2017

How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention

David Philip Johnson
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

David Johnson

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Timothy Perez, Committee Chairperson, Information Technology Faculty
Dr. Gail Miles, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control

Affects Information Security Behavior Intention

by

David P. Johnson

MS, Western Governors University, 2013

BS, Western Governors University, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2017

Abstract

The education sector is at high risk for information security (InfoSec) breaches and in need of improved security practices. Achieving data protections cannot be through technical means alone. Addressing the human behavior factor is required. Security education, training, and awareness (SETA) programs are an effective method of addressing human InfoSec behavior. Applying sociobehavioral theories to InfoSec research provides information to aid IT security program managers in developing improved SETA programs. The purpose of this correlational study was to examine through the theoretical lens of the theory of planned behavior (TPB) how attitude toward the behavior (ATT), subjective norm (SN), and perceived behavioral control (PBC) affected the intention of computer end users in a K-12 environment to follow InfoSec policy. Data collection was from 165 K-12 school administrators in Northeast Georgia using an online survey instrument. Data analysis occurred applying multiple linear regression and logistic regression. The TPB model accounted for 30.8% of the variance in intention to comply with InfoSec policies. SN was a significant predictor of intention in the model. ATT and PBC did not show to be significant. These findings suggest improvement to K-12 SETA programs can occur by addressing normative beliefs of the individual. The application of improved SETA programs by IT security program managers that incorporate the findings and recommendations of this study may lead to greater information security in K-12 school systems. More secure school systems can contribute to social change through improved information protection as well as increased freedoms and privacy for employees, students, the organization, and the community.

How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention

by

David P. Johnson

MS, Western Governors University, 2013

BS, Western Governors University, 2012

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2017

Dedication

I am dedicating this study to my wife, Cindy, and son, Ian. Without their unwavering encouragement, love, patience, understanding, and support this accomplishment would not be possible. The drive, commitment, strength, and tenacity they exhibit every day in meeting their own challenges provides me with the strength and motivation to meet my own.

Cindy, your grace and strength is amazing and I stand in awe of you every day. You inspire me. Ian, your heart, mind, and will are all remarkably strong. The joy and success they will bring you is only matched by how tremendously proud I am of you. I am forever humbled and grateful for all you both do.

It is my sincere hope that I can return the same love and support to empower you both so you too may accomplish all of your life's dreams. It is my desire to enable you to explore and learn until your head, heart, and soul are rich and full. Most of all, I wish for you the same life of happiness, love, and joy that you have given me.

Acknowledgments

I would like to acknowledge and thank Dr. Wendy Burns, Dr. Tom Kana, Dr. Kim Love, Dr. Barbara Martin, Dr. Jillian Skelton, Dr. Gary Torkington, Dr. Marie Underwood, and Dr. Christopher Wells. You each provided me with guidance, inspiration, and encouragement that made this process much more manageable and this goal more obtainable. Thank you to Mr. Bryan Yancey and Mr. Timothy England for your patience and support without which this effort would have been longer and harder. I give a heartfelt thank you to my immediate and extended family members who have cheered my progress and encouraged my growth.

I would like to extend my appreciation to my committee members, Dr. Timothy Perez, Dr. Gail Miles, and Dr. Steven Case, for their guidance and direction. Thank you as well to all the other researchers that have gone before me and provided a base of knowledge on which I could build. Especially to those who so graciously, kindly, and unselfishly granted me rights to use their work as building blocks for my own without even knowing me. My gratitude goes to my study organization and those in it who so readily accepted and supported my work and me. The dedication of all recognized here to the pursuit of knowledge and learning is evident and appreciated.

There are many others, far too many to list, who in some big or small way provided me with endless sources of support, motivation, and encouragement. Know that it does not go forgotten. I recognize and appreciate you all.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Information security requires many elements to be successful in the organization such as asset identification, vulnerability and risk analysis, implementing effective security controls, and creating a security-minded workforce culture through security education, training, and awareness (SETA) campaigns (National Institute of Standards and Technology [NIST], 2015). Technical solutions alone are not sufficient as vulnerabilities are not only caused by technology but also by flawed policies, individual practices, incorrect assumptions, and managerial decisions (Ahmad, Maynard, & Park, 2014; Da Veiga & Martins, 2015a; Flores, Antonsen, & Ekstedt, 2014; Safa, Von Solms, & Furnell, 2016). End users often engage in risky behavior and represent the weakest link in information security (Cox, 2012; Ifinedo, 2012). Information security program managers generally understand technical security controls; however, they often struggle to develop effective SETA campaigns (Herath & Rao, 2009). It is important to understand the effectiveness of information security communications and policies, the existing security culture, and how individuals react in response to these policies to improve SETA (Ashenden & Sasse, 2013; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015; Wilson & Hash, 2003).

