teer et al., 2007). A study of students' password security perceptions found that 61% of students may never change their passwords voluntarily, and just over 40% may not change them even if required to do so (Knott & Steube, 2012b). Students may also use the same password on multiple accounts (Helkala & Hoddo Bakas, 2014), including accounts with sensitive information, possibly indicating a lack of understanding of the risks of this practice (Duggan, Johnson, & Grawemeyer, 2012). A Norwegian study found that over 30% of users share their passwords with others (Helkala & Hoddo Bakas, 2014). Students may not believe the risk to their passwords is high enough to worry about password security (Duggan et al., 2012). One study suggested that employers might be able to evaluate a person's password management inclinations by investigating their personal characteristics, personality, and work ethics (Schuessler & Hite, 2014).

Internet use. Students may use the Internet for a number of reasons, including academic study, social networking, chat, downloading digital content, reading news, and email (Stanciu & Tinca, 2014). One of the few studies on U.S. student Internet use found that students surveyed had positive perceptions of social networking sites (Pumper,

Yaeger, & Moreno, 2013). Over 70% of surveyed U.S. students viewed themselves as advanced Internet users, while another 25% viewed themselves as average in Internet capabilities (Stanciu & Tinca, 2014). Fifty-eight percent of students in one study reported having some computer security training (Stanciu & Tinca, 2014). The same study reported that 99% of the respondents used the Internet on a daily basis, with 53% using the Internet for over four hours each day (Stanciu & Tinca, 2014). However, this study also found that students' Internet research skills may be lacking and in need of improvement (Stanciu & Tinca, 2014).

Some students may spend too much time on the Internet, at the expense of other activities (Stanciu & Tinca, 2014). One study on Internet addiction, drug abuse, and suicide proposed the possibility that Internet addiction "significantly predicts the suicide risk of college students," particularly when combined with drug and alcohol abuse (Kurt, 2014, p. 846). However, according to another study, about 95% of students seem to use the Internet without suffering more than limited detrimental effects (Derbyshire et al., 2013). The online nature of the latter survey could constitute a possible limitation of the study since it may have attracted students who spent more time online (Derbyshire et al., 2013). Typical student Internet use consists of academic work and social connections (Stanciu & Tinca, 2014). Such practices carried into the workplace may cause productivity and security concerns for employers (Lomo-David et al., 2011). In addition, vulnerabilities associated with the Internet and its supporting infrastructure may be present well into the future (Gabberty, 2013).

Self-efficacy and personal responsibility may be important factors in Internet use (LaRose, Rifon, & Embody, 2008). When the means for protection create too much

additional work for the user, there may be a gap between intentions and actual behaviors (LaRose et al., 2008; Wall, 2013). Indeed, for those with impulsive behavior problems, introduction to the Internet may increase their tendency toward thoughtless actions while reducing their level of internally controlled actions (Reed, Osborne, Romano, & Truzoli, 2015). However, it appears that students may be taking a more careful approach to Internet use, which could reduce the level of risk for their respective institutions (Case & King, 2014).

Email. Due to the risk posed by hackers, businesses and other organizations often restrict the use of personal email on their networks (Mensch & Wilkie, 2011), but such restrictions can prove detrimental to colleges and universities needing to access and share information freely (Grajek et al., 2014). Hackers have been known to use email phishing techniques to acquire confidential information from unsuspecting users seeking free things (Abraham, Chengalur-Smith, 2010). This could be due to the increased effectiveness of information security technology making it more difficult for hackers to breach security using only technology (Rocha Flores, Svensson, & Ericsson, 2014). A study by Lomo-David and Shannon (2009) indicated that 75% of students in the sample were unfamiliar with scanning email attachments, and 79% were unfamiliar with protecting email attachments with passwords (Lomo-David & Shannon, 2009). Phishing scams are sophisticated and difficult for some people to detect (Brody, Brizzee, & Cano, 2012). Since scanning attachments helps protect a computer from malicious software, failing to use this security mechanism could put users at risk of virus infection (Lomo-David & Shannon, 2009).

Phishing attacks often use email in attempts to gather confidential information

from undiscerning users (Wright, Chakraborty, Basoglu, & Marett, 2010). A qualitative study of student email security found that all of the student participants recognized inconsistencies in test emails (Wright et al., 2010). However, the students had been somewhat selected based on personal characteristics and contextual factors, supporting the idea that experience might improve the ability to detect phishing emails (Wright et al., 2010). Another study's findings suggested that the dangers of email phishing should be communicated on a continual basis (Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012). A more recent study found that fishing attacks decreased from 22 per month to 14 per month from 2008 to 2012, indicating that spam and phishing threats might be decreasing (Case & King, 2013). This study was limited by sample size and distribution, however, and the authors suggested that larger and more diverse samples might improve the accuracy of the results (Case & King, 2013).

Although some students have demonstrated they are knowledgeable regarding phishing emails, the proclivity to share confidential information may be high among students (Pinchot & Paullet, 2012). A study by Lomo-David and Shannon (2009) indicated that 75% of students in the sample were unfamiliar with scanning email attachments, and 79% were unfamiliar with protecting email attachments with passwords (Lomo-David & Shannon, 2009). Since scanning email attachments helps put users at risk of virus infection (Lomo-David & Shannon, 2009). Tools implemented to protect users from phishing attacks have been unsuccessful, and education may be the best way to help users protect themselves from phishing attacks (Purkait, 2012).

Sensitive and confidential information. Universities house sensitive confidential information on their networks, including academic records and medical

information, governed respectively by the Family Education and Privacy Rights Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) (Kiel & Knoblauch, 2010). Many countries have legislative restrictions concerning the handling of sensitive information, and information technology management is often responsible for ensuring compliance with existing regulations (Warkentin, Johnston, & Shropshire, 2011). One recent study indicated that for the right price, students might find it acceptable to disclose their organizations' sensitive information (Wright & Drozdenko, 2013). The exception to this was when the disclosure might result in injury to or death of another person (Wright & Drozdenko, 2013).

Students seem to disclose personal confidential information on social networking sites such as Facebook (Pinchot & Paullet, 2012). Stanciu and Tinca (2014) reported that students might spend about 14 hours a week on social networking sites (Stanciu & Tinca, 2014). In a study limited to 14-19 year old students, researchers suggested that students may also be wrong about who actually has access to their posted information, and unaware of the actual level of access to their information available to a given audience (Moll, Pieschl, & Bromme, 2014). Hackers may be able to glean such easily available information for use in identity theft schemes (Pinchot & Paullet, 2012), and in fact may frequently target social media users (Velmurugan & Mathiyalagan, 2015). As students tend to use social networking sites primarily for communication with personal acquaintances, they may be prone to exposing more information about themselves, making them targets for hackers (Velmurugan & Mathiyalagan, 2015).

Students reported a lack of attention to securing social media profile information, even though they seemed to understand the risks of posting inappropriate information

(Miller, Parsons, and Lifer, 2010). This is in spite of the fact that users may consider the security notices on such sites to be of significant import, and worthy of greater trust (Benson, Saridakis, & Tennakoon, 2015). Social networking sites have an appeal to college students (Hamade, 2013), and Facebook is the most used social networking site (Lenhart, Purcell, Smith, & Zickuhr, 2010), with over 700 million daily active users as of December 2014 (Facebook, 2015). Students may view Facebook as a purely social media and may harbor negative feelings about academic use of Facebook (Gettman & Cortijo, 2015). Facebook is not, however, the only social media presence on the Internet, as many other vehicles exist in the form of Twitter, LinkedIn, blogs, wikis, and others, and the security risks of these are increased when accessed using mobile devices (Wu, 2013).

Mobile devices. Individuals may use mobile devices to access many different services and more data than has been true previously (Harris, et al., 2014). In a study that may have been limited by the majority of respondents being business majors, smartphone ownership among students appears to have increased from about 51% in 2011 to about 51% in 2014 (Jones & Chin, 2015). According to a study by Pew Internet (2015), about 44% of young adults aged 18-29 may have used their smartphones to access educational content. In addition, about 15% of young adults report being very dependent on their smartphones for access to online content. (Pew Internet, 2015). Smartphones and similar networked mobile devices now pose a serious information security threat to college campuses, mostly because students might not give enough attention to security (Jones & Heinrichs, 2012).

Students may use smartphones to download applications from potentially non-

secure websites, conduct financial business, and link to forwarded website addresses (Jones & Heinrichs, 2012). Fifty-nine percent of Jones and Heinrich's respondents reported not using a smartphone password. This finding seems to be supported by another study where about 62% of third-year medical students reported never locking their phones electronically (Whipple et al., 2012). In contrast, another study found that the percentage of students who would download apps from sites whose trustworthiness was unknown decreased from 47% in 2011 to 43% in 2014. However, the "number of students quite comfortable with the idea has actually gone up 5% (from 11% to 16%)" (Jones & Chin, 2015, p. 565).

While students are aware they are at some risk when using a smartphone or other mobile device, they may not understand the true level of threat to their personal information (Jones, Chin, & Aiken, 2014). Unsecured smartphones may leave an opening for hackers to access confidential information (Jones et al., 2014), particularly since a higher percentage of students appear to be using phones for financial transactions (Jones & Chin, 2015). Individuals may also tether their computer to their mobile device (Constantinescu et al., 2013). Mobile social media attacks are becoming a more serious threat to mobile device users, and risks of using mobile devices for social media access are continually changing due to advances made by hackers (Wu, 2013).

As students continue to believe any device should be usable for work or personal reasons, the lines between personal and employer-provided devices may continue to erode (Cisco, 2011). In fact, as early as 2011 about 56% of IT directors felt they were "under pressure" (p. 13-14) to support devices owned and used in the office by employees, pointing to security and lack of control as primary reasons for not doing so

(Khoo Boo, Messmer, Ahn, & Reed, 2011). Employees may like the "productivity and convenience" (p. 36) of being able to use their own devices for work tasks (Kamau, 2013). This could be complicated by the possible existence of "a variety of weaknesses in the security attitudes and behaviors of mobile device users" (Harris et al., 2014, p. 199). One of those attitudes might be reflected in a finding that over 40% of students may not use a simple passcode as a protection mechanism for their smartphones, where they may also store passwords to other applications or websites (Jones & Chin, 2015). Additionally, students and employees may be uninformed about existing bring-your-own-device (BYOD) policies within their organizations (Crossler et al., 2014). In fact, some employers may not have a good understanding of the risks of BYOD to their information assets (Garba et al., 2015).

Wireless network security. Wireless computing technology is a driver of what was first called "ubiquitous computing" by Mark Weiser in 1991, which seeks to make connectivity available in multiple areas of life (Friedewald & Raabe, 2011). The results of one study indicated the need for security training on wireless networks, particularly home networks, in addition to fundamental network security training for all users (Wilkie & Mensch, 2012). The study also found that the decision to change or not change the default administrator password on a home network was a strong indicator of student wireless network behavior (Wilkie & Mensch, 2012). In addition, there may be a significant connection between the use of information security tools and wireless network security behaviors (Wilkie & Mensch, 2012).

Bluetooth wireless technology, used by many students to connect devices and transfer files, could also present opportunities for exposure to security threats. However,

most students may not be properly attentive to those threats and may not take reasonable precautions against them (Tan & Aguilar, 2012). Users who attach to public wireless networks may not secure their devices properly against attack. This is particularly critical if they are using these networks to conduct financial transactions. Further, this could present a danger to an employee's corporate network should the employee's computer become infected while using a public wireless network (Chenoweth et al., 2010).

Use of security tools. There are many security tools available for personal computer and information security. Among these are personal firewalls, Internet filters, pop-up blockers, anti-virus, anti-spyware, and email filters (Mensch & Wilkie, 2011; Yoon et al., 2012). One study suggested that students might employ such tools more if they felt confident in their abilities to do so (Yoon et al., 2012). Another study confirmed previous studies' findings that students are not attentive to information security (Lomo-David et al., 2011). The same study found that the respondents primarily used anti-virus software, simple passwords, email attachment scanning software, and a daily full scan (p. 73), but no sophisticated tools or measures (Lomo-David et al., 2011). The intention to use anti-spyware might be significantly affected by the tool's user-friendliness (Suki, Ramayah, Nee, & Suki, 2014). Raising the knowledge level of individuals concerning the existence of security tools may create a need for such tools (James, Nottingham, & Byung, 2012). Encryption seems to be used on a limited basis, in spite of its ability to provide security for information (James et al., 2012). Individuals may also believe that while the risk of being hacked is high, they are unlikely to be the target of a hacker (James et al., 2012). A person also might not use anti-spyware software even if they fear spyware infection, potentially because they do not know how to use the software tools

(Gurung, Luo, & Liao, 2009).

Perceived severity of a realized threat may be a significant predictor for using anti-spyware software (Gurung et al., 2009). However, Cox (2012) found that perceived threat might not affect intended information security behavior in a significant way (Cox, 2012). On the other hand, cost of anti-spyware software tools may be a predictor of non-use, possibly due to the intangible nature of a spyware threat (Gurung et al., 2009). Response efficacy is also a contributor to use of anti-spyware software tools, combining with self-efficacy and perceived severity to prompt users to adopt the protective technology (Gurung et al., 2009).

Downloading digital content. The advent of MP3 music files and websites that facilitate file sharing contributed to a decline in music CDs since the 1990s. The Digital Millennium Rights Act of 1998 was an attempt to protect against online music piracy. A study on illegal downloading habits of music consumers suggested that over 70% of respondents, who were between 17 and 24 years old, considered illegal downloading "as their main source of obtaining music" (Pikas et al., 2011, p. 148). Only about half of the respondents in the random survey said they purchased music from stores, whether physical or online (Pikas et al., 2011). These findings correspond with the findings of another study that only about 28% of the respondents reported never having used questionable or illegal sources for downloading content (Wang & McClung, 2012, p. 156). In a study focused on different methods of acquiring music found that just over 75% of respondents reported downloading music illegally (Dilmperi, King, & Dennis, 2011).

Agreeing with previously discussed findings, another study conducted to explore

the effectiveness of a message detailing the illegality of digital piracy found that almost 75% of the responding students downloaded music from the Internet. Women may be equally as likely as men to pirate online music, and a lower sense of ethical concern appeared to be a predictor. This seemed to be reflected in the finding that downloaders seemed more likely to steal an actual music CD from a store than non-downloaders (Robertson, McNeill, Green, & Roberts, 2012). A contrasting study, possibly limited by its convenience sample, suggested that respondents would rather download using legal methods, but at a reasonable price (Weijters, Goedertier, & Verstreken, 2014). Wang and McClung (2012) also found that anticipated guilt based on past downloading actions might motivate some previous downloaders to reject the temptation to repeat the illegal action. Students may wrestle with the conflicts between the cost of music and their apparent view that the music industry does not treat artists appropriately (Jambon & Smetana, 2011). However, among illegal downloaders, there appears to be an optimistic outlook on the likelihood of being caught and punished (Nandedkar & Midha, 2011).

Music is not the only digital content that individuals illegally download, as such actions include movie downloading (Jacobs, Heuvelman, Tan, & Peters, 2012). A study of movie downloading suggested that "the current generation does not seem to harbor many moral qualms about downloading movies" (Jacobs et al., 2012, p. 965). At the same time, they do not appear particularly fond of being called a 'movie pirate,' although downloading appeared to be a routine behavior on the part of the respondents (Jacobs et al., 2012). Indeed, when a student faces a situation requiring a decision, there is a good possibility that he or she will make the wrong decision (Hollier, Blankenship, & Jones, 2013). Consumers may have an entitlement mentality concerning Internet content,

expecting it to be free (McCorkle, Reardon, Dalenberg, Pryor, & Wicks, 2012). Concerning software, an Egyptian study suggested that students are not worried about software copyright protection, have no problem with using illegally copied software (Omar & Ahmed, 2012).

To summarize, many students interact with technology on a daily basis, and many of their behaviors may not be secure (Mensch & Wilkie, 2011). Students information security behaviors include, but are not limited to, creating and maintaining passwords, surfing the Internet, sending and receiving email, accessing university network with mobile devices, downloading digital content, accessing confidential information, implementing security tools, and connecting to wireless networks. While some research is available on these behaviors, conflicting findings in several of these areas require more research to try to identify perceptions and attitudes behind specific information security behaviors (Yoon et al., 2012).

Personal Characteristics and Student Information Security

Personal factors such as gender and age may account for some information security attitudes, with males scoring significantly higher than females in one study (Mensch & Wilkie, 2011). Age, on the other hand, may not play a significant role in attitudes or behaviors (Mensch & Wilkie, 2011). Personality traits may actually affect a student's behavioral intentions to practice smartphone security, particularly with respect to planned behavior and technology acceptance (Uffen, Kaemmerer, & Breitner, 2013). Differences may exist among academic majors, with information technology majors scoring highest on information security attitudes, and criminology majors scoring lowest in a prior study (Mensch & Wilkie, 2011). Different levels of security attitudes may exist

between ethnic groups, with Hispanics and Native Americans scoring low, and African-Americans and Other scoring high (Mensch & Wilkie, 2011). Surprisingly, previous victims of identity theft do not seem to differ significantly from non-victims in their information security attitudes (Mensch & Wilkie, 2011).

Perceptions. An individual's perceptions may also affect his or her information security behaviors (Yoon et al., 2012). The more vulnerable or susceptible a person believes he or she is to a given threat, and the greater the perceived severity, the greater may be the threat perception, and the more motivated the person may be to take avoidance actions (Liang & Xue, 2010). A study using electroencephalography compared responses in a risk-taking exercise against self-reported information security risk measures. The results indicated that the EEG measurements are potential predictors of information security behavior both before and after a security incident, while self-reported measures may only be valid predictors after a security incident (Vance, Anderson, Kirwan, & Eargle, 2014). This supports Mensch and Wilkie's findings that previous victims of ID theft were more positively inclined toward information security (Mensch & Wilkie, 2011).

One typical perceived threat is that of hackers stealing students' personal information, with serious negative impact on the victims (Yoon et al., 2012). Students may also perceive the risk of a computer virus attack to be their most likely vulnerability (Szde, 2014). Other perceptions involve an individual's perception of his or her ability to use technology or processes to prevent the materialization of a threat, and the ability of security tools to protect from attack (Yoon et al., 2012). In a study limited to Chinese participants, researchers found that "Knowledge, Impact, Severity and Possibility had a

significant effect on the perceived overall danger of the threats" (Ding-Long, Rau, & Salvendy, 2010, p. 230). A later study by the same authors suggested that it is possible to improve individuals' "perception of threats to information security" by improving their perception of potential severity (Ding-Long, Rau, & Slavendy, 2011, p. 882). A study of four Midwestern companies with security programs in place suggested that information security training programs should employ techniques for changing employees' information security attitudes, beliefs, and perceptions (Yan, Ramamurthy, & Kuang-Wei, 2015). One study suggested that for online consumers, companies should focus more on addressing security concerns than product experience (Marcelo et al., 2012). For the purposes of this study, one perceived threat is that of hackers stealing students' personal information, with serious negative impact on the victims (Yoon et al., 2012). Other perceptions involve an individual's perception of his or her ability to use technology or processes to prevent the materialization of a threat, and the ability of security tools to protect from attack (Yoon et al., 2012). The literature refers to these perceptions with the terms self-efficacy and response efficacy, respectively.

Effectiveness and capabilities. Response efficacy is the belief or perception that a given security response or action will avoid or provide protection from a given security threat (Rogers, 1975), while self-efficacy is an individual's belief that he or she is capable of performing the proper response or action (Bandura, 1986). According to one study, 95% of responding students viewed their computer skills as "better than average" (Slusky & Partow-Navid, 2012, p. 12). In that same study, 60% of the students rated information security awareness training as "significant or high" in importance (Slusky & Partow-Navid, 2012, p. 19). Response efficacy and self-efficacy may have a positive effect on an

individual's intention to adopt given security practices (Johnston & Warkentin, 2010). When students perceive that they can perform actions that will be effective in providing information security, and that the tool they are using will be effective, they may be more likely to apply the necessary effort to perform those actions (Yoon et al., 2012). In agreement with this premise, a study of personality traits and smartphone security indicated that "smartphone users' intentions to use security measures are mainly motivated by their beliefs about the usefulness and whether the use is under their control" (Uffen et al., 2013, p. 208). Another study suggested that online enterprises should provide necessary training so that customers can become more effective and confident while using information technology (Lai, Li, & Hsieh, 2012).

Behavioral intention. Behavioral intention refers to an individual's intention to behave in a certain manner (Ajzen, 1991; Ajzen, 2011; Fishbein & Ajzen, 1975). For this study, the behavior in question is compliance with proper information security practices or established policy. The Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB) suggest that intentions affect actions (Ajzen, 1991; Ajzen, 2011; Fishbein & Ajzen, 1975). Applied to information security, these theories suggest that students' intentions to practice information security may affect their security behaviors positively (Yoon et al., 2012). Another study of over 400 students suggested that attitudes might positively influence students' intention to observe ethical computer practices, and that an elevated view of information security might positively influence attitudes toward ethical computer use (Chiang & Lee, 2011). A contrasting study, however, found that attitudes showed the smallest effect of three variables measured. Resulting scores for subjective norm and perceived behavioral control were stronger than

scores for attitudes. Analysis resulted in regression coefficients of $\beta = 0.366$, $\beta = 0.360$, and $\beta = .197$, respectively (Hu, Dinev, Hart, & Cooke, 2012). Another study suggested that an individual may have intention to practice information security, but also may mediate the intention based on other situational knowledge (Komatsu, Takagi, & Takemura, 2013).

In addition, the possibility of some personal gain may contribute to intentions of unethical use of information technology (Chatterjee et al., 2015). The perceived anonymous nature of information technology may reduce the impact of subjective norms on individuals' unethical IT behaviors (Chatterjee et al., 2015). However, another study found that subjective norms exert a significant positive influence on an individual's behavioral intentions to practice information security (Chiang & Lee, 2011). A study which focused on the extant security research literature suggested that additional research should be conducted to more reliably establish behavioral intent (BI) as a security behavior predictor (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014).

Security habits. Habits are actions that become automatic through repetition (Aarts & Dijksterhuis, 2000; Vance et al., 2012; Polites & Karahanna, 2013). Information security habits are the automatic responses of users to various information security situations, made routine through repetition (Yoon et al., 2012). Some organizations may use intervention methods that make old information system actions more difficult to perform or use, and encourage the use of a new practice or system until it becomes a habit (Polites & Karahanna, 2013). The knowledge or awareness of an information security threat, or pressure from friends or colleagues to practice information security can cause one or more information security responses (Yoon et al., 2012).

Repetition of positive information security responses might help form security habits, which in turn might combine with intention to practice information security, potentially affecting students' security behaviors (Yoon et al., 2012). However, Mensch and Wilkie (2011) found that students' awareness of threats many not necessarily constitute action consistent with that awareness (Mensch & Wilkie, 2011). One study on student use of Internet-based learning management systems (LMS) found that habit appeared to be a significant moderator of the relationship between intention and behavior (Limayem & Cheung, 2011). In this particular case, the authors recommended that educators encourage the early development of a habit of using the LMS (Limayem & Cheung, 2011). Negative habits might also be formed, since the largest predictor of personal use of the Internet at work appears to be a combination of his or her intentions to use the Internet at work for personal reasons, and his or her habits of personal Internet use (Moody & Siponen, 2013).

In summary, a good amount of research literature exists on student information security intentions, attitudes, practices, and habits. However, much of the research to date has typically been on small samples lacking in diversity, and a number of the findings are in conflict. More research on larger, more diverse samples was needed to determine the extent to which awareness, capabilities, intentions, perceived self-efficacy, and habits influence information security behaviors (Yoon et al., 2012).

Higher Education Information Security Training

Information security continues to be a concern for individuals, institutions (White, Hewitt, & Kruck, 2013), and governments (Nakashima, 2013), and the demand for individuals with information security skills is high (Ralevich & Martinovic, 2012).