Background of the Problem

Information security is a regular topic of research due to the growing number of data breaches that threaten to expose private information (Kumar & Kumar, 2014). A major data breach can prove costly for individuals facing identity theft and organizations in the loss of assets, reputation, legal fees, and mitigation costs (Romanosky, Hoffman, &

Acquisti, 2014). The education sector is a major target for attack (Misenheimer, 2014; Romanosky et al., 2014). Since 2005 educational institutions have experienced the second highest number of information security breaches with 14.8 million records compromised (Privacy Rights Clearinghouse, 2016). The 1,247,812 records breached in the U.S. education sector in 2014 had a per capita cost of $140 resulting in losses of $17.5M (Identity Theft Resource Center, 2014; Ponemon Institute, 2015).

As information security has matured, the industry has made great strides in improving technical security controls (Lin, Ke, & Tsai, 2015; Şimşek, 2015; Wu, Lei, Yao, Wang, & Musa, 2013). However, the weakest link in the information security chain is not technology but computer end users (Crossler et al., 2013). Actions by employees in the form of negligence, maliciousness, and human error represented 54% of all information security incidents in 2014 (Ponemon Institute, 2015). Insider behavior is expected to continue to be the largest information security threat; however, organizations continue to neglect to focus on this area (Bartnes, Moe, & Heegaard, 2016; Experian, 2015; Montesdioca & Maçada, 2015; Posey, Roberts, & Lowry, 2015).

A trend in information security research is to study behaviors of end users (Crossler et al., 2013) so information security program managers can implement multilayered solutions that include addressing human reactions, behaviors, and motivators (Ahmad et al., 2014). Use of sociobehavioral theories has been effective in predicting information security compliant behavior (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Sommestad, Karlzén, & Hallberg, 2015) and providing data to improve SETA campaigns (Posey, Roberts, Lowry, & Hightower, 2014). Research applying these methods and theories to information security exists but is still in its early stages (Cox, 2012; Herath & Rao, 2009; Ifinedo, 2012). This section has provided the background to the problem; attention will now turn to the problem statement.

Problem Statement

Effective SETA programs are the key security control to protect against employee negligence, human errors, and malicious insiders although few organizations properly invest in the deployment of this control (Posey et al., 2015). Privileged computer users inside the organization are the cause of 70% of all information security incidents (Skorodumov, Skorodumova, & Matronina, 2015). The general IT problem is that some IT security program managers lack knowledge of what motivational factors affect the intention to follow information security policy in order to develop a SETA program to mitigate human behavior risks. The specific IT problem is that some IT security program managers in Bigg County Public Schools lack knowledge on the relationship between attitude toward the behavior, subjective norm, perceived behavioral control, and intention to follow information security policy in order to develop a SETA program to mitigate the human behavior risks of computer end users in a K-12 environment.

Purpose Statement

The purpose of this quantitative correlational study was to examine how attitude toward the behavior, subjective norm, and perceived behavioral control affected the intention of computer end users in a K-12 environment to follow information security policy to provide IT security program managers sufficient knowledge to develop effective security controls in the form of SETA to protect against human behavior risks.

Surveying computer end users in the Bigg County Public School System located in Northeast Georgia provided data collection. This study applied the theory of planned behavior (TPB; Sommestad et al., 2015) to provide sufficient knowledge of how the constructs of this theory affect the information security behavior intentions of computer end users so that IT security program managers can develop effective SETA programs as a security control. Applying sociobehavioral theories to information security research is a current trend with researchers calling for further academic study (Crossler et al., 2013). The independent variables of this theory are attitude toward the behavior, subjective norm, and perceived behavioral control. The dependent variable is intention. The implications for social change include the possibility for development of effective information security controls and improvement of data security protections for the employees and vulnerable student population of K-12 schools.