Organizations need to protect their information assets and infrastructures, and may begin to look more to higher education institutions for graduates with information security skills (Sauls & Gudigantala, 2013). Colleges and universities must protect their own confidential data and infrastructures that house them (Bulgurcu et al., 2010; Chen et al., 2012; Mensch & Wilkie, 2011), and prepare students for futures in various areas of the work force (White et al., 2013). Institutions of higher education provide an "ideal place" to deliver effective information security training to students (Fulton, Lawrence, & Clouse, 2013, p. 78), and help students form good information security practices and habits (Jones & Heinrichs, 2012; Lomo-David et al., 2011; White et al., 2013). In addition, the job market requires an increased number of professionals able to implement and manage organizational information security (Woodward, Imboden, & Martin, 2013). Information security should be considered for inclusion in higher education institutions' core curriculum for business and information systems majors (White et al., 2013). Some researchers have suggested that colleges and universities should teach ethics to information systems students in order to prepare them to be leaders in a world of developing technology (Harris, Lang, Yates, & Kruck, 2011).

Existing literature recommends coverage of a number of areas of information security in a higher education curriculum. Yoon et al. (2012) recommended emphasizing the positive returns of good security behaviors, along with available resources for efficiently carrying out secure behaviors (Yoon et al., 2012). It may also be advantageous to build a curriculum that focuses on information security aspects of a given major, and includes the disadvantages of information security ignorance (Slusky & Partow-Navid, 2012). Internships that introduce students to real-world information

security work may also play a significant role in educating students in the field (Ralevich & Martinovic, 2012). Actual work experiences including "hands-on projects" may indeed predict information security behaviors significantly, emphasizing their importance in an information security curriculum (Meso, Ding, & Xu, 2013). Additional areas that may need addressing in a college level curriculum include password construction, browser privacy settings, threat identification, and phishing filter configuration (Mensch & Wilkie, 2011).

These areas include mobile device security, which should prepare students defend mobile devices against a number of threat sources (Patten & Harris, 2013). Security training should also include "physical security, ethics, social engineering, social media, eCommerce" (Slusky & Partow-Navid, 2012, p. 24). Students might need to know how to recognize security risks, how to mitigate risks, and how to secure a computer and keep it secure (Slusky & Partow-Navid, 2012). Due to the global nature of the Internet, and threats that may originate anywhere, students might benefit from training that includes a "global perspective" (Long & White, 2010).

Summary

Information security is a critical concern of businesses and other organizations because a security breach creates an organizational vulnerability to potential financial and reputational loss. People are often considered the weakest link in organizational security structures, and may act out of negligence or malicious motives such as greed or revenge. Lax attitudes concerning information security may also affect employee security behaviors. Many students may develop bad security practices and habits while in college (Lomo-David et al., 2011), where parameters for technology use must facilitate free flow

of information (Grajek et al., 2014; Reichman et al., 2014). Academic culture might be a significant contributor to the lack of information security protections in U.S. higher education institutions (Kam & Katerattanakul, 2014). IT practitioners in higher education should ensure that information security goals must align with the higher education culture of academic freedom (Kam & Katerattanakul, 2014). However, as educators of current and future employees and "protectors of data and systems" (White et al., 2013, p. 14), colleges and universities may also have an obligation to produce graduates who both understand the issues of information security (White et al., 2013), and who have developed good information security habits (Jones & Heinrichs, 2012; Lomo-David et al., 2011). In order to address effectively students' information security attitudes and practices, it was necessary to discover and study the factors that influence them and identify the best approach for developing positive information security behaviors (Yoon et al., 2012).

Chapter 3: Research Method

University students should be trained in information security practices so they can protect their own data and contribute positively to their post-graduation employers by helping ensure information security (Jones & Heinrichs, 2012; Lomo-David et al., 2011). However, the problem is that many students may be lacking comprehensive security practices, security tools, and proper information security perceptions (Yoon, Hwang &, Kim, 2012) and attitudes (Mensch & Wilkie, 2011; Slusky & Partow-Navid, 2012). The purpose of this cross-sectional quantitative correlational and comparative study was to understand the relationship between information security attitudes and practices of higher education students at ABC University, a private liberal arts institution located in the Southeastern United States.

Q1. Are there differences in students' information security attitudes or behaviors based on academic major?

Q2. Are there differences in students' information security attitudes or behaviors based on hours of information security training?

Q3. Do students' information security attitudes predict their information security behaviors?

Hypotheses

$H1_0$. There are no differences in students' information security attitudes or behaviors based on academic major.

$H1_a$. There are statistically significant differences in students' information security attitudes or behaviors based on academic major.

$H2_0$. There are no differences in students' information security attitudes or behaviors based on hours of information security training.

$H2_a$. There are statistically significant differences in students' information security attitudes or behaviors based on hours of information security training.

$H3_0$. Students' information security attitudes do not predict their information behaviors.

$H3_a$. Students' information security attitudes statistically significantly predict their information behaviors.

The remainder of this chapter will describe the proposed approach to collecting and measuring data in an attempt to prove or disprove the stated hypotheses, and answer the research questions. The chapter will describe the population and desired sample, as well as the assumptions used to calculate the desired sample size. Further, the chapter will outline variables studied, and their respective operational definitions, as well as data collection and analysis methods. Finally, the chapter will conclude with assumptions, limitations, delimitations, and ethical assurances.

Research Methods and Design(s)

The research undertaken was a quantitative study of the information security behaviors and attitudes of university students. A quantitative approach proved best for this particular study, since its predefined goal was to measure actual (self-reported) behaviors and attitudes of university students for statistical analysis (McCusker & Gunaydin, 2015; Neill, 2007). This study sought to determine to what extent students practice certain security behaviors. A qualitative approach might have included observations of and interviews with students, and searched for themes concerning

information security, and sought to understand the students' behaviors. This, however, did not fit the purpose of this study (McCusker & Gunaydin, 2015). ANOVA and regression analysis were used to help discover whether student information security attitudes are related to information security behaviors (Salkind, 2010). MANOVA tests were used to examine the differences in attitudes and behaviors between students in different majors, and students with different amounts of prior information security training (Salkind, 2010). Correlation tests were used to determine whether a relationship existed between major and hours of information security training (Salkind, 2010).

One aspect of the study was correlational in nature, in that it sought to determine the degree of relationship between information security attitudes and behaviors (Salkind, 2010), specifically whether information security attitudes predict information security behaviors. These variables were measured by the Student Security Attitudes and Behaviors survey instrument (Appendix A) which was used by Yoon et al (2012). The study also had a comparative aspect, as it investigated differences between attitudes and behaviors based on academic major, and the differences between attitudes and behaviors based on hours of information security training. It is important to note that correlation does not necessarily indicate causation, just that two or more variables are related (Salkind, 2010). Results of correlational studies provide information for making predictions based on the relationships between variables. Due to time constraints, an experimental study was not feasible. Because the study sought to identify causes of security attitudes or behaviors, nor whether security attitudes cause security behaviors, a causal-comparative study was not appropriate (Salkind, 2010).

The study was cross-sectional, as the data was gathered in a single collection,

rather than over a prolonged time (Salkind, 2010). A longitudinal study might have been useful in determining whether a specific student improved his or her information security behaviors over the course of a university education (Salkind, 2010). However, the goal of this study was to determine where a group of students was at a given point in time so that information security training could be developed to address items identified by the results of the analysis. Additionally, a cross-sectional design was more feasible for this study due to timing and alignment with course start and end dates (Salkind, 2010).

One obvious threat to validity is the self-reporting nature of the survey. Another threat might be the cross-sectional approach, which assumes that independent and dependent variables are static, while a longitudinal design might have captured changes in behaviors over the duration of the study (Salkind, 2010). However, a cross-sectional study seemed best for this approach, as the goal was to measure student information security behaviors at a point in time (Salkind, 2010). A third threat might have been introduced by collecting survey data from only one institution. However, most test results were consistent with previous research. Several tests achieved a significance level of .05, and some achieved a .01 level, improving the validity of the results (Salkind, 2010).

Information gathered in this survey should prove valuable in understanding student security attitudes and behaviors. One goal of this study was to provide assistance and information to educators for designing training programs that teach and develop good information security attitudes and behaviors. It should also help information technology professionals at colleges and universities determine reasonable restrictions that encourage and build good information security habits. Responses to survey questions should

provide input for targeted training sessions that address those particular areas. The number of students in the population produced a larger sample than needed, which allowed for validation between randomly selected groups of responses. Similar results in different groups should validate the findings, giving more solid direction on causes of poor student information security practices.

Population

The study gathered data on security behaviors of U.S. higher education students enrolled at ABC University, a private liberal arts university in the Southeastern United States. Information provided by the ABC University Office of Planning, Research and Assessment (OPRA) shows that ABC University's student body is 5.7% Hispanic, 74.9% White or Caucasian, 1.4% Black or African-American, 2.3% Asian, 0.3% American Indian or Alaskan Native, 0.4% Native Hawaiian or Other Pacific Islander, 2.6% Two or More, 5.8% Non-resident Alien, and 6.6% Unknown. Approximately 43% of undergraduate students are male, while approximately 57% female. The student classification breakdown for the 2014-15 school year as reported by ABC University OPRA is documented in Table 1.

Table 1

ABC student classification statistics

Class	Resident			Distance		
	Full-time	Part-time	Total	Part-time	Total	%
Freshmen (First-year)	604	4	608	0	608	19.6
Freshmen (All other)	152	2	154	45	199	6.4
Sophomores	662	2	664	3	667	21.5
Juniors	566	4	570	1	571	18.4
Seniors	499	9	508	2	510	16.4
Graduate Students	166	31	197	80	277	8.9
Post-graduate	25	6	31	0	31	1
Special Students*	0	181	181	64	245	7.9
Totals	2,674	239	2,913	195	3,108	100

* High school student, audit only, or non-degree seeking faculty/staff member.

Note. ABC University, Office of Planning, Research, and Assessment, 2015.

The author used the survey instrument used by Yoon et al. (2012), which is documented in Appendix A. The author also used a modified version of the demographic questions used by Mensch and Wilkie (2011). Permissions are documented in Appendix B. Self-developed categorical questions were added to expand the number of demographic factors that potentially affect behaviors and attitudes. The generalizability of this study may be limited by the specific attributes of ABC University and its location. However, there is little reason to believe that, with respect to the variables being researched, ABC University student body should be different than other similar U.S. university student bodies. A survey distributed through social media might have

introduced confounding variables such as heavy social media use, potentially leaving out a segment of students who avoid social media. ABC University required using SurveyMonkey for data collection, due to the logistics involved in emailing a link to students. The approximately 2,600-student population provided a sample size of 699 after incomplete and indeterminate responses were eliminated. This is a larger sample size than Yoon's 202-student sample extracted from students in four classes (Yoon et al., 2012). Students not in a degree program and students under 18 years of age were not recruited for the study. Table 2 contains the categorized enrollment for the majors at ABC University. Academic majors were combined into groups of similar majors for analysis.

Table 2

ABC University academic major enrollment

Major	Students enrolled	% of all students
Natural sciences, health, and human services (biology, chemistry, nursing, pre-med, pre-dent, health and fitness sciences, exercise science, sports management, etc.)	543	20.0
Social sciences, English, literature, and languages (history, government, criminal justice, counseling, humanities)	277	10.1
Mathematical and technological sciences (engineering, physics, math, actuarial science, computer science, information technology)	214	7.9
Education (all education majors in all disciplines)	361	13.2
Fine arts and communication (music, drama, film, art, graphic design, interior design, textile design, speech, mass communication, creative or technical writing, journalism)	503	18.4
Business or accounting	436	15.9
Religion (Bible, Christian ministries, missions)	371	13.6
Other (non-degree, undeclared, post-grad special)*	33	1.2

Note. ABC University, Office of Planning, Research, and Assessment, 2015.
* - Non-degree students will not be included in the study

Sample

The sample consists of all properly completed surveys, and a drawing for cash prizes appears to have encouraged participation in the survey (Doerfling, Kopec, Liang, & Esdaile, 2010). This study also achieved more diversity with regard to academic majors than seen in previous studies, as suggested by Yoon, et al. (2012). Surveying the entire student body, rather than a subset of select majors, seems to have increased both the sample size and the diversity of majors. Regression analysis was used to analyze the relationship between information security attitudes and information security behaviors. G*Power calculations, using one predictor in regression (R^2 deviation from zero) F-tests with a .80 Power and medium effect size of .15, suggested a sample size of 55 students (Figure 1). The study actually obtained a sample size of $N = 699$ students. A small effect size would have increased the recommended sample size, thereby increasing the possibility of identifying a non-significant relationship as significant. A large effect size would have suggest a smaller sample size, which would have increased the possibility of missing statistically significant relationships, leaving a medium effect size as the best choice for this study (Salkind, 2010).

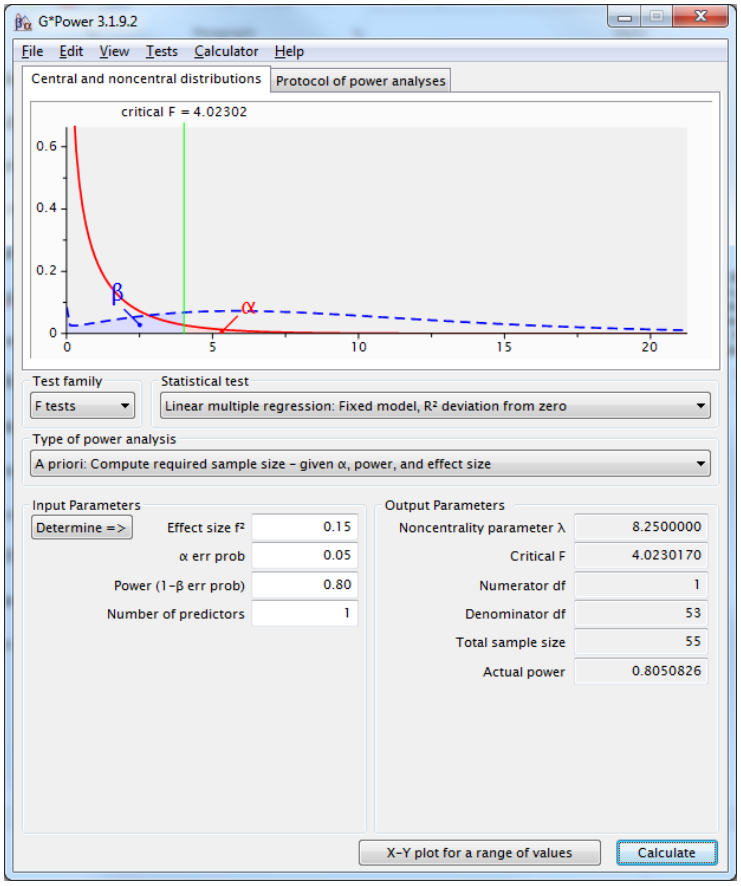

Figure 1. G*Power sample size calculation for RQ 3

MANOVA was used to analyze differences in information security attitudes and behaviors based on academic major and hours of information security training, respectively (Research Questions 1-2). G*Power calculations using MANOVA F-tests, with a .80 Power, a medium effect size of 0.0625, and seven groups, suggested a sample size of 158 students (Figure 2), exceeding the number needed for regression testing for RQ3. A small effect size would have increased the recommended sample size, thereby increasing the possibility of identifying a non-significant relationship as significant. A large effect size would have suggested a smaller sample size, which would have increased the possibility of missing statistically significant relationships, leaving a medium effect size as the best choice for this study (Salkind, 2010).

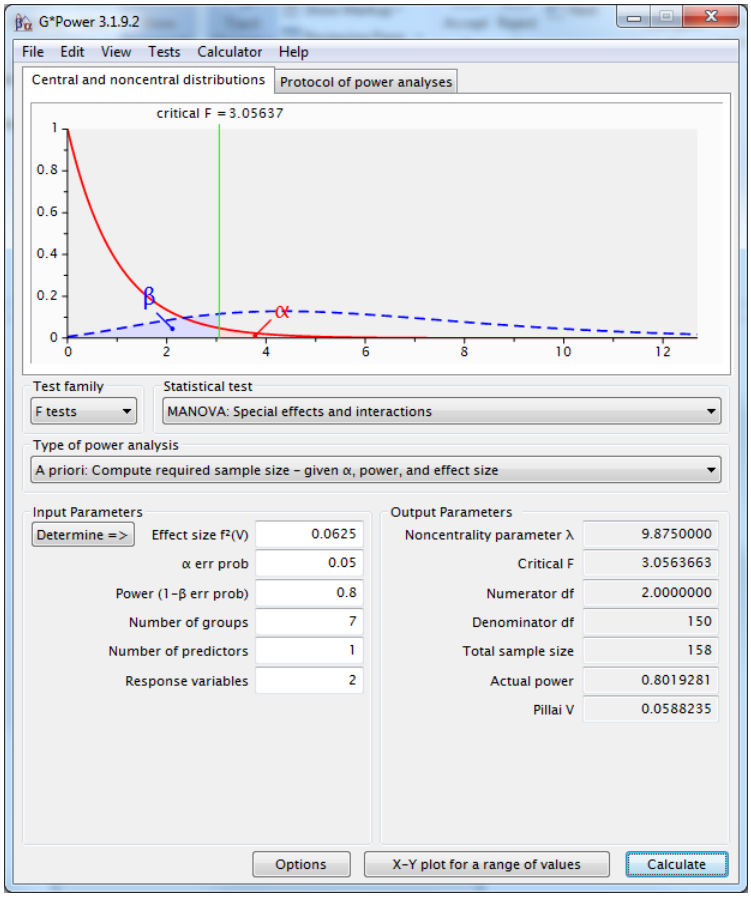

Figure 2. G*Power sample size calculations for RQ1

Data were collected using an online survey questionnaire composed of elements from previous research by Yoon et al. (2011). The survey link was distributed to students through ABC University email. SurveyMonkey was chosen as the data collection tool, aster, as ABC University requires it due to email logistics. The goal was to produce a larger sample size than the minimum calculated by G*Power, which for MANOVA testing with seven groups of majors, as discussed in Research Question 1, was 158 students. Question 2 required a smaller sample as there were less groups of hours of information security training. Question 3 only required 55 students according to G*Power. The final count, after initial response analysis, yielded $N = 699$ properly completed surveys, exceeding the minimum requirements. Due to the size of the sample

obtained, responses were randomly split into two groups for validation analysis for hypothesis H3.

Materials/Instruments

The study used the instrument used in previous research by Yoon et al. (2012). The questionnaire included Likert scales for measuring the items making up the variables in the research design. While Likert scales are ordinal in nature, the use of Likert scales has been debated, and some consider Likert scales as capable of producing interval-like results (Carifio & Perla, 2008). Measurements from studies by Yoon et al. (2012) and Mensch and Wilkie (2011) were used for the security behaviors and attitudes variables. Demographic information was analyzed using descriptive statistics, as was done in the Yoon (2012) and Mensch (2011) studies. MANOVA tests were used to determine whether there were significant differences between the means of different academic majors and hours of information security training variables in relationship to information security behaviors and attitudes. Mensch and Wilkie (2011) found statistically significant differences in security attitudes based on gender, classification, and installation of anti-spyware software. In contrast, the same study found no significant differences based on age, major, ethnicity, identity theft victimization, or installation of anti-virus software (Mensch & Wilkie, 2011). Mensch and Wilkie (2011), however, suggested striving for a larger effect size and testing with larger and more diverse samples.

Security behavior and attitude items from the Yoon et al. (2012) study were measured using a 7-point Likert scale. Available choices were “strongly disagree” (1), “disagree” (2), “somewhat disagree” (3), “neither agree nor disagree” (4), “somewhat agree” (5), “agree” (6), and “strongly agree” (7). An information security behavior

subscale was constructed, consisting of information security behavior items (ISB1, ISB2, ISB3), behavioral intention (BI1, BI2, BI3), and security habits (SB1, SB2). An information security attitude subscale was constructed, consisting of perceived vulnerability (PV1, PV2), perceived severity (PS1, PS2), response efficacy (RE1, RE2, RE3), response costs (RC1, RC2), self-efficacy (SE1, SE2, SE3), and subjective norms (SN1, SN2, SN3).

To verify validity and reliability, Yoon et al. (2012) performed confirmatory factor analysis, which resulted in all t-values being above 1.96, demonstrating convergent validity of measured items. Further analysis resulted in the square root of the average variance extracted (AVE) being less than the square root of the AVE of both constructs (Yoon et al., 2012, p. 411). Average variance extracted (AVE) scores were between .53 and .83, both of which are greater than the commonly accepted .50 level (Fornell and Larcker, 1981). AVE calculations are documented in Table 3. Reliability testing using reliability coefficients exceeded all recommended levels for reliability of the measurement items (Yoon et al., 2012).

Table 3

Average variance extracted and correlation matrix (Yoon et al., 2012)

Average Variance Extracted and Correlation Matrix

Construct	Factor									CCR*	AVE**
	1)	2)	3)	4)	5)	6)	7)	8)	9)		
Information security behaviors	(0.73)									0.77	0.53
Behavioral intention	0.46	(0.81)								0.85	0.66
Perceived vulnerability	0.12	0.18	(0.85)							0.83	0.72
Perceived severity	0.22	0.28	0.36	(0.87)						0.86	0.75
Response efficacy	0.41	0.40	0.15	0.20	(0.91)					0.94	0.83
Response costs	-0.13	-0.15	0.12	-0.02	0.08	(0.90)				0.90	0.82
Self-efficacy	0.10	0.24	-0.11	0.14	0.16	0.01	(0.85)			0.88	0.72
Subjective norm	0.37	0.35	0.15	0.28	0.51	-0.03	0.30	(0.88)		0.92	0.78
Security habits	0.54	0.28	0.15	0.20	0.49	-0.01	0.14	0.60	(0.84)	0.82	0.70

*CCR : Composite Construct Reliability
**AVE: Average Variance Extracted

Yoon et al. (2012) calculated composite coefficients to determine reliability of the constructs, and resulting scores were all between .77 and .94. These scores are higher than the commonly accepted threshold of .70 (Bagozzi & Yi, 2012). Results of Yoon's confirmatory factor analysis are documented in Table 4.

Table 4

Results of confirmatory factor analysis (Yoon et al., 2012)

Results of confirmatory factor analysis

Construct		Construct loading scores									t-value
		1)	2)	3)	4)	5)	6)	7)	8)	9)	
Information security behaviors	ISB1	**0.78**	0.37	0.06	0.13	0.22	-0.08	0.20	0.31	0.43	22.73
	ISB2	**0.77**	0.27	0.19	0.13	0.43	-0.04	-0.02	0.29	0.45	15.16
	ISB3	**0.63**	0.36	0.01	0.24	0.26	-0.17	0.03	0.20	0.27	7.56
Behavioral intention	BI1	0.40	**0.87**	0.09	0.22	0.34	-0.09	0.22	0.37	0.25	35.28
	BI2	0.32	**0.86**	0.15	0.22	0.38	-0.16	0.24	0.33	0.23	41.71
	BI3	0.39	**0.70**	0.20	0.25	0.24	-0.12	0.10	0.14	0.20	12.84
Perceived vulnerability	PV1	-0.01	0.05	**0.69**	0.30	0.03	0.07	-0.07	0.12	0.08	2.68
	PV2	0.14	0.20	**0.98**	0.34	0.17	0.12	-0.11	0.14	0.15	8.13
Perceived severity	PS1	0.00	0.12	0.31	**0.75**	0.02	0.09	0.10	0.09	0.00	6.15
	PS2	0.28	0.31	0.33	**0.97**	0.25	-0.05	0.14	0.31	0.25	53.60
Response efficacy	RE1	0.35	0.38	0.13	0.19	**0.89**	0.03	0.14	0.45	0.39	34.70
	RE2	0.39	0.33	0.12	0.17	**0.92**	0.14	0.12	0.47	0.48	56.82
	RE3	0.39	0.38	0.16	0.19	**0.92**	0.06	0.16	0.48	0.46	59.31
Response costs	RC1	-0.09	-0.13	0.07	0.00	0.08	**0.89**	0.02	0.00	0.00	5.09
	RC2	-0.13	-0.14	0.15	-0.02	0.07	**0.92**	-0.01	-0.05	-0.02	6.64
Self-efficacy	SE1	0.16	0.26	-0.06	0.19	0.20	-0.06	**0.90**	0.26	0.20	25.28
	SE2	0.05	0.17	-0.14	0.11	0.06	0.02	**0.88**	0.30	0.10	22.37
	SE3	0.00	0.13	-0.11	0.02	0.11	0.11	**0.75**	0.21	-0.02	8.97
Subjective norm	SN1	0.32	0.29	0.16	0.29	0.48	-0.02	0.29	**0.87**	0.53	30.46
	SN2	0.36	0.36	0.13	0.24	0.47	-0.04	0.25	**0.94**	0.51	101.60
	SN3	0.28	0.28	0.10	0.21	0.43	-0.02	0.27	**0.84**	0.55	24.21
Security habits	SB1	0.35	0.25	0.10	0.14	0.39	0.04	0.26	0.57	**0.76**	13.96
	SB2	0.53	0.23	0.14	0.19	0.43	-0.05	0.02	0.46	**0.90**	43.76

Standard statistical analysis was used to determine the extent to which students use available information security technology tools to protect their digital devices and data. Standard statistical analysis was also used to determine the extent to which students practice commonly accepted security procedures to protect their digital devices and data. Finally, standard statistical analysis was used to determine students' proclivity to disclose confidential personally identifiable information about themselves and others.

Operational Definition of Variables

The research model for this study focused on two constructs: student information security attitudes and student information security behaviors. Information security behaviors are a dependent variable in this study. The categorical data items of academic major and hours of information security training are independent variables. Information security attitudes may be both dependent (in Research Questions 1 and 2), as well as independent (in Research Question 3) variables. Categorical data collected are described in the demographic and categorical data section. This study, however, focused primarily on two categorical variables: academic major and hours of information security training. In the following discussion, all behavior and attitude variable constructs were measured as interval data, using 7-point Likert-scale responses from the survey, ranging from "strongly disagree" (1) to "strongly agree" (7) (Yoon et al., 2012).

Demographic and categorical data. Demographic and categorical data were collected, including gender, classification, age, academic major, hours of computer usage per day, whether the student has been a victim of identity theft, hours of prior information security training, whether the student uses a PC firewall, and whether the student has participated in illegal downloading of digital content (Mensch & Wilkie, 2011). This

data allowed for comparison within categories. Statistical analysis methods helped determine whether information security behaviors reported in the survey are predicted by demographic data, categorical data or information security attitudes. The instrument used by Yoon et al. (2012) on student security attitudes and behaviors was used to collect data. Demographic items, descriptions, and coding values are listed in Table 3, and were patterned after Mensch's study (Mensch & Wilkie, 2011), with minor additions.

Academic major. The academic major variable is a nominal level of measurement. Coded values were 1 through 7, for health and biological sciences (1), social sciences, language, communications, and humanities (2), mathematical and technological sciences (3), education (4), fine arts and communication (5), business and accounting (6), and Bible, missions, and Christian ministries (7). Data was recorded as reported by the respondent in the demographic portion of the questionnaire. Descriptive statistics and comparative testing were used to analyze relationships between academic major and behaviors, and academic major and attitudes, as well as interactions with other categorical variables. Correlational tests such were used to examine the relationship between academic major and hours of information security training.

Information security training hours. The information security training hours variable is an interval level of measurement. Data was collected in hours, with allowable values of 0 to 999. Collecting actual hours of training allowed for grouping of hours for analysis. Data was grouped and coded for analysis as follows: 0-10 hours (1); 11-20 hours (2); 21-30 hours (3); 31-50 hours (4); and over 50 hours (5). Data was recorded as entered by the respondent in the demographic portion of the questionnaire. Descriptive statistics and comparative testing were used to analyze relationships between information

security training and behaviors and attitudes, as well as interactions with other categorical variables. Correlational tests were used to determine whether there is a significant relationship between academic major and hours of information security training.

Information security attitudes. Information security attitudes include, but are not limited to, avoidance of phishing emails and illegal downloading of videos, music, and software. For the purposes of this study, information security attitudes were calculated using scores from the 23-item Student Security Attitudes and Behaviors survey (Yoon et al., 2012). The survey included questions about use of security tools, secure handling of Internet history, running anti-malware software, response to email and instant messaging links, information backups, password management, use of public computers, email security, and data privacy. For additional analysis, the items were grouped into subscales of information security attitudes and information security behaviors (Mensch & Wilkie, 2011). The items were scored using a 7-point Likert scale, with scores ranging from 1 ("strongly disagree") to 7 ("strongly agree"), providing interval-like data (Carifio & Perla, 2008). The data for these items were collected in the Student Security Attitudes and Behaviors survey (Yoon et al., 2012). An information security attitude subscale was constructed, consisting of perceived vulnerability (PV1, PV2), perceived severity (PS1, PS2), response efficacy (RE1, RE2, RE3), response costs (RC1, RC2), self-efficacy (SE1, SE2, SE3), and subjective norms (SN1, SN2, SN3). Scores were summed and averaged for statistical analysis. Higher scores indicate a higher positive attitude toward information security.

Information security behaviors. Information security behaviors include, but are not limited to, use of security tools email and other communication tool security, Internet

browsing behavior, locking a computer before walking away, performing backups, and using secure social media settings (Mensch & Wilkie, 2011). These and other positive information security practices help to ensure personal computer and information security by protecting access to the student's computing device, as well as access to the student's data through email or browser attacks (Mensch & Wilkie, 2011). The items were scored from 1 ("strongly disagree") to 7 ("strongly agree"), providing interval-like data (Carifio & Perla, 2008). The data was recorded as entered by the respondents in the Student Security Attitudes and Behaviors survey (Yoon et al., 2012). An information security behaviors subscale was constructed, consisting of information security behavior items (ISB1, ISB2, ISB3), behavioral intention (BI1, BI2, BI3), and security habits (SB1, SB2, SB3). Scores were summed and averaged for statistical analysis. Higher scores indicate a higher level of proper information security behavior.

A number of software tools exist that are capable of protecting computing devices and data from a successful attack (Mensch & Wilkie, 2011). The list includes, but is not limited to, personal firewalls, email filters, encryption software, browser filters, pop-up blockers, ad blockers, backup software, and various anti-malware software. Proper configuration and consistent use of such tools may prevent successful attacks on a computing device and the data stored on it (Mensch & Wilkie, 2011). However, students might not feel confident in their ability to use such tools correctly (Claar & Johnson, 2012; Yoon et al., 2012). They may also not feel confident that a given tool will be effective against an attack (Yoon et al., 2012).

Students are heavy users of social media sites (Hamade, 2013; Noel-Levitz, 2013), where they may share confidential information useful to identity thieves (Pinchot

& Paullet, 2012). Students may also connect to their financial institutions using public wireless networks (Mensch & Wilkie, 2011). Hackers have become adept at collecting information on various social media sites and using the connection points to steal an individual's identity (Pinchot & Paullet, 2012). Students should be aware of the public nature of information shared on the Internet, and the threat posed by identity thieves (Mensch & Wilkie, 2011). Students should practice good security on social media sites, as hackers may use these sites in identity theft schemes (Mensch & Wilkie, 2011).

Data Collection, Processing, and Analysis

Demographic and categorical data items were collected using a modified version of Mensch and Wilkie's demographic questions (Mensch & Wilkie, 2011). Attitude and behavior data was collected using the instrument used by Yoon et al. (2012), which consisted of a demographic and categorical data section, and a Likert-scale questionnaire on security attitudes and behaviors. The survey link was distributed to the student body through ABC University email. SurveyMonkey was the data collection tool, as ABC University requires it for facilitating email logistics. The goal was to produce a larger sample size than the Yoon's 202-student sample. The goal was exceeded with 812 total responses, resulting in a sample size of 699. To achieve an effect size of .15 and a Power of .80 for one predictor, a sample of 55 students would have been required for regression testing (Figure 1) for Research Question 3. For Research Questions 1 and 2, MANOVA using a .80 Power, 0.0625 effect size (medium), and $\alpha = .05$, G*Power suggested a sample size of 158. Enough surveys were received to randomly assign them to two data groups for validation analysis.

Data gathered in this study was analyzed and categorized using SPSS Student Version 16 and SPSS Version 22 in order to determine the extent of student information security attitudes and behaviors, as well as the relationship between attitudes and behaviors. Descriptive statistics were used to analyze demographic data. MANOVA was used to analyze academic major, prior information security training, security attitudes, and security behaviors (Research Questions 1 and 2). Regression testing was used to examine the relationship between security attitudes and security behaviors, as described in Research Question 3. The self-developed question concerning hours of prior training yielded useful information on the effect of information security training on information security behaviors, although the training reported may be of different quality with each student, a potential threat to validity. Information on student classification and age was examined to determine whether maturity has any effect on information security behaviors. Regression analysis allows for determining the relationship between variables (Salkind, 2010). Statistics are compiled showing the relationship of each independent variable to the dependent variable, after which regression testing can be used to increase the accuracy and power of predictions about the dependent variable (Salkind, 2010). Regression does assume several things, however, including random independent sampling, linear relationships, normal distribution of the dependent variable at all values of the independent variable, and homoscedasticity (Salkind, 2010). Random independent sampling means that any two respondents provide data that are not related (Salkind, 2010). There is a possibility that two student roommates might have participated in the survey, with one influencing the other with responses. This could pose a threat to validity, but the likelihood of roommates sharing or copying their answers should be

small, as there is no incentive to do so. When the relationships are not linear, the researcher may use nonlinear regression to perform analysis (Salkind, 2010). Multiple regression can also handle situations where the distribution is not normal (Salkind, 2010). Last, homoscedasticity assumes a consistent variance of errors in prediction (Salkind, 2010). A lack of homoscedasticity can call validity into question (Salkind, 2010).

Assumptions

A primary assumption in survey research, including this survey, is that the respondents answer questions honestly and accurately. Demographic questions that included such items as classification, age, gender, hours of information security training, and major should be reliable. For the purposes of this study, the researcher assumed general honesty on the part of the participants. It is possible, however, that some participants may have answered attitude and behavior items on the questionnaire with less than desirable accuracy. The researcher also assumed that a survey distributed to the entire student body, along with the offer of a drawing for cash awards, would produce a higher than normal response rate (Salkind, 2010). A high response rate was achieved, which contributed to the validity of the study. Another assumption was that the validity and reliability testing performed as part of the Yoon study would hold true of the 23-item questionnaire.

Limitations

Quantitative methods have several advantages in research. The researcher may test existing theories against observed or collected data (Morgan, 2015). The goals for data collection are that the data can be observed, can be measured with definite instruments, can be replicated, and are absent bias on the part of the researcher (Botti &

Endacott, 2005). When enough data is collected, the findings may be generalized to a larger population (Kamil, 2004; Wenger, 1999). Data collection time can be reduced by using electronic surveys, and the data may be collected in large volumes (Cope, 2014). Additionally, quantitative research data are normally independent of researcher bias (Neill, 2007). The data are typically numeric in nature, which lends itself to statistical analysis (Neill, 2007). However, the research model used in this study has potential limitations.

Variables or influences on data might remain uncollected or dismissed due to the influence of preconceptions or personal context on the interpretation of findings (Wroughton, McGowan, Weiss, & Cope, 2013). Since there appears to be little reason to believe that students at ABC University are significantly different from students at other schools, the limitation of having used a single site should not prove to be an issue. Another limitation that could have threatened validity was the self-reporting nature of the survey. While the researcher assumed that respondents would answer honestly and accurately, some respondents might have given false answers to some questions (Clayson & Haley, 2011). The cross-sectional nature of the study provided only a snapshot of student behaviors and attitudes, but this appeared to be the best approach for this study, as it emulated the Yoon et al. (2012) study.

In order to mitigate potential limitations and threats to validity, the researcher requested that the ABC OPRA email the survey link to the entire student body. While the student body consists of over 2,600 students, the elimination of under-18 students, and non-degree program students reduced the number invited to 2,445. Although participation was voluntary, a drawing for cash awards was held after the survey was

closed. This resulted in 812 responses, possibly a larger sample size than might otherwise have been obtained (Doerfling et al., 2010; Salkind, 2010). It is possible that there are factors at play in student information security attitudes and behaviors that were not addressed in this study (Yoon et al., 2012). The researcher leaves the study of factors not included here to future research.

Delimitations

This study was delimited to the information security attitudes and behaviors of graduate and undergraduate, degree program students, aged 18 and over, at ABC University, a liberal arts university in the Southeastern United States. While a nationwide survey using social media was considered, since it might have reached more students across a wider geographic area, the idea was rejected due to potential confounding variables with such a study. One major potential confounding variable would have been the likelihood of only reaching students who use social media, or spend a lot of time online otherwise. To help mitigate this, the study was delimited to on-campus students only, and distance-learning only students did not receive the invitation email. The researcher also considered surveying faculty and staff at ABC University, but made the decision to limit the study to graduate and undergraduate students enrolled in a degree program, as they were the focus of the problem statement. Only properly completed surveys were used in data analysis.

Ethical Assurances

Researchers, in particular, must bear the burden of responsibility for ethics violations in their studies (Alsmadi, 2008). A number of professions and professional organizations have codes of conduct to guide the practices and behavior of their

practitioners and members, respectively (reference). The American Psychological Association has a code of conduct that outlines requirements for research and interaction with subjects and patients (APA, 2010). This code also serves as a guide for researchers of human behavior (APA, 2010). The Ethical Principles of Psychologists and Code of Conduct define the guiding principles for psychologists in General Principles A-E (APA, 2010).

Principle A, Beneficence and Nonmaleficence, states that psychologists seek to benefit and not harm those they work with (APA, 2010; Bogolub, 2010). The principle also requires psychologists to guard against allowing personal benefit or other factors to guide their actions (APA, 2010). Principle B states the expectations concerning Fidelity and Responsibility, which includes truth in communications, avoidance or minimization of conflicts of interest, and ethical compliance on the part of themselves and others. Principle C involves the desire to be honest, not cheating, stealing, defrauding, or misrepresenting the truth (APA, 2010). Obligations should be taken seriously, and kept as far as is possible (APA, 2010). Justice is defined in Principle D, which includes equal access to and benefit from the activities in the field of psychology (APA, 2010). Psychologists must avoid and not excuse unjust behavior on their own or others' part (APA, 2010). Finally, Principle E, Respect for People's Rights and Dignity, encompasses respect, privacy, and an individual's right to make his or her own decisions (APA, 2010). It includes the responsibility that psychologists have a responsibility to recognize potential threats to these areas and take measures to protect the rights of individuals, respect differences, and minimize or avoid their own biases (APA, 2010).

In a similar manner, the Belmont Report covers much of the same content in its principles of ethical research (HHS, 1979). The Report documents principles that the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research outlined during its meetings in 1976 (HHS, 1979). The findings include three ethical principles for research using human subjects, as well as the need for informed consent, proper risk/benefit assessments, and ethical participant identification (HHS, 1979).

Beneficence is the first principle, and requires the researcher to do only good to the participant by minimizing potential harm or injury, and maximizing participant benefit (Alsmadi, 2008; HHS, 1979). The second principle in the Belmont Report is Autonomy, which refers to the rights of participants, including the right to be fully informed about potential risks (Alsmadi, 2008; HHS, 1979). Such information allows participants to make their own decisions about participation in a particular study (HHS, 1979). They should also be informed that they will not be penalized for not participating in a study, or quitting a study in progress (HHS, 1979). Finally, the Report outlines the principle of Justice, which insists upon equal treatment among participants (HHS, 1979). To summarize, the subjects have "the right to informed consent; right to privacy and confidentiality; and right not to be deceived or harmed as a result of participation in the research" (Alsmadi, 2008, p. 159).

The author provided an informed consent notice at the beginning of the survey. The notice included text that informed the potential participants of the voluntary nature of the survey, the lack of deception in the survey, and contact names for questions or complaints. The online survey included a clickable radio button to consent or not consent

to take the survey. The informed consent page is in Appendix C. Approvals were sought for permission to conduct the research from both Northcentral University's IRB and ABC University's IRB. Both institutions approved the research. The proposed questionnaire and appropriate forms were completed and submitted to the respective boards for review. No data was collected until both approvals were obtained. The proposed questionnaire, previously used and validated by Yoon et al. (2012), is documented in Appendix A. The demographic and categorical questions, also in Appendix A, are largely adapted from Mensch and Wilkie (2011), with some questions added by the researcher. While an email address was collected by the survey tool for purposes of the drawing to be facilitated by the University's OPRA, the researcher did not receive data with email addresses, thereby protecting the identity of the participants. The researcher will store the data in encrypted form on a flash drive. When data analysis is complete, the encrypted data will be kept in a safe location in the researcher's home until it is destroyed seven years from the close of the survey. Any printed copies will be also stored in the researcher's home and destroyed seven years from the close of the survey.

Summary

Most organizations experience one or more information security breaches annually resulting from security policy violations (Vance, Siponen, & Pahnila, 2012). Many information security breaches occur because employees take actions that put their companies at risk of cybercrime (PWC, 2015) either because they are unwilling to comply with security policies or are unintentional in their actions (Lomo-David et al., 2011). As colleges and universities are producing the employees of the future (Abel et al., 2014; Lomo-David et al., 2011; U.S. Department of Education, 2014), some believe

these institutions have a responsibility to properly prepare students in information security awareness and practices (Booker et al., 2009; Lomo-David et al., 2011). More research is needed to determine factors that influence student security behaviors so that universities can provide necessary information security training and produce more security-aware graduates (Wright & Drozdenko, 2013; Yoon et al., 2012). Such training could save their future employers millions of dollars (Booker et al., 2009). The practical application of this study is to use the findings to provide direction for content recommendations for an information security class for higher education students, and potentially an outline for building an information security culture in an organization.

This cross-sectional correlational and comparative quantitative study sought to identify the security attitudes and behaviors of students at ABC University by analyzing data from students who responded to a survey link distributed via email. An online survey using SurveyMonkey was used to collect data about student security attitudes and practices, including password practices, use of security tools, and handling of sensitive information. The goal of the study was to identify student security practices and attitudes, including the use of technology tools, handling of confidential information, secure password practices, and perceptions about threats and capabilities. The results of this study should be useful to universities in designing information security training classes and enhancing information technology curricula with the goal of producing students who follow good information security practices.

Chapter 4: Findings

The purpose of this cross-sectional quantitative correlational and comparative study was to investigate the information security attitudes and behaviors of higher education students at ABC University, a private liberal arts institution located in the Southeastern United States. The research was designed to specifically determine whether information security attitudes and behaviors are influenced by two independent variables: academic major and hours of information security training. Further, the study sought to determine whether information security attitudes predict information security behaviors.

This chapter will present the results of an email with a survey link that was sent to 2,445 students. Care was taken to ensure the researcher received no identifiable personally identifiable information with the data. Only properly completed surveys were used in the analysis for this study, which is largely based on the analysis in the studies by Mensch and Wilkie (2012), and Yoon et al. (2011). The survey received 812 responses, with 757 of those being completed surveys (according to SurveyMonkey statistics). Further analysis eliminated another 58 responses due to indeterminate or incomplete answers to one or more questions, leaving a sample size of $N = 699$ usable responses. SPSS Student Version 16 and SPSS Version 22 were used to analyze the survey data. Correlational analysis, ANOVA, MANOVA, and linear regression testing were used to analyze the data, in addition to standard descriptive statistics. The results of data analysis were used to answer the study's three research questions.

Results

Descriptive statistics. Analysis using descriptive statistics yielded information on gender as follows: males, 279 (39.9%); females, 420 (60.1%). This approximates the

school's overall reported demographics of 56% female and 44% male (ABC OPRA, 2016). Over 92% of participants were age 18-23. Analysis of ethnicity yielded the following: Caucasian, 600 (85.8%); African-American, 6 (.9%); Asian, 35 (5.0%); Native American, 5 (.7%); Hispanic, 31 (4.4%); Other, 22 (3.1%). Analysis of information specified for the 'Other' ethnicity category allowed for assigning a 'Hispanic' category due to the relatively higher percentage of participants identifying as Hispanic. Classification responses were as follows: Freshman (1), 162 (23.2%); Sophomore (2), 156 (22.3%); Junior (3), 167 (23.9%); Senior (4)166 (23.7%); Graduate student (5), 48 (6.9%). This reflects an almost even distribution among undergraduate students, depicted in the following figure.

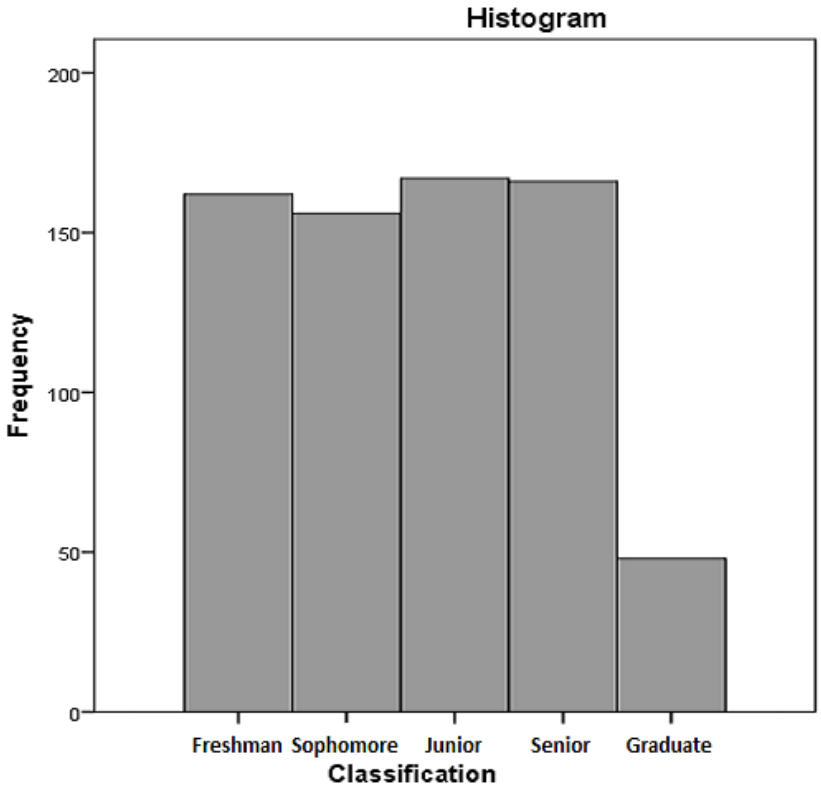

Figure 3. ABC student classification distribution

Daily hours of computer use varied from 0 to 20 hours. While the 20-hour

responses seem high, only three students indicated such a high level of use, so these numbers were not excluded. The mean was 5.73 hours a day, with a standard deviation of 2.900. Using groupings of 0-3, 4-6, 7-10, and 11+ yielded sub-totals of 149 (21.3%), 338 (48.4%), 168 (24.0%), and 44 (6.3%), respectively.