Nature of the Study

The nature of this research was that of a quantitative correlational study. The formation and intention of a research question aids in defining the proper research design. Research asking *how* questions are best served by the exploratory nature of qualitative methodologies (R. K. Yin, 2014). Studies that seek to answer *what* or *how much* effect particular constructs have on a situation fit well with quantitative approaches (Fetters, Curry, & Creswell, 2013). In this study, I suggested the constructs of TPB are what have an effect on the information security behavior intentions of computer end users in a K-12 environment. I also sought to know the significance of the effect these constructs have on this intended behavior, thus a quantitative methodology was appropriate.

Alternative methodologies considered included qualitative and mixed method. Qualitative studies are generally exploratory and often attempt to discover a phenomenon, recount experiences, explore a culture, or establish a theory (Flick, 2015), none of which were a goal of this study. This combined with the fact that qualitative methodologies do not meet the paradigmatic view of a postpositivist at ontological and epistemological levels (Yilmaz, 2013) made a qualitative method the incorrect approach. Researchers should choose a mixed method approach when driven by a purpose that they cannot meet by providing attention to a single method such as the need or desire to identify and corroborate data to establish a new theory (Heyvaert, Maes, & Onghena, 2013; Venkatesh, Brown, & Bala, 2013). This was not a goal of this study. Mixed method can also exceed the limitations of time, budget, and skill sets of a single researcher (Yoshikawa, Weisner, Kalil, & Way, 2013), which made a mixed method approach not pragmatic for this doctoral study.

Quantitative studies show a relationship between variables and typically follow a correlational, quasi-experimental, or experimental design (Tavakol & Sandars, 2014a). Correlational design is used to descriptively demonstrate, through the analysis of evidence gathered, if there is a relationship between independent and dependent variables (Goertz & Mahoney, 2013). In this study, I approached the constructs of TPB as correlational in the desire to establish statistically how much the independent variables affected the dependent variable of intention. Experimental and quasi-experimental designs show causation (Yoshikawa et al., 2013). The researcher must apply a treatment to a preferably random sample population and generally involve multiple data gathering cycles (Bettany-Saltikov & Whittaker, 2014; Tavakol & Sandars, 2014a). None of these goals or conditions existed in this study, thus experimental designs were inappropriate. I also recognized that other factors in addition to TPB could influence information security behavior intentions, which further prevented a demonstration of causation and precluded the use of experimental methods. The study was cross-sectional, as data gathering only occurred at a single point in time.

Quantitative Research Question

RQ: To what extent does attitude toward the behavior, subjective norm, and perceived behavioral control affect the intention of computer end users in a K-12 environment in the Bigg County Public School System located in Northeast Georgia to follow information security policy?

Hypotheses

Formation of the hypotheses for this study occurred based on the constructs exhibited in the study framework and research model. I used data analysis to determine the correlation of these constructs in order to accept or reject the null hypothesis. The specific hypotheses for this study were:

$H1_0$: Attitude toward the behavior, subjective norm, and perceived behavioral control does not affect the intention of computer end users in a K-12 environment to follow information security policy.

$H1_a$: Attitude toward the behavior, subjective norm, and perceived behavioral control does affect the intention of computer end users in a K-12 environment to follow information security policy.

Theoretical Framework

In this study, I examined attitude toward the behavior, subjective norm, and perceived behavioral control to test TPB (Ajzen, 1985) in predicting the information security behavior intentions of computer end users in a K-12 environment. The selected theoretical foundation for this study was TPB. TPB is the predominant theory applied to information security research involving sociobehavioral theories in the extant literature (Lebek et al., 2014). The independent variables of TPB are attitude toward the behavior, subjective norm, and perceived behavioral control. The dependent variable is intention. Researchers have shown that TPB provides sufficient knowledge of motivational factors that affect information security behavior intentions (Sommestad et al., 2015). As applied to this study, I expected that TPB would provide sufficient knowledge of the motivational factors of K-12 computer end users to allow IT security program managers to develop and deploy effective human behavior security controls in the form of SETA. Figure 1 shows the research model.