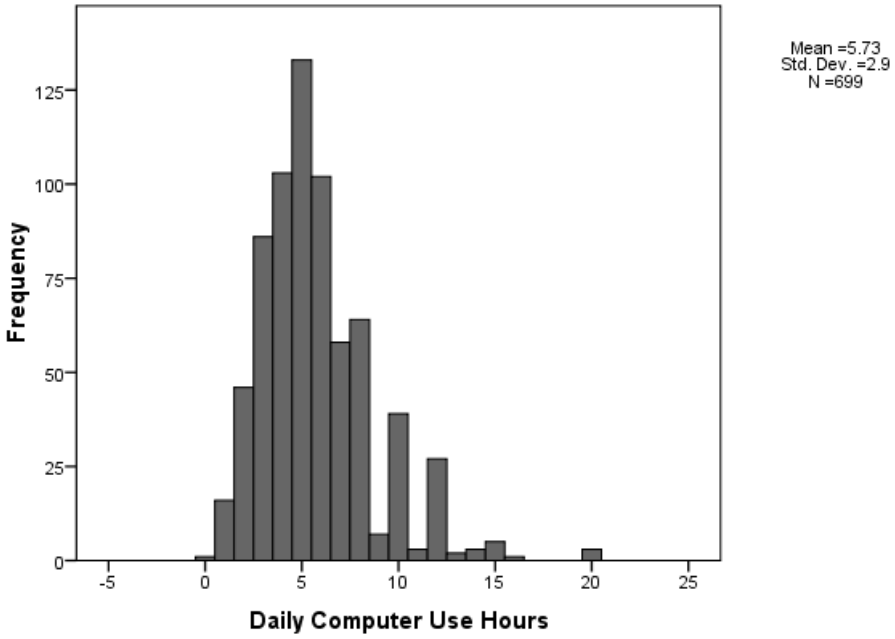

Figure 4. Daily computer use hours distribution

Regarding identity theft victimization, 5.7% of the respondents did not know if they had been victimized. Another 6.2% indicated they had been a victim of identity theft, leaving 616 students who reported they had not been victims of identity theft. Over 57% of the students indicated that they do have a personal firewall installed on their computers. Another 16.5% indicated that they do not have a personal firewall installed, while 32 students (4.6%) indicated their firewall was not activated. The final 152 students (21.7%) indicated that they do not know if a firewall is installed on their computer. On the question of illegal downloading of music or software, 58 students 8.3%) responded affirmatively, while 589 students (84.3%) responded that they do not

participate in this activity. Another 52 students (7.4%) indicated they do not know whether they illegally download music or software.

Table 5

Descriptive statistics of respondents' personal characteristics

Measure	Value (Coding)	Frequency (%)
Gender	Male (1)	420(60.1)
	Female (2)	279(39.9)
Ethnicity	Caucasian (1)	600(91.7)
	African-American (2)	6(.9)
	Asian (3)	35(5.0)
	Native American (4)	5(.7)
	Hispanic (5)	31(4.4)
	Other* (6)	22(3.1)
Age (years)	18-23 years	646(92.4)
	24-30 years	46(6.6)
	31-36 years	3(.4)
	37+ years	4(.6)

* Middle Eastern and multi-racial

Note. Format adapted from Mensch & Wilkie (2011). Information security activities of college students: An exploratory study. *Academy of Information & Management Sciences Journal, 14(2)*, 91-116.

Table 6

Descriptive statistics of respondents' academic characteristics

Measure	Value (Coding)	Frequency (%)
Classification	Freshman (1)	162(23.2)
	Sophomore (2)	156(22.3)
	Junior (3)	167(23.9)
	Senior (4)	166(23.7)
	Graduate Student (5)	48(6.9)
	Other** (6)	Not used for analysis
Major	Natural sciences, health and human services (nursing, pre-med, biology, pre-med, nursing, health sciences, exercise sciences, sports management) (1)	158(22.6)
	Social sciences and languages (history, government, pre-law, criminal justice, counseling, humanities, English, languages, writing) (2)	86(12.3)
	Mathematical and technological sciences (engineering, physics, math, actuarial science, computer engineering, computer science, information technology) (3)	83(11.9)
	Education (all education majors in all disciplines) (4)	79(11.3)
	Fine arts and communication (music, drama, film, art, speech, mass communication, journalism) (5)	125(17.9)
	Business and accounting (6)	82(11.7)
	Bible (Bible, Christian ministries, missions) (7)	86(12.3)

** Added by the author for this study, not used in analysis

Note. Format adapted from Mensch & Wilkie (2011). Information security activities of college students: An exploratory study. *Academy of Information & Management Sciences Journal, 14(2)*, 91-116.

Table 7

Descriptive characteristics of respondents' information security status

Measure	Value (Coding)	Frequency (%)
Hours of computer usage per day	0-3 hours	149(21.3)
	4-6 hours	338(48.4)
	7-10 hours	168(24.0)
	11+ hours	44(6.3)
Hours of prior information security training **	0-5 hours	654(93.6)
	6-10 hours	17(2.4)
	11-20 hours	9(1.3)
	21-30 hours	3(0.4)
	31-50 hours	8(1.1)
	51+ hours	8(1.1)
Victim of identity theft?	Yes (1)	43(6.2)
	No (2)	616(88.1)
	Don't know (3)	40(5.7)
PC personal firewall installed?	Yes (1)	400(57.2)
	No (2)	115(16.5)
	Yes, but not activated (3)	32(4.6)
	Don't know (4)	152(21.7)
Illegal downloading of music, videos or software? **	Yes (1)	58(8.3)
	No (2)	589(84.3)
	Don't know (3)	52(7.4)

** Added by the author for this study

Note. Format adapted from Mensch & Wilkie (2011). Information security activities of college students: An exploratory study. *Academy of Information & Management Sciences Journal, 14(2)*, 91-116.

Composite scores from the security attitudes and behaviors survey ranged from 84 to 161. The mean composite score was 121.08 (SD = 12.366). The majority of the scores were between 100 and 140. The summed scores are depicted in the figure below.

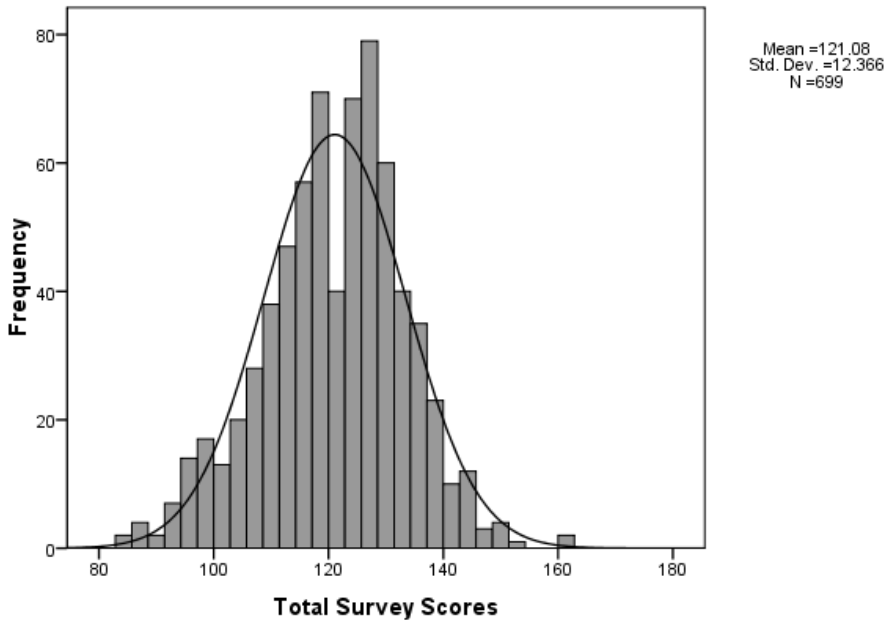

Figure 5. Total survey score distribution – all respondents

In order to provide a measure of validation, both sub-groups' total survey scores were analyzed and produced similar results. Analysis of the first group of $N = 348$ resulted in a mean score of 121.16, only .08 higher than for the entire group. Standard deviation was 12.534, compared to 12.366. The histogram for this test is displayed in the figure below.

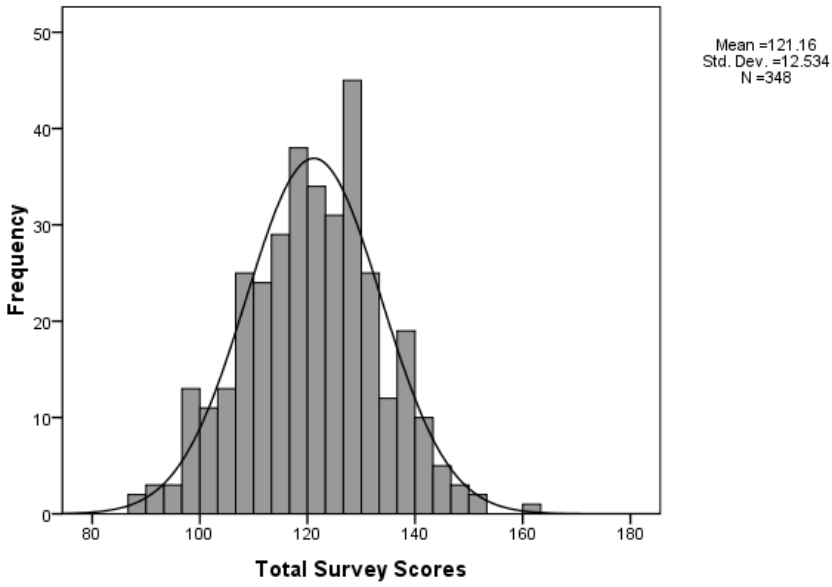

Figure 6. Total survey scores from Group 1

Group 2 analysis for *N* = 351 resulted in a mean score of 121.01, only .07 lower than the entire group's mean score. The standard deviation was 12.214, compared to 12.366. The histogram for this test is in the figure below.

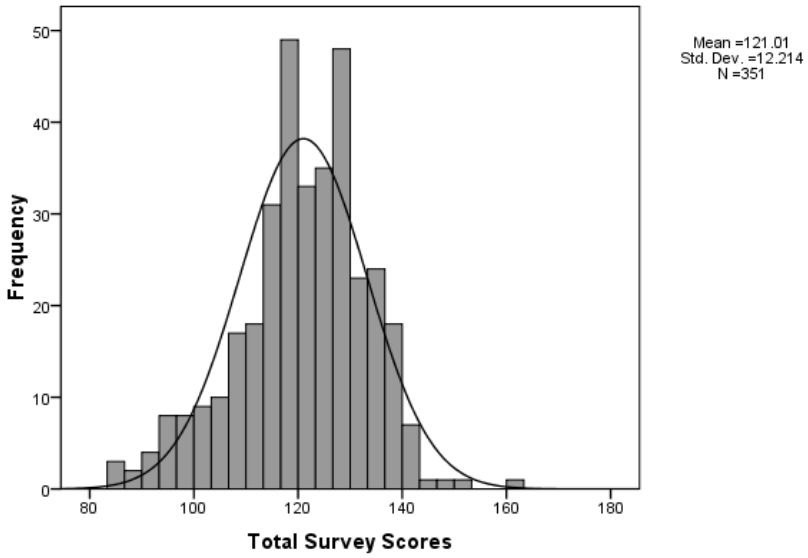

Figure **7.** Total survey scores from Group 2

An information security attitude subscale (SASS) consisted of perceived

vulnerability (PV1, PV2), perceived severity (PS1, PS2), response efficacy (RE1, RE2, RE3), response costs (RC1, RC2), self-efficacy (SE1, SE2, SE3), and subjective norms (SN1, SN2, SN3). Responses were summed and categorized into groups of Very low (51-60), Low (61-70), Medium (71-90), High (91-100), and Very high (100+). Results of descriptive statistics analysis are depicted in the following table.

Table 8

Security attitude subscale grouping

Security attitude subscale ranking	Frequency	%	Cumulative %
Very low (51-60)	18	2.6	2.6
Low (61-70)	91	13.0	15.6
Medium (71-90)	564	80.7	96.3
High (91-100)	24	3.4	99.7
Very high (100+)	2	.3	100.00

An information security behavior subscale was constructed which consisted of information security behavior items (ISB1, ISB2, ISB3), behavioral intention items (BI1, BI2, BI3), and security habits items (SB1, SB2, SB3). Higher scores indicate higher positive information security behaviors. Responses were summed and categorized into groups of Very low (20-29), Low (30-39), Medium (40-49), and high (50+). Higher scores reflect more positive information security behaviors. Results of descriptive statistical analysis for behaviors are depicted in the following table.

Table 9

Security behavior subscale grouping

Security behavior subscale ranking	Frequency	%	Cumulative %
Very low (20-29)	22	3.1	3.1
Low (30-39)	169	24.2	27.3
Medium (40-49)	356	50.9	78.2
High (50+)	152	21.7	99.9 *

*Total does not equal 100.0 due to rounding.

Reliability and Validity

Reliability testing was performed against the 23 survey item scores. SPSS factor analysis produced the total variance explained table below. The Eigen values for the first seven factors were greater than 1.0, and accounted for 63.8% of the variance, with the first factor (ISB1) accounting for 25.071% of the variance. The remaining 16 factors accounted for the remaining 36.2% of the variance.

Table 10

Total variance explained – generated by SPSS

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	5.766	25.071	25.071	5.766	25.071	25.071
2	2.155	9.369	34.440	2.155	9.369	34.440
3	1.669	7.257	41.697	1.669	7.257	41.697
4	1.602	6.963	48.660	1.602	6.963	48.660
5	1.374	5.975	54.635	1.374	5.975	54.635
6	1.090	4.741	59.375	1.090	4.741	59.375
7	1.035	4.500	63.875	1.035	4.500	63.875
8	.975	4.241	68.117			
9	.835	3.633	71.749			
10	.733	3.186	74.935			
11	.703	3.055	77.990			
12	.626	2.722	80.712			
13	.585	2.544	83.256			
14	.523	2.274	85.530			
15	.492	2.141	87.670			
16	.460	1.999	89.669			
17	.440	1.914	91.583			
18	.417	1.814	93.397			
19	.391	1.700	95.097			
20	.373	1.623	96.720			
21	.309	1.345	98.065			
22	.296	1.287	99.352			
23	.149	.648	100.000			

Note: Extraction method: Principal component analysis

Additional reliability testing was performed using Cronbach's Alpha. The results are shown in Table 11 below. The calculated Cronbach's Alpha score was .766, which

indicates an acceptable degree of internal reliability. The Item-Total Statistics table, also shown below in Table 12, shows that all items except PV1, PV2, RC1, and RC2 would result in lower scores (.792, .785, .780, .776, respectively) if removed, so we would not want to remove those items in future studies (Laerd, 2013).

Table 11

Cronbach's Alpha reliability testing of 23-item questionnaire

Reliability Statistics for Full Questionnaire

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.766	.800	23

Table 12

Item-total statistics for 23-item questionnaire

Full 23-item Questionnaire Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
ISB1	116.63	130.568	.428	.390	.749
ISB2	115.41	137.423	.405	.398	.751
ISB3	115.96	136.254	.359	.267	.755
BI1	115.22	139.212	.527	.505	.748
BI2	115.53	135.264	.548	.523	.743
BI3	115.75	139.575	.359	.234	.755
PV1	117.58	156.842	-.161	.342	.792
PV2	117.94	154.462	-.102	.348	.785
PS1	115.50	142.024	.259	.327	.761
PS2	115.05	143.629	.246	.363	.762
RE1	115.35	142.133	.438	.475	.753
RE2	115.09	141.208	.515	.558	.750
RE3	115.26	141.355	.475	.525	.751
RC1	116.03	151.496	-.020	.306	.780
RC2	115.75	149.604	.037	.291	.776
SE1	116.19	137.634	.456	.721	.749
SE2	116.20	137.183	.477	.747	.748
SE3	116.83	134.073	.400	.386	.751
SN1	115.25	141.391	.431	.334	.753
SN2	115.05	142.261	.440	.418	.753
SN3	115.70	139.913	.404	.322	.753
SB1	114.92	142.148	.458	.299	.753
SB2	115.62	136.383	.401	.349	.751

Next, the SASS subscale was tested for reliability using Cronbach’s Alpha (CA). The CA scores and the item-total statistics are displayed in Tables 13 and 14,

respectively. For the attitudes subscale, the CA score was .621, which was lower than the full questionnaire score, and may call the subscale into question. The item-total statistics scores indicated that the CA score would be higher if PV1, PV2, and RC1 items were removed. The higher scores for PV1, PV2, and RC1 would be .667, .647, and .627, respectively. In addition, PV1, PV2, RC1, and RC2 have low corrected item-total scores of -.076, .008, .118, and .160, respectively, so consideration should be given to removing or rewriting those items in future studies (Laerd, 2013).

Table 13

Cronbach's Alpha reliability test for SASS

Reliability Statistics for Security Attitudes Subscale

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.621	.685	15

Table 14

Cronbach's Alpha item-total statistics for SASS

Security Attitudes Subscale Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PV1	73.96	58.312	-.076	.323	.667
PV2	74.32	56.730	.008	.334	.647
PS1	71.88	52.387	.224	.299	.608
PS2	71.43	51.679	.309	.347	.594
RE1	71.73	52.432	.420	.469	.585
RE2	71.47	52.467	.451	.537	.583
RE3	71.65	51.756	.474	.520	.579
RC1	72.41	54.400	.118	.291	.627
RC2	72.13	53.748	.160	.279	.620
SE1	72.57	50.842	.364	.715	.585
SE2	72.58	50.794	.371	.742	.584
SE3	73.21	50.140	.247	.307	.607
SN1	71.63	52.256	.392	.314	.587
SN2	71.43	52.979	.386	.391	.590
SN3	72.08	52.067	.319	.288	.593

Finally, the security behaviors subscale (SBSS) was tested for reliability using Cronbach's Alpha (CA). The CA scores and the item-total statistics are displayed in Table 15 and Table 16, respectively. For the behaviors subscale, the CA score was .767, which is acceptable. This score was higher than the SASS, and slightly higher (.01) than the full 23-item questionnaire. The item-total statistics scores indicated that the CA score would be lower if any of the scores were removed, so none of these items should be removed in future studies (Laerd, 2013).

Table 15

Cronbach's Alpha reliability test for SBSS

Reliability Statistics for Security Behaviors Subscale

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.767	.783	8

Table 16

Cronbach's Alpha item-total statistics for SBSS

Security Behaviors Subscale Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
ISB1	39.17	34.349	.477	.276	.746
ISB2	37.95	37.635	.518	.370	.732
ISB3	38.50	37.004	.442	.239	.748
BI1	37.76	40.133	.581	.478	.731
BI2	38.06	38.035	.582	.485	.724
BI3	38.29	39.699	.418	.210	.750
SB1	37.45	42.933	.412	.197	.754
SB2	38.15	38.302	.429	.319	.749

Factor analysis included the Kaiser-Meyer-Olkin Mesure of Sampling Adequacy, which scored .820, generally considered to indicate a good sample (reference). Bartlett's Test of Sphericity resulted in a significance of $p = .000$, indicating the matrix is not an identity matrix. Results are shown in the following table.

Table 17

Partial results of factor analysis on 23-item questionnaire

KMO and Bartlett's Tests

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.820
Bartlett's Test of Sphericity	Approx. Chi-Square	5501.125
	Df	253
	Sig.	.000

Finally, validity was examined using Pearson correlation testing on the 23 survey items. The results approximated the previous results of reliability and validity testing in the PV1 and PV2 were the only two items not significant at least at the .05 level. PV1 and PV2 scores correlated with total scores at significance levels of .405 and .647, respectively. These two items did demonstrate significance at least at the .05 level for most of the other items, but not all. This confirms the previous results for these two variables, and suggests that they could be eliminated in future studies to improve reliability and validity. At the very least, omitting the items in future studies would not be likely to harm validity or reliability.

Research questions and hypotheses. Three research questions were developed and provided direction for this study. The research questions addressed the nature of relationships between academic major, hours of information security training, information security attitudes, and information security behaviors. The results presented in this chapter provide descriptive statistics, answers for the research questions, and guidance on acceptance or rejection of the hypotheses developed for each question.

Q1. Are there differences in students' information security attitudes or behaviors based on academic major?

Q2. Are there differences in students' information security attitudes or behaviors based on hours of information security training?

Q3. Do students' information security attitudes predict their information security behaviors?

Research Question 1: Are there differences in students' information security attitudes or behaviors based on academic major? This question addressed the relationship between academic major and information security attitudes and behaviors. Participants were well distributed across academic majors. Hypothesis 1 proposed that there are differences in students' information security attitudes and behaviors based on academic major. The largest group was the natural sciences majors (1), with 158 respondents (22.6%). Next was the fine arts group (5), with 125 respondents (17.9%). Others were as follows: Bible (7) and social sciences (2) tied at 86 each (12.3%); mathematical sciences (3), 83 (11.9%); business (6), 82 (11.7%); education (4), 79 (11.3%). These percentages are somewhat aligned with the academic major enrollment reported by the ABC OPRA, with the exception of the mathematical and technological sciences category, which had a participation rate higher than enrollment percentages in those majors. Descriptive statistics are depicted in the following table.

Table 18

Descriptive statistics for academic major

Major	Frequency	%	Valid %	Cumulative %
Bible, ministry, missions	86	12.3	12.3	12.3
Business	82	11.7	11.7	24.0
Education	79	11.3	11.3	35.3
Fine arts and communication	125	17.9	17.9	53.2
Mathematical, technological sciences	83	11.9	11.9	65.1
Natural and health sciences	158	22.6	22.6	87.7
Social sciences and languages	86	12.3	12.3	100.0
Total	699	100.0	100.0	

MANOVA was used for multivariate data analysis. MANOVA assumes that the dependent variables are continuous, the independent variable consists of more than one group, no participants are in more than one group, the sample size is adequate, no significant outliers, a normal distribution exists, there is a sameness of variance, a linear relationship exists, and the dependent variables are somewhat correlated with each other (Salkind, 2010). Concerning the data in this test, security attitude and behavior scores were continuous, there were seven groups of majors, no student was a member of more than one group, the sample size was $N = 699$ (greater than the 158 required by G*Power for seven groups), there was a normal distribution of scores (Figures 8 and 9), there was a linear relationship between information security attitudes and behaviors, and the two were highly correlated with each other.

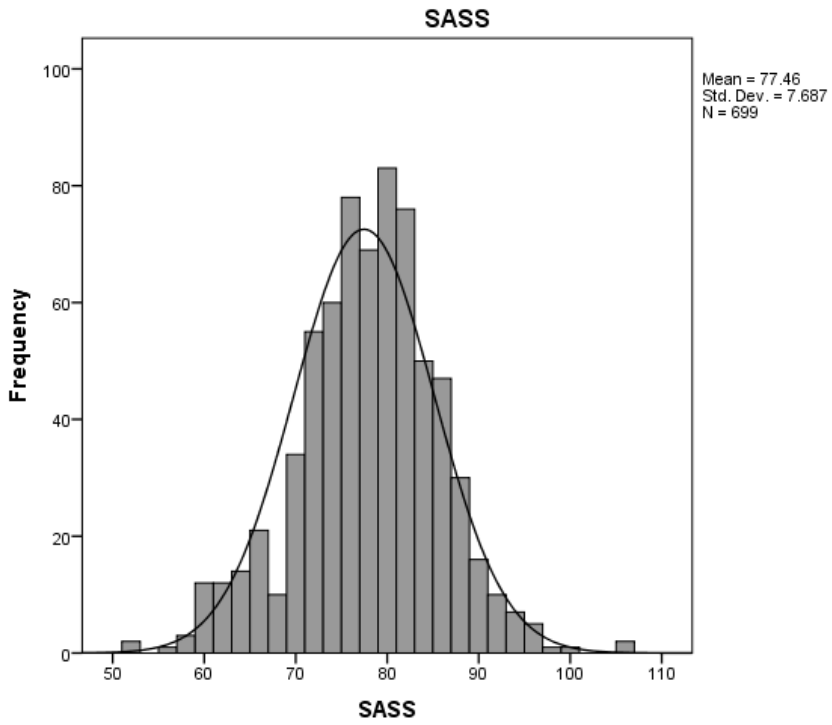

Figure 8. Student information security attitudes scores

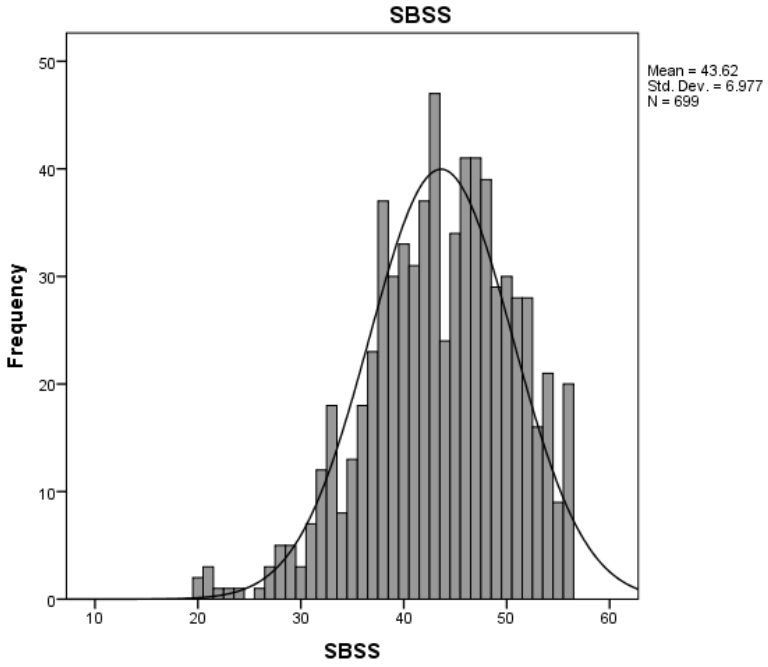

Figure 9. Student information security behaviors scores

Analysis using Pearson correlation tests identified a significant positive

correlation between information security attitudes and information security behaviors (*R* = .421, *p* = .000, α = .01, two-tailed). This tests confirmed that the data met this assumption requirements for MANOVA analysis. The results are depicted in the table below.

Table 19

SBSS-SASS Correlation analysis results

		SASS	SBSS
SASS	Pearson Correlation	1	.421**
	Sig. (2-tailed)		.000
	Sum of Squares and Cross-products	41243.820	15756.296
	Covariance	59.089	22.573
	N	699	699
SBSS	Pearson Correlation	.421**	1
	Sig. (2-tailed)	.000	
	Sum of Squares and Cross-products	15756.296	33976.775
	Covariance	22.573	48.677
	N	699	699

**. Correlation is significant at the 0.01 level (2-tailed).

To confirm these results, regression testing was performed on the security attitudes and security behaviors subscales (SASS, SBSS). Results produced the following histogram and p-plot. The first figure demonstrates the regression distribution, while the second figure shows the linear relationship between SASS and SBSS. As information security attitude scores increase, information security behaviors also increase, and vice versa, as depicted in the figures below.

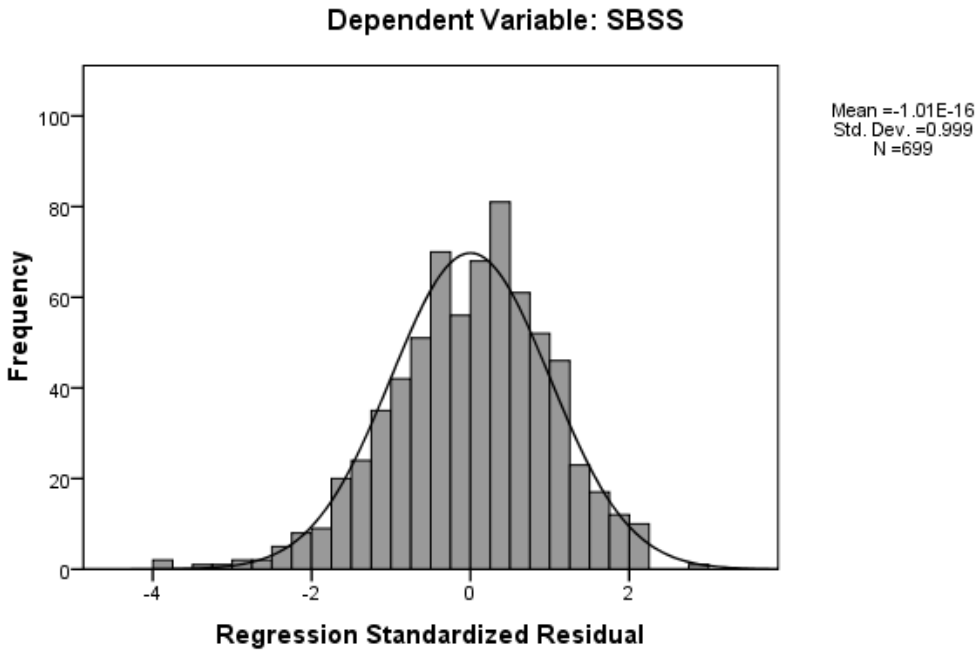

Figure 10. SBSS score distribution

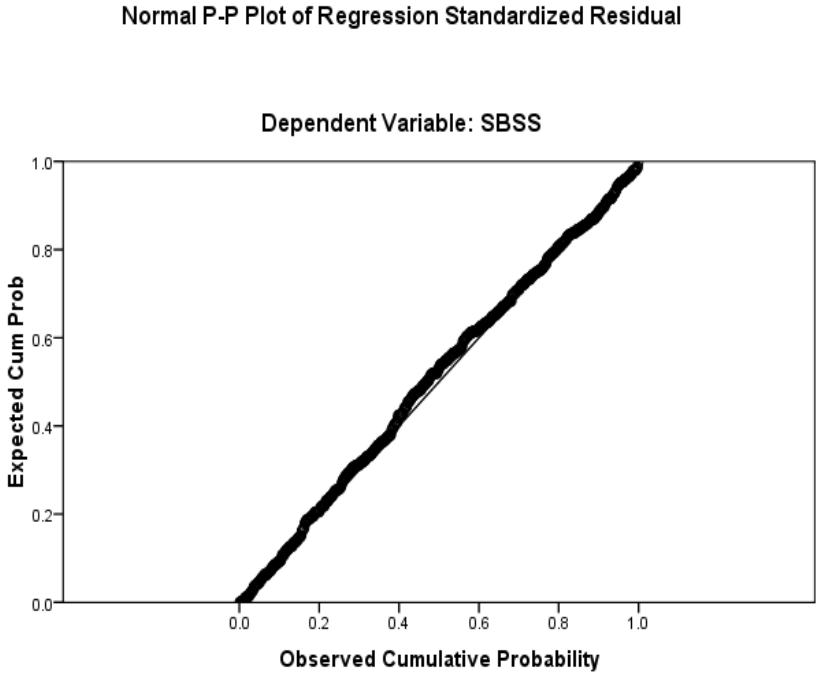

Figure 11. SASS-SBSS scores regression plot

Having confirmed the data met the assumptions for MANOVA testing, analysis proceeded with analysis of subscale scores based on academic major. Results indicated

no significant statistical difference in information security attitudes or behaviors based on academic major (F (12, 1382) = 1.160, p = .307; Wilks' Λ = 0.980, partial η^2 = .010). Multivariate test results are depicted in the following table.

Table 20

Results of multivariate analysis SASS, SBSS, and academic major

Multivariate Tests[a]

Effect		Value	F	Hypoth-esis df	Error df	Sig.	Partial eta Squared
Intercept	Pillai's Trace	.990	35093.462[b]	2.000	691.000	.000	.990
	Wilks' Lambda	.010	35093.462[b]	2.000	691.000	.000	.990
	Hotelling's Trace	101.573	35093.462[b]	2.000	691.000	.000	.990
	Roy's Largest Root	101.573	35093.462[b]	2.000	691.000	.000	.990
Academic major groups	Pillai's Trace	.020	1.158	12.000	1384.000	.309	.010
	Wilks' Lambda	.980	1.160[b]	12.000	1382.000	.307	.010
	Hotelling's Trace	.020	1.163	12.000	1380.000	.305	.010
	Roy's Largest Root	.019	2.156[c]	6.000	692.000	.045	.018

a. Design: Intercept + Academic major groups
b. Exact statistic
c. The statistic is an upper bound on F that yields a lower bound on the significance level

Results of Tukey comparisons indicated no statistically significant relationships between information security attitude subscale scores (SASS) and academic major. Neither were any statistically significant relationships found between information

security behavior subscale scores (SBSS) and academic major. The major group most closely approaching a significant relationship involved information security behaviors and the mathematical and technological sciences major group, with the lowest significance level being $p = .061$. This is likely due to that group including the computer science and information technology majors, both of which require a semester of information security training. The results of multiple comparison analysis are depicted in the table in Appendix D.

The results of MANOVA testing point to accepting the null hypothesis ($H1_0$), and stating that there were no statistically significant differences in information security attitudes or behaviors based on academic major. There was a slightly higher relationship between the mathematical and technological sciences major and behaviors, possibly due to the inclusion of computer science and information technology majors in that group. However, we conclude that the answer to Research Question 1 is that there were no significant differences in information security attitudes or behaviors based on academic major.

Research Question 2: Are there differences in students' information security attitudes or behaviors based on hours of information security training? This question addressed the relationship between information security training and information security attitudes and behaviors. Hypothesis 2 proposed that there are differences in students' information security attitudes or behaviors based on hours of information security training. Reported hours of information security training ranged from 0 (the highest percentage, at 69.4%) to 120 (one respondent, 0.1%). Seventeen students reported having had between 6 and 10 hours of training. The responses

indicated that of the 699 responses analyzed, 654 reported having had less than six hours of information security training, or 93.6% of the respondents. The skewness of the distribution may be a factor in the findings. Had more participants had more hours of training, resulting in a more even distribution, the findings might have been different. Indeed, the problem addressed by this research is that students are not trained in information security, resulting in risky information security attitudes and behaviors.

Table 21

Information security training by group

Information security training hours	Frequency	%
0-5	654	93.6
6-10	17	2.4
11-20	9	1.3
21-30	3	.4
31-50	8	1.1
51+	8	1.1
Total	699	100.0

MANOVA was used for multivariate data analysis. MANOVA assumes that the dependent variables are continuous, the independent variable consists of more than one group, no participants are in more than one group, the sample size is adequate, no significant outliers, a normal distribution exists, there is a sameness of variance, a linear relationship exists, and the dependent variables have somewhat correlated with each other (Salkind, 2010). Concerning the data for this test, security attitude and behavior scores were continuous, there were six groups of hours of training, no student was a member of more than one group, the sample size was $N = 699$ (greater than the minimum required by G*Power for six groups), there was a normal distribution of scores (Figures 8 and 9),

there was a linear relationship between information security attitudes and behaviors (Figure 11), and the two were highly correlated with each other (Table 19).

Testing was performed using information security attitudes and behaviors as the dependent variables, hours of information security training as the factor, and $\alpha = .05$. The results demonstrated that there was a statistically significant difference in information security attitudes and behaviors based on a student's prior hours of information security training (F (10, 1384) = 1.160, $p < .001$; Wilks' $\Lambda = 0.959$, partial $\eta^2 = .021$). The results are depicted in the table below.

Table 22

Results of multivariate analysis SASS, SBSS, and information security training hours

Multivariate Tests[a]

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.889	2782.568[b]	2.000	692.000	.000	.889
	Wilks' Lambda	.111	2782.568[b]	2.000	692.000	.000	.889
	Hotelling's Trace	8.042	2782.568[b]	2.000	692.000	.000	.889
	Roy's Largest Root	8.042	2782.568[b]	2.000	692.000	.000	.889
Security training hours groups	Pillai's Trace	.041	2.888	10.000	1386.000	.001	.020
	Wilks' Lambda	.959	2.906[b]	10.000	1384.000	.001	.021
	Hotelling's Trace	.042	2.924	10.000	1382.000	.001	.021
	Roy's Largest Root	.039	5.423[c]	5.000	693.000	.000	.038

a. Design: Intercept + STHGroups
b. Exact statistic
c. The statistic is an upper bound on F that yields a lower bound on the significance level

Tukey post hoc testing confirmed there were no statistically significant differences in security attitude scores based on hours of information security training.

Tests of between-subjects effects showed a significance level of .156 for information security attitudes, and a significance level of .000 for information security behaviors, indicating a statistically significant relationship between hours of information security training and information security behaviors.

Spearman non-parametric correlation testing demonstrated that there is a very slight statistically significant difference in information security attitudes based on hours of information security training (R = .105, p = .005, α = .01, two-tailed). However, the effect size is only .011, accounting for only about 1% of the variance. The skewness of this category may cause a similar skew in results as 654 of the participants reported having had 0-5 hours of training. Results are depicted in the following table.

Table 23

Spearman correlation test results – SASS, hours of information security training

			Security training hours	SASS
Spearman's rho	Security training hours	Correlation Coefficient	1.000	.105**
		Sig. (2-tailed)	.	.005
		N	699	699
	SASS	Correlation Coefficient	.105**	1.000
		Sig. (2-tailed)	.005	.
		N	699	699

** - Correlation is significant at the 0.01 level (2-tailed).

The Spearman test confirmed MANOVA results and allowed us to reject the null hypothesis and state that the answer to Research Question 2 was that there were differences in both information security attitudes and information security behaviors behaviors based on hours of information security training. While the relationship to attitudes is weak, the strong relationship of training to behaviors allows us to suggest that the answer to Research Question 2 was that there were differences in information security

attitudes or behaviors based on hours of information security training.

Research Question 3: Do students' information security attitudes predict their information security behaviors? Research Question 3 addressed the relationship between information security attitudes and information security behaviors. Hypothesis 3 proposed that students' information security attitudes predict their information security behaviors. The scores were divided into a security attitudes subscale (SASS), and a security behaviors subscale (SBSS). These scores were normally distributed, as depicted in Figures 8 and 9.

Regression testing was performed on the security attitudes and security behaviors subscales using SBSS as the dependent variable and SASS as the independent variable. Results produced the histogram and p-plot in Figures 10 and 11, respectively. Figure 10 illustrates the regression distribution, while Figure 11 depicts the linear relationship between SASS and SBSS. As information security attitude scores increase, information security behaviors also increase, and vice versa, as depicted in the figures. The scatterplot in Figure 12 illustrates homoscedasticity, as the points are primarily arranged in a linear pattern that corresponds with the p-plot in Figure 11. The model summary for regression testing is presented in the following table. The R Square value indicates that information security attitudes account for about 17.7% of the variance in behaviors.

Table 24

Linear regression analysis model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.421[a]	.177	.176	6.333	1.107

a. Predictors: (Constant), SASS

b. Dependent Variable: SBSS

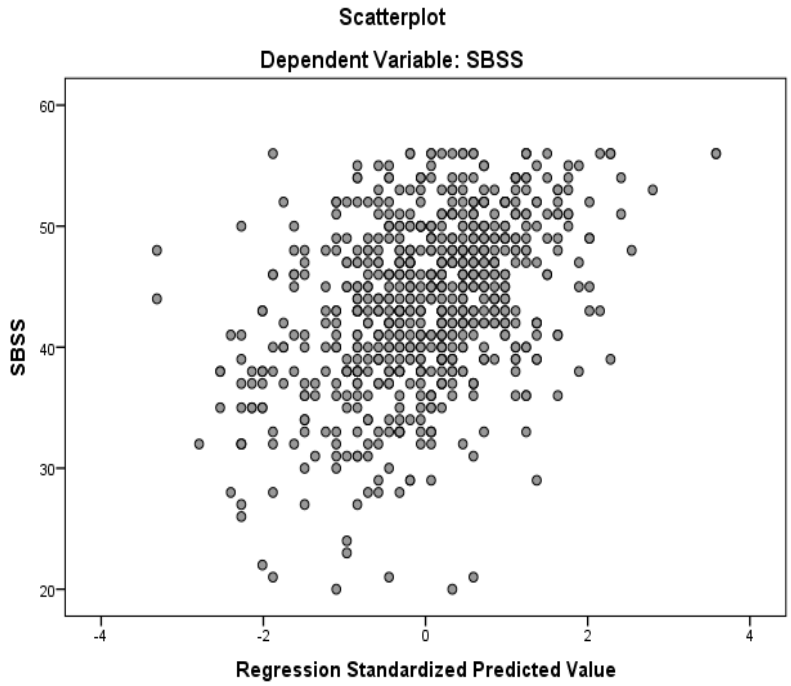

Figure 12. SASS-SBSS linear regression scatterplot

Pearson correlation testing identified a significant positive correlation between information security attitudes and information security behaviors (R = .421, p = .000, α = .01, two-tailed). The R^2 figure of .177 demonstrates that over 17% of the variances in information security behaviors are attributable to their relationship to information security attitudes. Results of correlation testing are depicted in the following table.

Table 25

Pearson correlation testing results – SASS, SBSS

		SASS	SBSS
SASS	Pearson Correlation	1	.421**
	Sig. (2-tailed)		.000
	N	699	699
SBSS	Pearson Correlation	.421**	1
	Sig. (2-tailed)	.000	
	N	699	699

**. Correlation is significant at the 0.01 level (2-tailed).

One-way ANOVA testing using the security attitude score groupings resulted in $p = .000$. This finding indicated a statistically significant relationship between information security attitudes and information security behaviors (ANOVA $F(4,694) = 24.605$, $p = .000$). The results are depicted in the following table.

Table 26

ANOVA – One-way, information security attitudes (factor) and information security behaviors (dependent variable)

Source	Sum of Squares	df	MS	F	Sig.
Between Groups	4219.919	4	10054.980	24.605	.000
Within Groups	29756.857	694	42.877		
Total	33976.775	698			

The data was randomly split into two groups for further validation of the relationship between attitudes and behaviors. Results of correlation testing on the first group confirmed the results for the group overall with sample size $N = 348$ ($R = .434$, $p = .000$, $\alpha = .01$, two-tailed). Pearson correlation testing on the second group resulted in a

statistically significant correlation as well, with $N = 351$ ($R = .408$, $p = .000$, $\alpha = .01$, two-tailed). The results of these tests are illustrated in the following tables.

Table 27

Correlation tests - Group 1

		SASS	SBSS
SASS	Pearson Correlation	1	.434**
	Sig. (2-tailed)		.000
	N	348	348
SBSS	Pearson Correlation	.434**	1
	Sig. (2-tailed)	.000	
	N	348	348

**. Correlation is significant at the 0.01 level (2-tailed).

Table 28

Correlation tests - Group 2

		SASS	SBSS
SASS	Pearson Correlation	1	.408**
	Sig. (2-tailed)		.000
	N	351	351
SBSS	Pearson Correlation	.408**	1
	Sig. (2-tailed)	.000	
	N	351	351

**. Correlation is significant at the 0.01 level (2-tailed).

The results of correlation testing, MANOVA, ANOVA, regression, and cross-validation led us to accept $H3_a$ and conclude that information security attitudes have strong predictive power with regard to information security behaviors. Therefore, we suggest the answer to Research Question 3 was that students' information security

attitudes were a statistically significant factor in predicting information security behaviors.

Evaluation of Findings

The context of this cross-sectional correlation study involved the information security attitudes and behaviors of a liberal arts university student body. However, since many students will be employees in the future (Abel et al., 2014; Lomo-David et al., 2011; U.S. Department of Education, 2014), the results may have implications beyond the university setting study context. Given the existing literature, the results were not entirely surprising. Mensch and Wilkie found a "disconnect" between students' information security attitudes (what they know or perceive) and their information security behaviors (what they do) (Mensch & Wilkie, 2011, p. 107). This results of this study, however, indicated that information security behaviors and information security attitudes are statistically significantly related ($R = .421$, $p = .000$, $\alpha = .01$, two-tailed).

On the other hand, consistent with Mensch and Wilkie (2011), this study found no statistically significant differences in information security attitudes or behaviors based on academic major (Mensch & Wilkie, 2011). While this study followed the combined methodologies of two previous studies (Mensch & Wilkie, 2011; Yoon et al., 2012), an incremental contribution of this study is the relatively large sample size of $N = 699$, larger than either of these studies by over 400 participants. Existing literature consistently recommends larger sample sizes for better generalizability. The distribution of participants across academic major, gender, and classification should contribute toward the generalizability of this study.

Practical implications of these findings point to the need for an increased level of

information security training at the university level. Higher education institutions should consider requiring information security training for all students, regardless of major. Given the findings on the influence of information security habits on information security behaviors, such training should include hands-on repetitive practice of positive information security behaviors (Meso et al., 2013). Such training may better prepare graduating students to enter the work force with more secure behaviors and habits, thereby benefiting their future employers (Booker et al, 2009).

Summary

The results of this cross-sectional correlational study were presented in this chapter. Findings were organized around research variables and related hypotheses. The study investigated the information security attitudes and behaviors of students at ABC University, a liberal arts university in the Southeastern United States. Data was collected in the spring semester during late April and early May of 2016. Data collection was facilitated through an online SurveyMonkey survey. An email link was sent to 2,445 eligible participants through the university's email system, and 812 students participated. Of the 812 responses, 113 were eliminated due to improper or incomplete answers, leaving a sample size of $N = 699$.

Data analysis, including correlation testing, ANOVA, MANOVA, and regression testing provided insight into student attitudes and behaviors regarding information security. The findings indicated that academic major had no statistically significant relationship to information security behaviors. While the results also indicated no statistically significant relation between academic major and information security attitudes, the significance level was found to be just outside the .05 significance level at α

= .059. Interestingly, prior information security training did not seem to be significantly related to information security attitudes, but information security attitudes did appear to be statistically significantly related to information security behaviors. These findings point to a need for information security training across all majors that includes both awareness and practice.

Concerning hypotheses, the findings led us to reject $H1_a$, as no statistically significant differences were found in information security attitudes or information security behaviors based on academic major. The findings were mixed on H2, as Pearson correlation testing indicated statistically significant differences, but MANOVA and ANOVA indicated no statistically significant differences in information security attitudes based on information security training hours. The results allowed us to accept $H2_a$, as hours of information security training did seem to be significantly related to information security behaviors, though this did not prove to be so with information security attitudes. However, the study results allowed us to accept $H3_a$, as information security attitudes had a statistically significant relationship with information security behaviors. While correlation does not prove causality, it does demonstrate that a significant relationship exists. The dataset was randomly split into two groups for cross validation, and the results for each group were similar to the entire group's results, all achieving a significance level of $\alpha = .01$. This allows us to confidently propose that information security attitudes are strong predictive factors of information security behaviors.

Chapter 5: Implications, Recommendations, and Conclusions

University students should be trained in generally accepted information security practices in order to protect their own data and contribute positively to their future employers by helping assure information security (Jones & Heinrichs, 2012; Lomo-David et al., 2011). The problem is that many students may be not be following generally accepted information security practices, using security tools, or may have negative information security perceptions (Yoon, Hwang &, Kim, 2012) and attitudes (Mensch & Wilkie, 2011; Slusky & Partow-Navid, 2012). The purpose of this cross-sectional quantitative correlational and comparative study was to understand the relationship between information security attitudes and behaviors of higher education students at ABC University, a private liberal arts institution located in the Southeastern United States.

The ABC Office of Planning, Research, and Assessment (OPRA) emailed the survey link to selected students out of the 2,600+ student body. The elimination of under-18 students and non-degree program students reduced the number invited to 2,445. Participation was voluntary, and a drawing for five cash awards was held after the survey was closed. This resulted in 812 responses, with $N = 699$ complete and usable responses. The incentive may have resulted in a larger sample size than might otherwise have been obtained (Doerfling et al., 2010; Salkind, 2010).

A cross-sectional correlational quantitative approach was used to design the questionnaire, which combined Yoon's Student Security Attitudes and Behaviors survey (Yoon et al., 2012) with a modified demographic section from Mensch and Wilkie's study (Mensch & Wilkie, 2011). This non-experimental study explored the data resulting

from self-reported attitudes and behaviors of the higher education participants. The online survey link was sent to students in an invitation email to students age 18 and over, who were part of a degree program, and who attended classes on campus.

The author provided an informed consent notice at the beginning of the survey that informed the potential participants of the voluntary nature of the survey, the lack of deception in the survey, and contact names for questions or complaints. The online survey included a clickable radio button to consent or not consent to take the survey. IRB approvals from both NCU and ABC were obtained before beginning data collection. Care was taken by the ABC OPRA and the researcher to protect the identities of the respondents. Electronic data will be stored in encrypted format for seven years and then destroyed. No paper form of the data was produced for this study.

A potential limitation was that of using a single site for the survey. However, there is little reason to believe that students at ABC University are significantly different from students at other schools. Another limitation was the self-reporting nature of the survey, and while some respondents might have given false answers to some questions (Clayson & Haley, 2011), the researcher assumed that respondents would answer questions honestly and accurately. The cross-sectional nature of the study provided only a snapshot of student behaviors and attitudes, and thus did not take into consideration the effects of a treatment or other time-dependent variables (Salkind, 2010). However, this appeared to be the best approach for this study, due to the time constraints of a dissertation project. The purpose of the study was to investigate attitudes and behaviors at a point in time, as opposed to studying the effects of a treatment such as an information security class. In addition, this approach more closely emulated Yoon's study (Yoon et

al., 2012). Finally, almost 86% of respondents were Caucasian, and did not provide a great diversity across ethnicity. However, the responses approximated the ethnic makeup of the ABC student body.

This chapter includes a short review and discussion of the three research questions and the study's findings, including comparison and contrast to related extant literature. Future research considerations and potential applications of the study's findings are presented in this chapter. Conclusions that may be drawn from this research precede a chapter summary.

Implications

Three research questions gave structure and direction to this study, and provided a basis for its purpose. The problem studied was that many students might be lacking in proper information security practices, use of information security tools, and proper information security perceptions (Yoon, Hwang &, Kim, 2012) and attitudes (Mensch & Wilkie, 2011; Slusky & Partow-Navid, 2012). The increased student use of mobile devices, combined with students' lax security practices (Slusky & Partow-Navid, 2012) and information security attitudes (Mensch & Wilkie, 2011), seems to make students easy targets for hackers and malware. Prior research has been inconclusive regarding the critical vulnerabilities in their behaviors and technology use (Jones & Heinrichs, 2012; Mensch & Wilkie, 2011; Yoon et al., 2012).

The purpose of this study was to explore factors related to information security attitudes and behaviors. The findings of this study regarding specific relationships regarding information security attitudes and behaviors contribute to the understanding the subject. Specifically, the results demonstrated that information security behaviors were

strongly related to information security attitudes. Analysis also confirmed that academic major was not significantly related to information security attitudes or behaviors, confirming previous findings (Mensch & Wilkie, 2011). Analysis of the data indicated that there is a significant relationship between hours of information security training and information security behaviors. Finally, the results also demonstrated that specific information security habits were strongly related to information security behaviors, confirming previous research (Yoon et al., 2012). Several behavioral theories provided a context, including protection motivation theory (PMT), theory of planned behavior (TPB), theory of behavioral intention (TBI), and theory of reasoned action (TRA) (Yoon et al., 2012).

Research Question One: Are there differences in students' information security attitudes and behaviors based on academic major? The findings indicated there were no statistically significant difference in students' information security attitudes based on academic major. ANOVA testing confirmed the null hypothesis $H1_0$ to be correct in proposing that there were no significant differences in information security attitudes or behaviors based on academic major. MANOVA testing further confirmed no differences in attitudes and behaviors based on academic major, and helped reduce the chance of a Type I error that was possible with ANOVA testing.

Regarding behaviors, the MANOVA and ANOVA findings indicated there was a slight difference (ANOVA $F(6,292 = 2.034)$ between major groups. However, this is not a significant difference, with the math and technological sciences group scoring less than three points higher than the next highest scores. This is consistent with previous findings that academic major is not significantly related to information security behaviors

(Mensch & Wilkie, 2011). This led us to accept the null hypotheses $H2_0$, that there were no statistically significant differences in information security behaviors based on academic major.

These findings are consistent with previous studies' findings (Mensch & Wilkie, 2011). On their own, the findings for this question may appear to have no implications for higher education institutions. However, when considered in the context of the entire study and previous research, there are several implications. Information security training should be included in at least business and information technology programs (White et al., 2013), and should be included in other academic major programs to facilitate behavioral change (NIST, 2003). Further, building program-specific information security curricula for different majors could be advantageous (Slusky & Partow-Navid, 2012). This should be helpful for students who might need to know how to secure a computer and maintain it at an acceptable security level (Slusky & Partow-Navid, 2012). As colleges and universities are educating the employees of the future, they might have an obligation to train students to understand information security issues (White et al., 2013), across all majors. Yoon et al. (2012) recommended focusing on the positive returns of good information security behaviors. Institutions of higher learning are the "ideal place" to deliver effective information security training to students (Fulton, Lawrence, & Clouse, 2013, p. 78).

Existing literature has not consistently presented a significant relationship between academic major and security attitudes and behaviors, with the exception of slightly higher scores for technology majors (Mensch & Wilkie, 2011). Taken alone, this finding might appear to have no implications for higher education. However, when

viewed in the context of this study and previous research, there are implications for higher education institutions from this finding. Today's students are tomorrow's "protectors of data and systems" (White et al., 2013, p. 14), and higher education institutions may have an obligation to produce graduates who have developed good information security habits (Jones & Heinrichs, 2012; Lomo-David et al., 2011). As colleges and universities are educating the employees of the future, they might have an obligation to train students (across all majors) who understand information security and have developed good information security habits (White et al., 2013).

Research Question Two: Are there differences in students' information security attitudes and behaviors based on hours of information security training? The ANOVA findings indicated a slightly significant relationship between the hours of training and information security attitudes ($R = .105$, $p = .005$, $\alpha = .01$, two tailed), but not enough to fully embrace hypotheses $H2_a$. However, the difference was enough to lead us to reject $H2_0$, and conclude that information security training was slightly related to information security attitudes. MANOVA testing further confirmed these findings, and reduced the possibility of a Type I error.

The ANOVA findings for hours of training and information security behaviors ($R = .202$, $p = .000$, $\alpha = .01$, two-tailed) indicated a stronger relationship than was found in the ANOVA results for information security attitudes. The R^2 (.041) value indicated that information security training accounted for about 4% of the variableness in information security behaviors with $\alpha = .01$ significance level. MANOVA tests against the attitudes and behaviors dependent variables, using hours of training as the factor, confirmed ANOVA findings, leading us to accept $H2_a$, and state that the answer to Research

Question 2 is that there are differences in both information security attitudes and behaviors based on hours of information security training.

The implication for higher education institutions is that information security training is likely to produce students with more positive information security behaviors. Interestingly, while more natural and health sciences majors reported having had information security training (N = 158), the mean was only .75, indicating an average of less than an hour of training for each student. Conversely, only 83 participants reported as mathematical and technological sciences, but the average amount of training was over 11 hours, with a standard deviation of 23. The computer science and information technology majors were included in this group. These programs require a course on information security in the junior or senior year. This group also had the highest security attitudes composite score, at 79.01, and the highest security behaviors score at 46.06, both about 3 points higher than the other groups. This seems to reinforce the finding that hours of information security training have a positive effect on information security attitudes and behaviors.

Higher education institutions should require such training for all majors in order to produce information security aware graduates (Mensch & Wilkie, 2011; Yoon et al., 2012). This implication may also transfer to the corporate environment, where information security training should produce more security aware employees (Knapp & Ferrante, 2012). Students' information security attitudes are, according to analysis for RQ3, an influencing factor related to information security behaviors (Mensch & Wilkie, 2011), and changing attitudes should precipitate a change in behaviors. Attitudes toward their own abilities or the ability of security tools to protect information assets from

security attacks also may predict information security behaviors (Yoon et al., 2012). Part of the problem in non-compliance may have to do with lax attitudes toward information security (Guo et al., 2011), in turn potentially raising the risk level for organizations (Ponemon, 2012). Previous research has suggested that information security awareness training should be delivered to university students to educate them on threats and risks, and proper responses (Kim, 2014; Lomo-David et al., 2011). This finding reinforces many previous research suggestions for information security awareness training at the university level.

NIST has stated that a goal of security awareness programs is to both produce better information security behaviors and to reinforce existing good security behaviors (NIST, 2003). The intent of information security awareness training is to teach good security skills and change information security behaviors (NIST, 2003). Information security awareness training should focus on activities that train employees to respond in a systematic way when working with information (Puhakainen & Siponen, 2010). This recommendation is supported by a study that proposed training students in actual information security practices to improve their information security behaviors (Yoon et al., 2012). Alternatively, some have suggested requiring students to learn how to carry out information security attacks to develop an understanding of the need for information security (Papanikolaou et al., 2013). This research supports much of the previous research suggesting information security training at the university level. This implication concerning training may be transferrable to the corporate environment in that more security-aware employees may produce a more secure corporate environment (Knapp & Ferrante, 2012).

Research Question Three: Do students' information security attitudes predict their information security behaviors? The findings (Pearson's $R = .421$, $p = .000$, $\alpha = .01$, two-tailed) indicated that information security attitudes were strongly predictive factors in information security behaviors. The R^2 value of .177 indicated that attitudes accounted for about 17% of the variance in behaviors. This finding was consistent with previous research indicating a relationship between information security attitudes and behaviors (Mensch & Wilkie, 2011). The implication for higher education institutions is that they must find ways to influence information security attitudes in a positive way, thereby indirectly affecting a positive influence on information security behaviors. Given the relationship between information security training and both attitudes and behaviors, higher education institutions should develop training that influences both. Higher learning institutions should also consider internships that require hands-on information security work (Meso et al, 2013).

Interestingly, consistent with Yoon's findings, habit appeared to play a large role in information security behaviors (Yoon et al., 2012). Both habit item scores (SB1, SB2) proved significant at $\alpha = .01$ (two-tailed), and the *p* values were .517 and .598 respectively. These scores showed that habit accounts for over 60% of the variation in information security behaviors. To this end, higher education institutions should seek to make good information security behaviors a habit for students (Yoon et al., 2012). This might involve courses that educate students on threats, risks, and proper responses (Kim, 2014; Lomo-David et al., 2011), and include enough practice to transform responses into habits (Polites & Karahanna, 2013; Vance et al., 2012; Yoon et al., 2012). Compliance

with security policy should also be a central part of information security training for students (Chenoweth et al., 2010).

One perplexing aspect of the findings was the results showing a weak relationship between hours of information security training and student information security attitudes, followed by the finding of a statistically significant relationship of hours of training to information security behaviors. The perplexity was compounded by the finding that information security attitudes were significantly related to information security behaviors to the point of being a strong predictive factor in security behaviors. This may pose a question for colleges and universities in how to positively influence students' information security attitudes, with the end goal being to positively shape their information security behaviors. Future research should consider revising the security attitudes questionnaire and subscale to better study and understand this relationship.

Recommendations

The findings of this study informed several recommendations for institutions of higher learning on the topic of information security. The finding of a significant positive relationship between hours of information security training and higher information security behavior scores suggested that universities should require courses that instruct students in basic information security. This is consistent with previous research by Mensch and Wilkie (2011). This training should include how to use security tools and techniques that help mitigate risks, reduce threats, and reduce severities. The list of tools and techniques should at a minimum include anti-malware (anti-virus, anti-spam, email filters, and others), browser security software (pop-up blockers, ad blockers, browser

filters), firewalls, recognizing potential infections, encryption, and backup and restore operations (Mensch & Wilkie, 2011).

Given the finding on the significant relationship between information security attitudes and information security behaviors, the negative aspects of information security ignorance should be stressed in information security courses (Slusky & Partow-Navid, 2012). Training should therefore include information on information security risks, threats, and severities to better inform students of the potential consequences of a security event. Training should also include use of tools and techniques that help reduce risk, counter threats, and reduce severities of a security event. This recommendation was accentuated by the fact that neither attitudes nor behaviors were found to be significantly related to having actually been a victim of identity theft. Given the relationship of habit to information security behavior, training should include enough hands-on practice to form behaviors into habits.

The finding on the relationship of habit to information security behaviors may be the one of the most significant additional findings of this study. Correlation testing between SB1 and information security behaviors demonstrated a statistically significant relationship ($R = .517$, $p = .000$, $\alpha = .01$, two-tailed). Similarly, correlation testing between SB2 and information security behaviors demonstrated a statistically significant relationship ($R = .598$, $p = .000$, $\alpha = .01$, two-tailed). These findings support Yoon's similar findings that information security habits seem to strongly influence information security behaviors (Yoon et al., 2012). This finding suggested universities should require real-world internships or classes that require frequent, repetitive hands-on security activities. Such experiences may help form positive information security habits through

repetition, agreeing with Ralevich and Martinovic (2012), and Meso et al. (2013). The fact that habit appeared to be more significant than an actual negative experience suggested again the importance of training that requires actual repetitive positive security practice to instill positive habits.

Limitations and Future Research

This study was limited to one private faith-based liberal arts institution. Therefore, some might perceive participants' backgrounds and social grouping as too similar (Yoon et al., 2012). Future studies should include multiple institutions, including secular private and public institutions, to achieve more diversity of backgrounds and social grouping. It is possible that there are factors at play in students' information security attitudes and behaviors that were not addressed in this study, such as economic status, country of high school education, and others. The researcher leaves the identification and study of factors not included here to future research. The questionnaire could be expanded to include more factors for both information security attitudes and behaviors (Yoon et al., 2012). The questionnaire and subscale could also be revised to achieve a higher level of reliability and validity. Finally, future research could consider a longitudinal approach, surveying students before and after an information security fundamentals course, and studying the results to determine the efficacy of the training in order to refine the curriculum.

Conclusions

This cross-sectional quantitative and correlational study investigated the information security attitudes and behaviors of undergraduate and graduate students at ABC University. The purpose of the study was to gain an understanding of the factors

related to those attitudes and behaviors, with an eye toward development of curricula that might be useful in better preparing students for both their time in college, as well as employment after college. This chapter presented a review of the purpose of the study, the research questions addressed, and the findings of data analysis. This chapter also presented implications and comparisons with related previous literature.

Research results indicate that while about 80% of students scored medium to very high information security attitudes, almost 80% scored medium to very low information security behaviors. This is consistent with the gap between attitudes and behaviors in previous research (Mensch & Wilkie, 2011). Information security attitudes were found to be the most predictive analyzed factor in information security behaviors. Analysis of information security training hours produced mixed results, with one test showing a slightly positive relationship with attitudes, and another showing no significant relationship. Information security training was found to have a statistically significant relationship with information security behaviors.

It is up to colleges and universities to train students to have positive information security attitudes and behaviors, so that they may enter the workforce prepared to protect their employers' information and computing assets. Training should include information to shape information security attitudes, which in turn affect behaviors. Training should also include practice of positive behaviors to the point of forming good information security habits. Such a two-pronged approach to information security training should effect positive information security behaviors.

References

Aarts, H., & Dijksterhuis, A. (2000). Habits as knowledge structures: Automaticity in goal-directed behavior. *Journal of Personality and Social Psychology, 78*(1), 53-63. doi:10.1037/0022-3514.78.1.53

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 236-247. doi:10.1080/0144929X.2012.708787

ABC University (2015). Enrollment statistics for 2014-2015 academic year. ABC Office of Planning, Research, and Assessment.

Abel, J. R., Deitz, R., Su, Y. (2014). Are recent college graduates finding good jobs? *Current Issues in Economics and Finance, 20*(1), 1-8. Retrieved from http://www.newyorkfed.org/research/current_issues/ci20-1.pdf?utm_source=s5_mobile_site&utm_medium=mobile&utm_campaign=77726

Abraham, S., Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications, *Technology in Society, 32*(3), 183-196. DOI: 10.1016/j.techsoc.2010.07.001

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370. doi:http://dx.doi.org/10.1007/s10845-012-0683-0

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179–211.

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections, *Psychology & Health, 26*(9), 1113-1127, DOI: 10.1080/08870446.2011.613995

Albarrak, A. I. (2011). Evaluation of users' information security practices at King Saud University hospitals. *Global Business & Management Research, 3*(1), 1-6.

AlHogail, A. (2015). Design and validation of information security culture framework, *Computers in Human Behavior, 49*, 567-575, doi:http://dx.doi.org/10.1016/j.chb.2015.03.054.

Alsmadi, S. (2008). Marketing research ethics: Researcher's obligations toward human subjects. *Journal of Academic Ethics, 6*(2), 153-160. doi:10.1007/s10805-008-9060-1

American Psychological Association (APA) (2010). Ethical principles of psychologists and code of conduct. Retrieved from http://www.apa.org/ethics/code/index.aspx

Astakhova, L. V. (2014). The concept of the information-security culture. *Scientific and Technical Information Processing, 41*(1), 22-28. doi:http://dx.doi.org/10.3103/S0147688214010067

Bagozzi, R., & Yi, Y. (2012). Specification, evaluation, and interpretation of structural equation models. *Journal of the Academy of Marketing Science, 40*(1), 8-34. doi:10.1007/s11747-011-0278-x

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Englewood Cliffs, Prentice-Hall, NJ.

Barrios, R. M. (2013). A multi-leveled approach to intrusion detection and the insider threat. *Journal of Information Security, 4*(1), 54-65.

Baskerville, R., Park, E. H., & Kim, J. (2014). An emote opportunity model of computer abuse. *Information Technology & People, 27*(2), 155-181. doi:http://dx.doi.org/10.1108/ITP-11-2011-0068

Benson, V., Saridakis, G. & Tennakoon, H. (2015). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People, 28*(3), pp. 426-441.

Bogolub, E. (2010). The obligation to bring about good in social work research. , *Qualitative Social Work 9*(1), 9-15. doi: 10.1177/1473325009355614

Booker, Q. E., Rebman, C., & Kitchens, F. L. (2009). The impact of computer and internet security training for undergraduate students: Attitudinal changes. *Issues in Information Systems 10*(1), 191-197.

Boss, S. R., Galletta, D. F., Lowry, B., P., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864.

Botti, M., & Endacott, R. (2005). Clinical research 5: Quantitative data collection and analysis. *Intensive & Critical Care Nursing, 21*(3), 187-93. doi:http://dx.doi.org/10.1016/j.iccn.2005.02.005

Brody, R. G., Brizzee, W. B., & Cano, L. (2012). Flying under the radar: Social engineering. *International Journal of Accounting and Information Management, 20*(4), 335-347. doi:http://dx.doi.org/10.1108/18347641211272731

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-A7.

Carifio, J., & Perla, R. (2008). Resolving the 50-year debate around using and misusing Likert scales. *Medical Education, 42*(12), 1150-1152. doi:10.1111/j.1365-2923.2008.03172.x

Case, C. J., & King, D. L. (2013). Cyber security: A longitudinal examination of undergraduate behavior and perceptions. *ASBBS Ejournal, 9*(1), 21-29.

Case, C. J., & King, D. L. (2014). System security: A trend analysis of student electronic resources use policy perceptions and risky behavior. *ASBBS Ejournal, 10*(1), 31-42.

Cavallari, M. (2011). The organizational relationship between compliance and information security. *International Journal of the Academic Business World, 5*(2), 63-76.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems, 31*(4), 49-87. doi:10.1080/07421222.2014.1001257

Chen, Y., Ramamurthy, K., & Wen, K. (2012). Organizations' information security policy compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29*(3), 157-188.

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11-19.

Chenoweth, T., Minch, R., & Tabor, S. (2010). Wireless insecurity: Examining user security behavior on public networks. *Communications of the ACM, 53*(2), 134-138. doi:10.1145/1646353.1646388

Chiang, L., & Lee, B. (2011). Ethical attitude and behaviors regarding computer use. *Ethics & Behavior, 21*(6), 481-497. doi:10.1080/10508422.2011.622181

Chigona, W. w., Robertson, B., & Mimbi, L. (2012). Synchronised smart phones: The collision of personal privacy and organisational data security. *South African Journal of Business Management, 43*(2), 31-40.

Ciocchetti, C. A. 2011. The eavesdropping employer: A twenty-first century framework for employee monitoring. *American Business Law Journal 48*(2): 285–369.

Cisco Systems. (2013). Cisco 2011 annual security report. Retrieved from http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, *52*(4), 20-29.

Clayson, D. E., & Haley, D. A. (2011). Are students telling us the truth? A critical look at the student evaluation of teaching. *Marketing Education Review*, *21*(2), 101-112. doi:10.2753/MER1052-8008210201

Collins, J. D., Sainato, V. A., & Khey, D. N. (2011). Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors. *International Journal of Cyber Criminology, 5*(1), 794-810.

Constantinescu, M., Onur, E., Durmus, Y., Nikou, S., de Reuver, M., Bouwman, H., Djurica, M., & Maria Glatz, P. (2014). Mobile tethering: Overview, perspectives and challenges. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*, *16*(3), 40-53.

Cope, D. G. (2014). Using electronic surveys in nursing research. *Oncology Nursing Forum*, *41*(6), 681-682. doi:10.1188/14.ONF.681-682

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849-1858, doi:http://dx.doi.org/10.1016/j.chb.2012.05.003.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226. doi:10.2308/isys-50704

Custer, W. L. (2010). Information security issues in higher education and institutional research. *New Directions for Institutional Research*, *2010*(146), 23-49. doi:10.1002/ir.341

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658. doi:http://dx.doi.org/10.1057/ejis.2011.23

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318. doi:10.2753/MIS0742-1222310210

de Albuquerque, A. E., Jr., & dos Santos, E. M. (2015). Adoption of information security measures in public research institutes. *Journal of Information Systems and Technology Management, 12*(2), 289-315.

Derbyshire, K. L., Lust, K. A., Schreiber, L. R. N., Odlaug, B. L., Christenson, G. A.,

Golden, D. J., & Grant, J. E. (2013). Problematic internet use and associated risks in a college sample. *Comprehensive Psychiatry, 54*(5), 415. doi:http://dx.doi.org/10.1016/j.comppsych.2012.11.003

Dilmperi, A., King, T., Dennis, C. (2011). Pirates of the web: The curse of illegal downloading, *Journal of Retailing and Consumer Services 18*(2), 132-140, doi:http://dx.doi.org/10.1016/j.jretconser.2010.12.004.

Ding-Long H., Rao, P. P., Salvendy, F. G., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices, *International Journal of Human-Computer Studies, 69(*12), 870-883, doi:http://dx.doi.org/10.1016/j.ijhcs.2011.07.007

Ding-Long, H., Rau, P. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221-232. doi:10.1080/01449290701679361

Doerfling, P., Kopec, J. A., Liang, M. H., & Esdaile, J. M. (2010). The effect of cash lottery on response rates to an online health survey among members of the Canadian association of retired persons: A randomized experiment. *Canadian Journal of Public Health, 101*(3), 251-4.

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. *The International Journal of Information Management, 31*(3), 201-209.

Duggan, G. B., Johnson, H., Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies, 70,* (6), 415-431. doi: http://dx.doi.org/10.1016/j.ijhcs.2012.02.008.

Facebook (2015). *Press room.* Retrieved from https://newsroom.fb.com/company-info/

Fisher, W., & Allen, C. (2015). Road warriors and information systems security: Risks and recommendations. *Journal of Management Information and Decision Sciences, 18*(1), 84-96.

Fleischmann, K. R., Robbins, R. W., & Wallace, W. A. (2011). Information ethics education for a multicultural world. *Journal of Information Systems Education, 22*(3), 191-201.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research (JMR), 18*(1), 39-50.

Franqueira, V. N. L., van Cleeff, A., van Eck, P., & Wieringa, R. J. (2013). Engineering security agreements against external insider threat. *Information Resources Management Journal, 26*(4), 66-91. doi: 10.4018/irmj.2013100104.

Friedewald, M., & Raabe, O. (2011). Ubiquitous computing: An overview of technology impacts. *Telematics and Informatics 28*(2), 55-65. doi:10.1016/j.tele.2010.09.001

Fulton, E., Lawrence, C., & Clouse, S. (2013). White hats chasing black hats: Careers in IT and the skills required to get there. *Journal of Information Systems Education, 24*(1), 75-80.

Gabberty, J. W. (2013). Educating the next generation of computer security professionals: The rise and relevancy of professional certifications. *The Review of Business Information Systems (Online), 17*(3), 85-97.

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy & Security, 11*(1), 38-54.

Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security, 19*(4), 216-230. doi:http://dx.doi.org/10.1108/09685221111173049

Gettman, H. J., & Cortijo, V. (2015). "Leave me and my Facebook alone!" Understanding college students' relationship with Facebook and its use for academic purposes. *International Journal for the Scholarship of Teaching & Learning, 9*(1), 1-16.

Grama, J., and EDUCAUSE (2014). Just in time research: Data breaches in higher education. Retrieved from https://net.educause.edu/ir/library/pdf/ECP1402.pdf.

Grajek, S., & 2013-2014 EDUCAUSE IT Issues Panel (2014). Top-ten IT issues, 2014: Be the change you see. *EDUCAUSE Review.* Retrieved from http://www.educause.edu/ero/article/top-ten-it-issues-2014-be-change-you-see

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management & Computer Security, 17*(3), 276-289. doi:http://dx.doi.org/10.1108/09685220910978112

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155-176. doi:http://dx.doi.org/10.1108/09685221111153546

Hamade, S. N. (2013). Perception and use of social networking sites among university students. *Library Review, 62*(6), 388-397. doi:http://dx.doi.org/10.1108/LR-12-2012-0131

Harris, G. E., & Dalton, S. (2014). University student expectations of confidentiality when disclosing information to their professors. *Higher Education Studies, 4*(1), 43-50.

Harris, M. A., Furnell, S., & Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy & Security, 10*(4), 186-202.

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97-114. doi:http://dx.doi.org/10.1108/IMCS-03-2013-0019

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals. *Information Management & Computer Security, 21*(4), 266-287. doi:http://dx.doi.org/10.1108/IMCS-08-2012-0043

Helkala, K., & Hoddø Bakås, T. (2014). Extended results of Norwegian password security survey. *Information Management & Computer Security, 22*(4), 346-357.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:10.1016/j.dss.2009.02.005

Hollier, G., Blankenship, D., & Jones, I. (2013). College business students' attitudes toward ethics. *Journal of Business and Behavioral Sciences, 25*(1), 54-68.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81. doi:10.1145/2063176.2063197

Hovav, A. & D'Arcy, J. (2012), Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49*(2), 99-110.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660. doi:10.1111/j.1540-5915.2012.00361.x

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information

security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems, 31*(4), 6-48. doi:10.1080/07421222.2014.1001255

Hua, J., & Bapna, S. (2013). Who can we trust? The economic impact of insider threats. *Journal of Global Information Technology Management (Ivy League Publishing)*, 47-67.

Hutchings, A. (2012). Computer security threats faced by small businesses in Australia. *Trends & Issues in Crime & Criminal Justice*, (433), 1-6.

IBM (2013). Understanding the economics of IT risk and reputation: Making the business case for business continuity and IT security. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_RL_IH_USEN&htmlfid=RLW03024USEN&attachment=RLW03024USEN.PDF#loaded

IBM (2014). IBM security services cyber security intelligence index. Retrieved from http://www-935.ibm.com/services/us/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic/

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, Vol. 51*, 69-79.

Jacobs, R. S., Heuvelman, A., Tan, M., & Peters, O. (2012). Digital movie piracy: A perspective on downloading behavior through social cognitive theory. *Computers in Human Behavior 28*(3), 958-967. doi:http://dx.doi.org/10.1016/j.chb.2011.12.017.

Jambon, M., Smetana, J. (2011). College students' moral evaluations of illegal music downloading. *Journal of Applied Developmental Psychology 33*(1), p. 31-39. DOI: 10.1016/j.appdev.2011.09.001.

James, T., Nottingham, Q., & Kim, B. C. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information Technology and Management, 14*(2), 69-89. doi:http://dx.doi.org/10.1007/s10799-012-0147-4

Jang, Y., Chang, S. E., & Tsai, Y. (2014). Smartphone security: Understanding smartphone users' trust in information security management. *Security & Communication Networks, 7*(9), 1313-1321. doi:10.1002/sec.787

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-A4.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal

rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-A7.

Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management, 35*(5), 561.

Jones, B., Chin, A., & Aiken, P. (2014). Risky business: Students and smartphones. *Techtrends: Linking Research & Practice to Improve Learning*, *58*(6), 73-83.

Jones, B. H., Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, *53(2)*, 22-30.

Kam, H., & Katerattanakul, P. (2014). Information security in higher education: A neo-institutional perspective. *Journal of Information Privacy & Security, 10*(1), 28-43.

Kamau, W. T. (2013). *The bring your own device phenomena: Balancing productivity and corporate data security* (Doctoral dissertation, University of Nairobi). Retrieved from http://erepository.uonbi.ac.ke:8080/bitstream/handle/11295/63049/Kamau_The Bring Your Own Device Phenomena A Balancing Productivity And Corporate Data Security ?sequence=3&isAllowed=y

Kamil, M. L. (2004). The current state of quantitative research. *Reading Research Quarterly, 39*(1), 100-107.

Khoo Boo, L., Messmer, E., Ahn, N., & Reed, B. (2011). Smartphone security challenges in the enterprise. *Networkworld Asia*, *8*(1), 11-18.

Kiel, J. M., PhD., & Knoblauch, L. M., M.B.A. (2010). HIPAA and FERPA: Competing or collaborating? *Journal of Allied Health*, *39*(4), e161-5.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*(1), 115-126. doi:http://dx.doi.org/10.1108/IMCS-01-2013-0005

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice, 13*(5), 66-80.

Knott, C. L., & Steube, G. (2012a). Perceptions about data security for portable storage devices. *Journal of Service Science (Online), 5*(1), 1-18.

Knott, C. L., & Steube, G. (2012b). Student perceptions of password security and maintenance. *International Journal of Management & Information Systems (Online), 16*(3), 189.

Kruck, S. E., & Teer, Faye P. (2008). Computer security practices and perceptions of the next generation of corporate computer users. *International Journal of Information Security and Privacy, 2*(1), 80-90.

Kurt, D. G. (2015). Suicide Risk in College Students: The effects of internet addiction and drug use. *Educational Sciences: Theory & Practice*, *15*(4), 841-848. doi:10.12738/estp.2015.4.2639

Laerd (2013). Cronbach's Alpha (α) using SPSS Statistics. Retrieved from https://statistics.laerd.com/spss-tutorials/cronbachs-alpha-using-spss-statistics.php

Lai, F., Li, D., & Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353-363. doi:10.1016/j.dss.2011.09.002

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM, 51*(3), 71-76. doi:10.1145/1325555.1325569

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M.,H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review, 37*(12), 1049-1092.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social media & mobile internet use among teens and young adults. *Pew Internet.* Retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413.

Limayem, M., & Cheung, C. K. (2011). Predicting the continued use of Internet-based learning technologies: The role of habit. *Behaviour & Information Technology, 30*(1), 91-99. doi:10.1080/0144929X.2010.490956

Limayem, M., Khalifa, M., and Chin, W. W. (2004). Factors motivating software piracy: A longitudinal study. *IEEE Transactions on Engineering Management*, 51(1), 414–425.

Lomo-David, E., Acılar, A., Chapman, B. F., & Shannon, L. (2011). University students' computer security practices in two developing nations: A comparative analysis. *Business Studies Journal*, 363-76.

Lomo-David, E., & Shannon, L. (2009). Information systems security and safety

measures: The dichotomy between students' familiarity and practice. *Academy of Information and Management Sciences Journal, 12*(1), 29-47.

Long, J., & White, G. (2010). On the global knowledge components in an information security curriculum-a multidisciplinary perspective. *Education and Information Technologies, 15*(4), 317-331. doi:http://dx.doi.org/10.1007/s10639-010-9121-0

Marcelo, V. N., Laroche, M., Marie-Odile, R., & Eggert, A. (2012). Relationship between intangibility and perceived risk: Moderating effect of privacy, system security and general security concerns. *The Journal of Consumer Marketing, 29*(3), 176-189. doi:http://dx.doi.org/10.1108/07363761211221701

Marchany, R. (2014). Higher education: Open and secure? *SANS Institute InfoSec Reading Room.* Retrieved from http://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240

McCorkle, D., Reardon, J., Dalenberg, D., Pryor, A., & Wicks, J. (2012). Purchase or pirate: A model of consumer intellectual property theft. *Journal of Marketing Theory and Practice, 20*(1), 73-86.

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion, 30*(7), 537-542. doi:10.1177/0267659114559116

McLellan, M. L., Sherer, J. A., & Fedeles, E. R. (2015). Wherever you go, there you are (with your mobile device): Privacy risks and legal complexities associated with international "Bring Your Own Device" programs. *Richmond Journal of Law & Technology, 21*(3), 1-50.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information & Management Sciences Journal, 14(2)*, 91-116.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy & Security, 9*(1), 47-67.

Mishra, S., Caputo, D. J., Leone, G. J., Kohun, F. G., & Draus, P. J. (2014). The role of awareness and communications in information security management: A health care information systems perspective. *International Journal of Management & Information Systems (Online), 18*(2), 139-138.

Mitnick, K. (2002). *The art of deception*. Hoboken, NJ: John Wiley & Sons.

Mohamed, N., Karim, N. S. A., & Hussein, R. (2012). Computer use ethics among university students and staffs: The influence of gender, religious work value and

organizational level. *Campus - Wide Information Systems, 29*(5), 328-343. doi:http://dx.doi.org/10.1108/10650741211275099

Moll, R., Pieschl, S., Bromme, R. (2014). Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers in Human Behavior, 41*(12), 212-219. doi:http://dx.doi.org/10.1016/j.chb.2014.09.033.

Moody, G., Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information & Management 50*(6), 322-335, doi:http://dx.doi.org/10.1016/j.im.2013.04.005.

Morgan, D. L. (2015). From themes to hypotheses: following up with quantitative methods. *From themes to hypotheses: Following up with quantitative methods, 25*(6), 789-793. DOI: 10.1177/1049732315580110

Morgan, J., & Neal, G. (2011). Student assessments of information systems related ethical situations: Do gender and class level matter? *Journal of Legal, Ethical & Regulatory Issues, 14*(1), 113-130.

Myers, N. D., Ahn, S., & Jin, Y. (2011). Sample size and power estimates for a confirmatory factor analytic model in exercise and sport: A Monte Carlo approach. *Research Quarterly for Exercise and Sport 82*(3), 412-423.

Nakashima, E. (2013). Pentagon to boost cybersecurity force. *The Washington Post*. Retrieved January 22, 2016 from https://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html

Nakashima, E. (2014). U.S. notified 3,000 companies in 2013 about cyberattacks. *The Washington Post.* Retrieved from http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html

Nandedkar, A., & Midha, V. (2011). It won't happen to me: An assessment of optimism bias in music piracy. *Computers in Human Behavior, 28*(1), 41-48. doi:http://dx.doi.org/10.1016/j.chb.2011.08.009.

National Institute for Standards and Technology (NIST) (1998). Information technology security training requirements: A role- and performance-based model. NIST Special Publication No. 800-16. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

National Institute for Standards and Technology (NIST) (2003). Building an information technology security awareness and training program. NIST Special Publication No. 800-50. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-

50/NIST-SP800-50.pdf

Neill, J. (2007). Qualitative versus quantitative research: Key points in a classic debate. Retrieved from http://wilderdom.com/research/QualitativeVersusQuantitativeResearch.html February 6, 2016.

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

Noel-Levitz (2013). The impact of mobile browsing on the college search process. *2013 E-Expectations Report.*

Okenyi, P. O., & Owens, T. J. (2007). On the anatomy of human hacking. *Information Systems Security, 16*(6), 302-314. DOI: 10.1080/10658980701747237

Olusegun, O. J., & Ithnin, N. B. (2013). "People are the answer to security": Establishing a sustainable information security awareness training (ISAT) program in organization. *International Journal of Computer Science and Information Security, 11*(8), 57-64.

Omar E. M. K. & Ahmed A. S. S. (2012). Attitudes towards information ethics: A view from Egypt. *Journal of Information, Communication & Ethics in Society, 10*(4), 240-261. doi:http://dx.doi.org/10.1108/14779961211285872

Papanikolaou, A., Vlachos, V., Venieris, A., Ilioudis, C., Papapanagiotou, K., & Stasinopoulos, A. (2013). A framework for teaching network security in academic environments. *Information Management & Computer Security, 21*(4), 315-338. doi:http://dx.doi.org/10.1108/IMCS-11-2011-0056

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making, 9*(2), 117-129. doi:10.1177/1555343415575152

Patten, K., & Harris, M. (2013). The need to address mobile device security in the higher education IT curriculum. *Journal of Information Systems Education, 24*(1), 41-52.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18-28. doi:http://dx.doi.org/10.1108/09685221211219173

Pearson Education (2014). Pearson student mobile device survey 2014 (Conducted by Harris Poll). Retrieved from http://www.pearsoned.com/wp-

content/uploads/Pearson-HE-Student-Mobile-Device-Survey-PUBLIC-Report-051614.pdf

Pew Internet (2015). U.S. smartphone use in 2015. Retrieved from http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security & Emergency Management, 11*(4), 489-510. doi:10.1515/jhsem-2014-0035

Pikas, B., Pikas, A., & Lymburner, C. (2011). The future of the music industry. *Journal of Marketing Development and Competitiveness, 5*(3), 139-149.

Pinchot, J. L., Paullet, K. L. (2012). What's in your profile? Mapping Facebook profile data to personal security questions. *Issues in Information Systems, 13*(1), 284-293. Retrieved from http://iacis.org/iis/2012/65_iis_2012_284-293.pdf

Polites, G. L., & Karahanna, E. (2013). The embeddedness of information systems habits in organizational and individual level routines: Development and disruption. *MIS Quarterly, 37*(1), 221-246.

Ponemon Institute (2015). 2014: A year of mega breaches. Retrieved from http://www.ponemon.org/local/upload/file/2014 The Year of the Mega Breach FINAL_3.pdf

Ponemon Institute (2012). 2011 Cost of Data Breach Study. Retrieved from http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

Ponemon Institute (2014). 2014 Cost of Data Breach Report (2014). Retrieved from http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Price, Waterhouse, Cooper (PWC) (2015). Managing cyber risks in an interconnected world: Key findings from the global state of information security survey 2015. Retrieved from http://www.pwc.com/gsiss2015

Prislan, K. (2014). Efficiency of corporate security systems in managing information threats: An overview of the current situation. *Varstvoslovje: Journal of Criminal Justice & Security, 16*(2), 128-147.

PrivacyRights.org Web Site (2014). Chronology of data breaches (custom sort) on education only, year 2014, all types of breaches listed. Retrieved from https://www.privacyrights.org/data-breach/new

Pugmire, D. (1978). Altruism and ethics. *American Philosophical Quarterly 15*(1), 75-80. Retrieved from http://www.jstor.org/stable/20009697, March 28, 2015

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 767-A4.

Pumper, M. A., Yaeger, J. P., & Moreno, M. A. (2013). Perceptions and use of social networking sites in the United States and Ecuador: A mixed-methods approach. *College Student Journal, 47*(3), 478-484.

Purkait, S. (2012). Phishing counter measures and their effectiveness - literature review. *Information Management & Computer Security, 20*(5), 382-420. doi:http://dx.doi.org/10.1108/09685221211286548

Qing, H., Zhengchuan, X., Dinev, T., & Hong, L. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of The ACM, 54*(6), 54-60. doi:10.1145/1953122.1953142

Reed, P., Osborne, L., Romano, M., & Truzoli, R. (2015). Higher impulsivity after exposure to the internet for individuals with high but not low levels of self-reported problematic internet behaviours, *Computers in Human Behavior 49*, 512=516. doi: http://dx.doi.org/10.1016/j.chb.2015.03.064.

Reichman, H., Dawson, A., Garnar, M., Hoofnagle, C., Jaleel, R., Klinefelter, A., Nichols, J. (2014). Academic freedom and electronic communications. *Academe, 100*(4), 18-34.

Reno, J. (2013). Multifactor authentication: Its time has come. *Technology Innovation Management Review, 3*(8), 51-58.

Robertson, K., McNeill, L., Green, J., & Roberts, C. (2012). Illegal downloading, ethical concern, and illegal behavior. *Journal of Business Ethics, 108*(2), 215-227. doi:http://dx.doi.org/10.1007/s10551-011-1079-3

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(5), 93-114.

Ruhnka, J., & Loopesko, W. E. (2013). Risk management of email and internet use in the workplace. *The Journal of Digital Forensics, Security and Law, 8*(3), 7-19.

Salkind, N. J. (Ed.). (2010). *Encyclopedia of research design* (Vols. 1-3). Thousand Oaks, Calif: SAGE Publications, Inc.

Sauls, J., & Gudigantala, N. (2013). Preparing information systems (IS) graduates to meet the challenges of global IT security: Some suggestions. *Journal of Information Systems Education, 24*(1), 71-73.

Schuessler, J. H., & Hite, D. M. (2014). Pre-employment screening for security risk: An exploratory study. *The Journal of Applied Business and Economics, 16*(1), 84-95

Seda, L. (2014). Identity theft and university students: Do they know, do they care? *Journal of Financial Crime, 21*(4), 461.

Shropshire, J. D., Warkentin, M., & Johnston, A. C. (2010). Impact of negative message framing on security adoption. *The Journal of Computer Information Systems, 51*(1), 41-51.

Silic, M., & Back, A. (2014). Information security. *Information Management & Computer Security, 22*(3), 279-308.

Singh, N. A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management, 27*(5), 644-661.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-A12.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy & Security (Ivy League Publishing), 8*(4), 3-26.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security, 22*(1), 42-75. doi:http://dx.doi.org/10.1108/IMCS-08-2012-0045

Son, J. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302. DOI:10.1016/j.im.2011.07.002

Stanciu, V., & Tinca, A. (2014). A critical look on the student's internet use - an empirical study. *Accounting and Management Information Systems, 13*(4), 739-754.

Suki, N. M., Ramayah, T., Nee, A. S., & Suki, N. M. (2014). Consumer intention to use anti-spyware software: An application of structural equation modeling. *International Journal of Technology and Human Interaction, 10*(3), 19-31. doi:10.4018/ijthi.2014070102.

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems, 111*(4), 570-588. doi:http://dx.doi.org/10.1108/02635571111133551

Sykes, G., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review 22*(6), 664-670.

Symantec (2013). Internet security threat report. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

Szde, Y. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology, 8*(1), 36-46.

Tan, M., & Aguilar, K. S. (2012). An investigation of students' perception of bluetooth security. *Information Management & Computer Security, 20*(5), 364-381. doi:http://dx.doi.org/10.1108/09685221211286539

Taylor, R. G., & Robinson, S. L. (2014). The roles of positive and negative exemplars in information security strategy. Academy of Information & Management Sciences Journal, 17(2), 57-79.

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empirical study of students' computer security practices/perceptions. *Journal of Computer Information Systems, 47*(3), 105-110.

Tenable-Security (2012). Mobile device vulnerability management flagged as top concern for security professionals in 2012. Retrieved from http://www.tenable.com/press-releases/mobile-device-vulnerability-management-flagged-as-top-concern-for-security

Terry, M. (2015). HIPAA and your mobile devices. *Podiatry Management*, 99-104.

The Council of Australian Governments (2007). An agreement to a national identity security strategy. The Council of Australian Governments, Australia.

Trinkle, B. S., Crossler, R. E., & Warkentin, M. (2014). I'm game, are you? Reducing real-world security threats by managing employee activity in online social networks. *Journal of Information Systems, 28*(2), 307-327. doi:10.2308/isys-50776

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management, 52*(4), 506-517. doi:10.1016/j.im.2015.03.002

U.S. Department of Education FERPA Website (2015). Family education rights and privacy act of 1974. Retrieved from http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

U.S. Department of Education, National Center for Education Statistics (2014). *The Condition of Education 2014* (NCES 2014-083). Retrieved from http://nces.ed.gov/programs/coe/indicator_cbc.asp

U.S. Department of Health & Human Services (HHS) (1979). *The Belmont Report – Ethical Principles and guidelines for the Protection of Human Subjects of Research (1979).* Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html#, February 7, 2016.

Uffen, J., Kaemmerer, N., & Breitner, M. H. (2013). Personality traits and cognitive determinants-an empirical investigation of the use of smartphone security measures. *Journal of Information Security, 4*(4), 203-212.

Vance, A., Brinton Anderson, B., Brock 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*(10), 679-722.

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

Velmurugan, J. S., & Mathiyalagan, P. (2015). Social networking threats and security issues: An enquiry. *International Journal of Management Research and Reviews, 5*(4), 270-274.

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior, 27*(5), 751-1759. doi:10.1016/j.chb.2011.03.002

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal, 26*(2), 107-124. doi:http://dx.doi.org/10.1057/sj.2012.1

Walters, P. (2012). The risks of using portable devices. US-CERT. Retrieved from: http://www.us-cert.gov/reading_room/RisksOfPortableDevices.pdf

Wang, X., McClung, S. (2012). The immorality of illegal downloading: The role of anticipated guilt and general emotions. *Computers in Human Behavior, 28*(1), 153-159. doi:http://dx.doi.org/10.1016/j.chb.2011.08.021.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267-284. doi:http://dx.doi.org/10.1057/ejis.2010.72

Weeger, A., Wang, X., & Gewald, H. (2015). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *The Journal of Computer Information Systems, 56*(1), 1-10.

Weijters, B., Goedertier, F., & Verstreken, S. (2014). Online music consumption in today's technological context: Putting the influence of ethics in perspective. *Journal of Business Ethics, 124*(4), 537-550. doi:http://dx.doi.org/10.1007/s10551-013-1892-y

Wenger, G. C. (1999). Advantages gained by combining qualitative and quantitative data in a longitudinal study. *Journal of Aging Studies, 13*(4) 369-376. doi:http://dx.doi.org/10.1016/S0890-4065(99)00015-8.

Whipple, E. C., Allgood, K. L., & Larue, E. M. (2012). Third-year medical students' knowledge of privacy and security issues concerning mobile devices. *Medical Teacher, 34*(8), e532-e548. doi:10.3109/0142159X.2012.670319

White, G. L., Hewitt, B., & Kruck, S. E., P. (2013). Incorporating global information security and assurance in I.S. education. *Journal of Information Systems Education, 24*(1), 11-16.

Wilkie, L., & Mensch, S. (2012). Wireless computing technology. *Global Education Journal, 2012*(3), 1-36.

Williams, J., Feild, C., & James, K. (2011). The effects of a social media policy on pharmacy students' Facebook security settings. *American Journal of Pharmaceutical Education, 75*(9), 1-177.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *The Review of Business Information Systems, 15*(3), 9-21.

Woodward, B., Imboden, T., & Martin, N. L. (2013). An undergraduate information security program: More than a curriculum. *Journal of Information Systems Education, 24*(1), 63-70.

Workman, M., Bommer, W., and Straub, D. (2008). Security lapses and the omission of information security measures: An empirical test of the threat control model, *Journal of Computers in Human Behavior*, 24(6), 2799-2816. DOI: 10.1016/j.chb.2008.04.005

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. *Group Decision and*

Negotiation, *19*(4), 391-416. doi:http://dx.doi.org/10.1007/s10726-009-9167-9

Wright, M. A., & Drozdenko, R. G. (2013). Implications of student perceptions regarding the disclosure of sensitive information. *Journal of Leadership, Accountability & Ethics*, *10*(3), 79-97.

Wroughton, J. R., McGowan, H. M., Weiss, L. V., & Cope, T. M. (2013). Exploring the role of context in students' understanding of sampling. *Statistics Education Research Journal*, *12*(2), 32-58.

Wu, H. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security*, *21*(5), 381-400. doi:http://dx.doi.org/10.1108/IMCS-12-2012-0068

Yang, F., & Wang, S. (2014). Students' perception toward personal information and privacy disclosure in E-learning. *TOJET : The Turkish Online Journal of Educational Technology*, *13*(1), 207-216.

Yaseen, Q., & Panda, B. (2012). Insider threat mitigation: Preventing unauthorized knowledge acquisition. *International Journal of Information Security*, *11*(4), 269-280. doi:http://dx.doi.org/10.1007/s10207-012-0165-6

Yoon, C., Hwang, J-W, & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407-415.

Yoon, C., Kim, H. (2013). Understanding computer security behavioral intention in the workplace. *Information Technology & People*, *26*(4), 401-419.

Appendices

Appendix A: Student Information Security Behaviors Questionnaire

Demographic/Categorical Questions

What is your gender? (M/F)

What is your ethnicity? (African-American, Asian, Caucasian, Native-American, Other)

What is your age in years? (nn)

What is your classification? (Freshman, Sophomore, Junior, Senior, Graduate student, Other)

What is your major? (Biological and health sciences, social sciences and languages, mathematical and technological sciences, education, fine arts and communication, business and accounting, Bible)

How many hours per day do you use a computer on average? (nn)

How many hours of information security training have you had? (nnn)

Have you been a victim of identity theft? (y, n, don't know)

Do you have a firewall installed on your personal computer? (y, n, yes, but not activated, don't know)

Do you participate in illegal downloading of music, videos, software, or other digital content? (y, n, don't know)

Survey Questions

All questions will be measured using a 7-point Likert scale (1-strongly disagree, 2-disagree, 3-somewhat disagree, 4-neither agree nor disagree, 5-somewhat agree, 6-agree, 7-strongly agree).

Information security	ISB1	I periodically check and erase viruses and malicious software	Yoon et al. (2012)
	ISB2	I immediately delete suspicious e-mails without	Yoon et al.

behaviors		reading them	(2012)
	ISB3	Under no circumstances would I ever tell anyone my ID or password	Yoon et al. (2012)
Behavioral intention	BI1	I will take precautions against information security violations	Workman et al. (2008)
	BI2	I will actively use security technologies to protect confidential information	Workman et al. (2008)
	BI3	I will never install unreliable software or ActiveX on my computer	Yoon et al. (2012)
Perceived vulnerability	PV1	There's a chance that my personal information has been disclosed due to hacking	Workman et al. (2008)
	PV2	The data on my computer is likely to be undermined by malicious software such as viruses	Workman et al. (2008)
Perceived severity	PS1	Losing data privacy as a result of hacking would be a serious problem for me	Woon et al. (2005)
	PS2	Having the data in my computer destroyed by malicious software such as viruses would be a serious problem for me	Woon et al. (2005)
Response efficacy	RE1	Using security technologies is effective for protecting confidential information	Workman et al. (2008)
	RE2	Taking preventive measures is effective for protecting my personal information	Workman et al. (2008)
	RE3	Enabling security measures on my computer is an effective way of preventing computer data from being damaged by malicious software such as viruses	Workman et al. (2008)
Response costs	RC1	Acquiring new security technology to protect confidential information is annoying	Yoon et al. (2012)
	RC2	Maintaining security procedures (such as changing the password regularly) to protect personal information is cumbersome	Yoon et al. (2012)
Self-efficacy	SE1	I am able to protect my personal information from external threats	Ng et al. (2009)
	SE2	I am able to protect the data on my computer from being damaged by external threats	Ng et al. (2009)
	SE3	I am capable of responding to malicious software such as viruses	Ng et al. (2009)
Subjective norm	SN1	If I actively use security technologies, most of the people who are important to me would approve	Yoon (2011)
	SN2	Most people who are important to me think it is a good idea to take preventive measures to protect personal information	Yoon (2011)
	SN3	My friends think computer security behavior is important	Yoon (2011)
Security habits	SB1	I should periodically remove viruses and malicious software	Limayem, Khalifa, & Chin, (2004)
	SB2	I automatically send suspicious e-mails to the recycle bin	Limayem et al. (2004)

Appendix B: Permissions

Sure but please cite the Limayem et al. article.

Good luck Alan.

Moez

Sent from my iPhone

On Apr 18, 2015, at 7:12 PM, Hughes, Alan <Ahughes@ABC.edu> wrote:

Dear Dr. Limayem,

Hello.

My name is Alan Hughes, and I teach information technology at ABC University in the US. I am working on a dissertation based on a replication of Dr. Yoon's study (Yoon, C., Hwang, J-W, & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407-415.) at my university. He used some items from your study (Limayem, M., Khalifa, M., and Chin, W. W. (2004). Factors motivating software piracy: A longitudinal study. *IEEE Transactions on Engineering Management*, 51(1), 414–425.), which I would also like to use.

Specifically, I would like to request permission to use these items from your original study:

Security habits	B1	I should periodically remove viruses and malicious software	Limayem, et al.(2004)
	B2	I automatically send suspicious e-mails to the recycle bin	Limayem, et al.(2004)

May I use these items in my study?

Thank you for your time and consideration,

Alan Hughes

ABC University

Sure, you have my permission.

_____

Michael Dee Workman, Ph.D.

Professor of Human Factors and Information Systems

Department of Computer Sciences and Cyber Security

College of Engineering

Florida Institute of Technology

http://www.fit.edu/faculty/profiles/profile.php?tracks=workmanm

---

From: Hughes, Alan [Ahughes@ABC.edu]

Sent: Saturday, April 18, 2015 4:41 PM

To: Michael Workman

Subject: request

Dear Dr. Workman,

My name is Alan Hughes and I teach information technology at ABC University, in [redacted]. I am working on a terminal degree, and hope to replicate a study by Dr. Choelho Yoon, who used some material from your article (Security lapses and the omission of information security measures: An empirical test of the threat control model, *Journal of Computers in Human Behavior*, 24(6), 2799-2816. DOI: 10.1016/j.chb.2008.04.005). May I have permission to use the instrument questions created by you (et al) and used by Dr. Yoon in his study?

Sincerely,

Alan Hughes

ABC University

Hi

Sure, go ahead as long as I am cited. Good Luck with the dissertation!

irene

On 4/19/2015 5:53 AM, Hughes, Alan wrote:

Dear Dr. Woon,

My name is Alan Hughes, and I teach information technology at ABC University in the US. I am working on a dissertation project, and would like to request permission to use some of the items that Dr. Choelho Yoon used in his 2012 study (which I am replicating). The items cited were in the following article:

Woon, I., Tan, G. W., and Low, R., (2005). A protection motivation theory approach to home wireless security, in proceedings of the 26th International Conference on Information Systems (ICIS). 367-380.

The items are:

Perceived severity	S1	Losing data privacy as a result of hacking would be a serious problem for me	Woon, et al. (2005)
	S2	Having the data in my computer destroyed by malicious software such as viruses would be a serious problem for me	Woon, et al. (2005)

May I used these survey items in my survey, which will replicate Yoon (Yoon, C., Hwang, J-W, & Kim, R. (2012). Exploring factors that influence students' behaviors in

information security. *Journal of Information Systems Education*, *23*(4), 407-415.) with slight modifications.

Thank you for your time and consideration,

Alan Hughes

ABC University

[redacted]

USA

From: 윤철호 [mailto:carlyoon@empas.com]

Sent: Friday, January 30, 2015 7:00 PM

To: Hughes, Alan

Subject: Re:RE: Re:request

Hughes,

1. You can use the Appendix as you said.

2. You and your colleagues can carry out the survey in the class.

Best regards,

Cheolho

------ Original Message ------

Date: Friday, Jan 30, 2015 11:57:28 PM

From: "Hughes, AlanAhughes@ABC.edu>

To: "윤철호" <carlyoon@empas.com>

Cc: "hjw504@kunsan.ac.kr" <hjw504@kunsan.ac.kr>, "rhkim@ucr.edu" <rhkim@ucr.edu>

Subject: RE: Re:request

Hello again,

I am planning to replicate (slightly modified) your "Exploring Factors That Influence Students' Behaviors in Information Security" as published in the Journal of Information Systems Education, Vol 23(4), 2012, at my university in the US. I and my statistics advisor like the methodology you used, and would like to follow it, perhaps with an additional analysis method.

Would it be possible for me to get the questionnaire and permission to use it so that we can go over it and make any necessary adjustments? Or is that what is in the Appendix to the paper, with the constructs on the left, codes, statements, and source on the right, and using the 7-point Likert scale from "strongly disagree" (1?) to "Strongly agree" (7?)?

And, could you share with me how you got so many students to respond, considering the time it must take to answer the survey?

Any help you can give me would be appreciated as I pursue my doctoral degree.

Thanks,

Alan Hughes

Dear Alan,

Yes, you may use the items.

Regards,

Boon Yuen

From: Hughes, Alan <Ahughes@ABC.edu>

Sent: Wednesday, April 22, 2015 12:51 AM

To: Ng Boon Yuen

Subject: FW: request

Dr. Ng,

Hello. My name is Alan Hughes, and I teach information technology at ABC University in the US. I am working on a dissertation based on a replication of Dr. Yoon's study (Yoon, C., Hwang, J-W, & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education, 23*(4), 407-415.) at my university. He used some items from your study (Ng, B.Y., Kankanhalli, A., and Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems,* 46(4), 815-825.), which I would also like to use.

Specifically, I would like to request permission to use these items from your original study:

Self-efficacy	E1	I am able to protect my personal information from external threats	Ng, Kankanhalli, & Xu (2009)
	E2	I am able to protect the data on my computer from being damaged by external threats	Ng, et al. (2009)
	E3	I am capable of responding to malicious software such as viruses	Ng, et al. (2009)

May I use these in my replication study?

Thank you for your time and consideration,

Alan Hughes

ABC University

Appendix C: Informed Consent Letter

Introduction:

My name is Alan Hughes. I am a doctoral student at Northcentral University. I am conducting a research study on computer and information security attitudes and behaviors of college students. I am completing this research as part of my doctoral degree. I invite you to participate.

Activities:

If you participate in this research, you will be asked to:

1. Answer some questions about yourself, such as your gender, age, classification, major, etc.
2. Answer some questions about your information security behaviors.

Eligibility:

You are eligible to participate in this research if you:

1. Are a student enrolled in an on-campus degree program at ABC University, including graduate and undergraduate students.
2. Are age 18 or older.

You are not eligible to participate in this research if you:

1. Are not a student enrolled in an on-campus degree program at ABC University.
2. Are under 18 years of age.

I hope to include at least 231 participants in this research.

Risks:

There are minimal risks in this study. Some possible risks include exposure of your answers with your email address (which will be required for the cash award drawing). The researcher will not see your email address at any time. The drawing will be conducted by an individual from the ABC University Office of Planning, Research, and Assessment.

To decrease the impact of these risks, you can stop participation at any time.

Benefits:

If you decide to participate, there are no direct guaranteed benefits to you. However, a drawing will be held for five cash prizes of $100, $50, $50, $25, and $25. The survey link will be emailed to approximately 2,600 students, resulting in a 1 in 520 chance of winning a prize.

The potential benefits to others are that the results may be of benefit to universities who wish to gain an understanding of student information security attitudes and behaviors. This information may also help universities develop training courses to help students maintain a higher level of information security.

Confidentiality:

The information you provide will be kept confidential to the extent allowable by law. Some steps I will take to keep your identity confidential are: your email address will be kept separate from your data, and I will not ask for your name. The presentation of the findings will not disclose the name of the participating institution.

The people who will have access to your information are myself, my dissertation chair, my dissertation committee, and the Office of Planning, Research, and Assessment of ABC University. The North Central University Institutional Review Board may also review my research and view your information.

I will secure your information with these steps: encrypting your information on my computer; keeping printed copies in a secure place; keeping your email address separate from your answers.

I will keep your data for 7 years. Then, I will delete electronic data and destroy paper data.

Contact Information:

If you have questions for me, you can contact me at A.Hughes8897@email.ncu.edu, or at (864) 906-1024

My dissertation chair's name is Dr. Gregory Caicco. He works at Northcentral University, and is supervising me on the research. You can contact him at gcaicco@ncu.edu, (928) 541-8254.

If you have questions about your rights in the research, or if a problem has occurred, or if you are injured during your participation, please contact the Institutional Review Board at irb@ncu.edu or 1-888-327-2877 ext. 8014.

Voluntary Participation:

Your participation is voluntary. If you decide not to participate, or if you stop participation after you start, there will be no penalty to you. You will not lose any benefit to which you are otherwise entitled. However, you will not be eligible for the cash prize drawing.

Termination of Participation:

If you decide to stop participation, you may do so by closing the survey browser session. If so, I will not use the information I gathered from you.

Electronic Signature:

Clicking the “I consent” radio button below indicates that you are at least 18 years old, you are a student at ABC University, and you give your consent to participate in this study.

Clicking the “I do not consent” radio button below indicates that you are either not at least 18 years old, not a student at ABC University, or otherwise do not give your consent to participate in the study.

O I consent

O I do not consent

Appendix D: MANOVA Results – Academic Major, SASS, SBSS

Multiple Comparisons – Tukey HSD

Dependent Variable	(I) Major	(J) Major	Mean Diff. (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
SASS	Bible, ministry, missions	Business	.49	1.187	1.000	-3.02	4.00
		Education	-.01	1.198	1.000	-3.55	3.53
		Fine arts and communication	-.37	1.077	1.000	-3.56	2.81
		Mathematical, technological sciences	-2.05	1.183	.596	-5.55	1.45
		Natural and health sciences	-.57	1.030	.998	-3.61	2.48
		Social sciences and languages	-.95	1.172	.984	-4.42	2.51
	Business	Bible, ministry, missions	-.49	1.187	1.000	-4.00	3.02
		Education	-.50	1.212	1.000	-4.08	3.09
		Fine arts and communication	-.86	1.093	.986	-4.09	2.37
		Mathematical, technological sciences	-2.54	1.197	.343	-6.08	1.00
		Natural and health sciences	-1.06	1.046	.952	-4.15	2.04
		Social sciences and languages	-1.44	1.187	.888	-4.95	2.07
	Education	Bible, ministry, missions	.01	1.198	1.000	-3.53	3.55
		Business	.50	1.212	1.000	-3.09	4.08
		Fine arts and communication	-.36	1.105	1.000	-3.63	2.91
		Mathematical, technological sciences	-2.04	1.208	.626	-5.61	1.54

	Natural and health sciences	-.56	1.059	.998	-3.69	2.58
	Social sciences and languages	-.94	1.198	.986	-4.49	2.60
Fine arts and communication	Bible, ministry, missions	.37	1.077	1.000	-2.81	3.56
	Business	.86	1.093	.986	-2.37	4.09
	Education	.36	1.105	1.000	-2.91	3.63
	Mathematical, technological sciences	-1.68	1.089	.721	-4.90	1.54
	Natural and health sciences	-.20	.920	1.000	-2.92	2.53
	Social sciences and languages	-.58	1.077	.998	-3.77	2.60
Mathematical, technological sciences	Bible, ministry, missions	2.05	1.183	.596	-1.45	5.55
	Business	2.54	1.197	.343	-1.00	6.08
	Education	2.04	1.208	.626	-1.54	5.61
	Fine arts and communication	1.68	1.089	.721	-1.54	4.90
	Natural and health sciences	1.48	1.042	.791	-1.60	4.56
	Social sciences and languages	1.09	1.183	.969	-2.40	4.59
Natural and health sciences	Bible, ministry, missions	.57	1.030	.998	-2.48	3.61
	Business	1.06	1.046	.952	-2.04	4.15
	Education	.56	1.059	.998	-2.58	3.69
	Fine arts and communication	.20	.920	1.000	-2.53	2.92
	Mathematical, technological sciences	-1.48	1.042	.791	-4.56	1.60
	Social sciences and languages	-.39	1.030	1.000	-3.43	2.66
Social sciences and languages	Bible, ministry, missions	.95	1.172	.984	-2.51	4.42
	Business	1.44	1.187	.888	-2.07	4.95

		Education	.94	1.198	.986	-2.60	4.49
		Fine arts and communication	.58	1.077	.998	-2.60	3.77
		Mathematical, technological sciences	-1.09	1.183	.969	-4.59	2.40
		Natural and health sciences	.39	1.030	1.000	-2.66	3.43
SBSS	Bible, ministry, missions	Business	.33	1.072	1.000	-2.84	3.50
		Education	.19	1.082	1.000	-3.01	3.39
		Fine arts and communication	.00	.973	1.000	-2.87	2.88
		Mathematical, technological sciences	-2.79	1.069	.124	-5.95	.37
		Natural and health sciences	-.15	.931	1.000	-2.90	2.60
		Social sciences and languages	-.38	1.059	1.000	-3.52	2.75
	Business	Bible, ministry, missions	-.33	1.072	1.000	-3.50	2.84
		Education	-.14	1.095	1.000	-3.38	3.10
		Fine arts and communication	-.32	.987	1.000	-3.24	2.59
		Mathematical, technological sciences	-3.12	1.082	.061	-6.32	.08
		Natural and health sciences	-.48	.945	.999	-3.27	2.32
		Social sciences and languages	-.71	1.072	.994	-3.88	2.46
	Education	Bible, ministry, missions	-.19	1.082	1.000	-3.39	3.01
		Business	.14	1.095	1.000	-3.10	3.38
		Fine arts and communication	-.19	.998	1.000	-3.14	2.76
		Mathematical, technological sciences	-2.98	1.092	.092	-6.21	.24

	Natural and health sciences	-.34	.957	1.000	-3.17	2.49
	Social sciences and languages	-.58	1.082	.998	-3.78	2.63
Fine arts and communication	Bible, ministry, missions	.00	.973	1.000	-2.88	2.87
	Business	.32	.987	1.000	-2.59	3.24
	Education	.19	.998	1.000	-2.76	3.14
	Mathematical, technological sciences	-2.80	.984	.069	-5.70	.11
	Natural and health sciences	-.15	.831	1.000	-2.61	2.30
	Social sciences and languages	-.39	.973	1.000	-3.26	2.49
Mathematical, technological sciences	Bible, ministry, missions	2.79	1.069	.124	-.37	5.95
	Business	3.12	1.082	.061	-.08	6.32
	Education	2.98	1.092	.092	-.24	6.21
	Fine arts and communication	2.80	.984	.069	-.11	5.70
	Natural and health sciences	2.64	.942	.076	-.14	5.43
	Social sciences and languages	2.41	1.069	.268	-.75	5.57
Natural and health sciences	Bible, ministry, missions	.15	.931	1.000	-2.60	2.90
	Business	.48	.945	.999	-2.32	3.27
	Education	.34	.957	1.000	-2.49	3.17
	Fine arts and communication	.15	.831	1.000	-2.30	2.61
	Mathematical, technological sciences	-2.64	.942	.076	-5.43	.14
	Social sciences and languages	-.23	.931	1.000	-2.99	2.52
Social sciences and languages	Bible, ministry, missions	.38	1.059	1.000	-2.75	3.52
	Business	.71	1.072	.994	-2.46	3.88

	Education	.58	1.082	.998	-2.63	3.78
	Fine arts and communication	.39	.973	1.000	-2.49	3.26
	Mathematical, technological sciences	-2.41	1.069	.268	-5.57	.75
	Natural and health sciences	.23	.931	1.000	-2.52	2.99

Based on observed means.

The error term is Mean Square(Error) = 48.249.

Appendix E: MANOVA Results – Security Training Hours, SASS, SBSS

Multiple Comparisons – Tukey HSD

Dependent Variable	(I) STH Groups	(J) STH Groups	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
SASS	0-5 hours	11-20 hours	-4.25	2.574	.565	-11.61	3.11
		21-30 hours	-8.03	4.439	.461	-20.71	4.66
		31-50 hours	.93	2.728	.999	-6.87	8.73
		51+ hours	-1.57	2.728	.993	-9.37	6.23
		6-10 hours	-2.52	1.884	.765	-7.90	2.87
	11-20 hours	0-5 hours	4.25	2.574	.565	-3.11	11.61
		21-30 hours	-3.78	5.113	.977	-18.39	10.84
		31-50 hours	5.18	3.727	.733	-5.47	15.83
		51+ hours	2.68	3.727	.980	-7.97	13.33
		6-10 hours	1.73	3.162	.994	-7.30	10.77
	21-30 hours	0-5 hours	8.03	4.439	.461	-4.66	20.71
		11-20 hours	3.78	5.113	.977	-10.84	18.39
		31-50 hours	8.96	5.193	.516	-5.88	23.80
		51+ hours	6.46	5.193	.815	-8.38	21.30
		6-10 hours	5.51	4.803	.861	-8.22	19.24
	31-50 hours	0-5 hours	-.93	2.728	.999	-8.73	6.87
		11-20 hours	-5.18	3.727	.733	-15.83	5.47
		21-30 hours	-8.96	5.193	.516	-23.80	5.88
		51+ hours	-2.50	3.835	.987	-13.46	8.46
		6-10 hours	-3.45	3.289	.901	-12.85	5.95
	51+ hours	0-5 hours	1.57	2.728	.993	-6.23	9.37
		11-20 hours	-2.68	3.727	.980	-13.33	7.97
		21-30 hours	-6.46	5.193	.815	-21.30	8.38
		31-50 hours	2.50	3.835	.987	-8.46	13.46
		6-10 hours	-.95	3.289	1.000	-10.35	8.45
	6-10 hours	0-5 hours	2.52	1.884	.765	-2.87	7.90
		11-20 hours	-1.73	3.162	.994	-10.77	7.30
		21-30 hours	-5.51	4.803	.861	-19.24	8.22
		31-50 hours	3.45	3.289	.901	-5.95	12.85
		51+ hours	.95	3.289	1.000	-8.45	10.35

SBSS	0-5 hours	11-20 hours	-7.93*	2.306	.008	-14.52	-1.34
		21-30 hours	-6.37	3.975	.597	-17.73	4.99
		31-50 hours	-1.33	2.444	.994	-8.31	5.65
		51+ hours	-6.08	2.444	.129	-13.06	.90
		6-10 hours	-4.53	1.688	.080	-9.35	.29
	11-20 hours	0-5 hours	7.93*	2.306	.008	1.34	14.52
		21-30 hours	1.56	4.580	.999	-11.53	14.64
		31-50 hours	6.60	3.338	.357	-2.94	16.14
		51+ hours	1.85	3.338	.994	-7.69	11.39
		6-10 hours	3.40	2.832	.837	-4.69	11.49
	21-30 hours	0-5 hours	6.37	3.975	.597	-4.99	17.73
		11-20 hours	-1.56	4.580	.999	-14.64	11.53
		31-50 hours	5.04	4.651	.888	-8.25	18.33
		51+ hours	.29	4.651	1.000	-13.00	13.58
		6-10 hours	1.84	4.302	.998	-10.45	14.14
	31-50 hours	0-5 hours	1.33	2.444	.994	-5.65	8.31
		11-20 hours	-6.60	3.338	.357	-16.14	2.94
		21-30 hours	-5.04	4.651	.888	-18.33	8.25
		51+ hours	-4.75	3.435	.737	-14.57	5.07
		6-10 hours	-3.20	2.945	.887	-11.62	5.22
	51+ hours	0-5 hours	6.08	2.444	.129	-.90	13.06
		11-20 hours	-1.85	3.338	.994	-11.39	7.69
		21-30 hours	-.29	4.651	1.000	-13.58	13.00
		31-50 hours	4.75	3.435	.737	-5.07	14.57
		6-10 hours	1.55	2.945	.995	-6.87	9.97
	6-10 hours	0-5 hours	4.53	1.688	.080	-.29	9.35
		11-20 hours	-3.40	2.832	.837	-11.49	4.69
		21-30 hours	-1.84	4.302	.998	-14.14	10.45
		31-50 hours	3.20	2.945	.887	-5.22	11.62
		51+ hours	-1.55	2.945	.995	-9.97	6.87

Based on observed means.

The error term is Mean Square(Error) = 47.193.

*. The mean difference is significant at the .05 level.