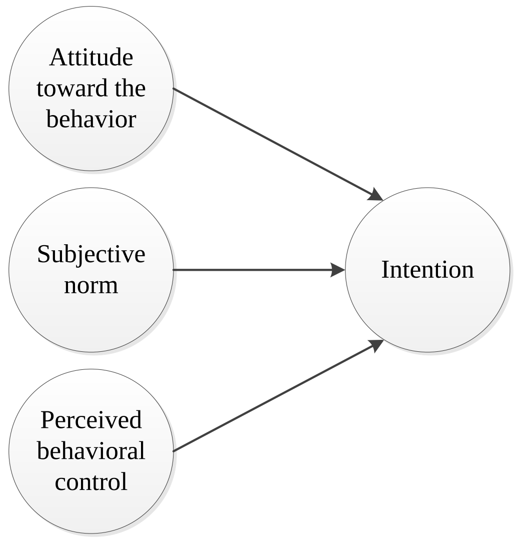

Figure 1. Research model based on the theory of planned behavior.

Definition of Terms

The following terms have specific meaning in the context of information security, behavioral theory, and/or this research study.

Information security: Information security refers to protective measures and actions taken to assure the confidentiality, integrity, and availability of electronic data and information systems (NIST Joint Task Force, 2013).

Information security risk: An information security risk is a calculated measure of the likelihood of an event occurring that could negatively impact an information system or the data it contains (NIST Joint Task Force, 2013).

Information security threat: An information security threat is an event that has the potential to negatively impact an information system or the data it contains (NIST Joint Task Force, 2013).

Information security vulnerability: An information security vulnerability is a weakness in an information system that if exploited could expose or damage an information system or stored data (NIST Joint Task Force, 2013).

Information system: An information system is an electronic resource or collection of resources used in the storage, presentation, and transfer of data (NIST Joint Task Force, 2013).

Information system asset: An information system asset is an identified information system and/or electronic data set that has been deemed to be valuable to an organization (NIST Joint Task Force, 2013).

Security control: A security control is a safeguard put in place to protect an information system or the data it contains (NIST Joint Task Force, 2013).

Security education, training, and awareness (SETA): SETA refers to communications developed to teach computer end users on proper methods to protect information systems and data (Posey et al., 2015).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions in a research study are beliefs or positions the researcher takes for granted or holds true without absolute proof (Tavakol & Sandars, 2014a). There were some assumptions related to the study topic and purpose. The first was the assumption that information security program managers lack knowledge of TPB. Next was the assumption that information security program managers desire this information in order to improve SETA. Mitigation of these assumptions happened through the exhaustive literature review presented in this paper that substantiated the lack of this knowledge and the need to improve SETA.

The first general assumption of this study was that computer end users have past exposure to SETA in some manner. This exposure may occur through the actions of an organization or happen through the individual life experiences of the study participants (Shillair et al., 2015). Should the end users not have exposure to such information, the ability to measure intent to comply with information security is limited, as the expectation for the end user to comply with guidelines for which they have no knowledge is not valid. Mitigation of this assumption occurred through verification with the target organization that all individuals had signed documents stating they had reviewed the information security policies of the organization. The study survey also contained questioning to validate the participant's exposure to SETA campaigns.

The next general assumption of this study was that computer end users are able to think of and discuss their computer usage actions in terms of information security. It is possible that information security practices become habitual to end users and are not actions that they think of as occurring separately from normal operational practices (Shropshire, Warkentin, & Sharma, 2015). This could be the result of SETA or a practical understanding of correct and ethical behavior on the part of the end users (Shillair et al., 2015). As a mitigation, I formulated survey questions in a manner that reduced technical jargon and focused attention on the intent of the question and its related factor.

The third general assumption of this study was that computer end users are willing to discuss their information security behaviors honestly and openly. It is possible that end users would respond to information security questions in a manner deemed socially desirable instead of providing details of their actual thoughts or behaviors (Krumpal, 2013). This would introduce response bias (Krumpal, 2013) into the study limiting the credibility of the findings. Proper development of survey questions addressed response bias as well as did the use of proper survey techniques in regards to question order and protecting the anonymity of the respondent.

The final assumption of the study was that the views of the researcher would not influence the findings. Subjective bias can be introduced in a study if the researcher allows their perspectives or opinions to enter the analytical process (Tavakol & Sandars, 2014a). Mitigation for this bias occurred through the use of an Internet-based survey that provided direct contact separation from the population, the use of properly formed survey questions that focused on measuring the intended factors, and the use of the quantitative method that deploys statistical analysis to draw conclusions based only on the data presented.

Limitations

Limitations are issues that have the potential to threaten the internal validity of a study (Aguinis & Edwards, 2014). Several limitations existed for the study when generalizing or practically applying the study findings in a universal manner. First, SETA exposure could be different for each computer end user. SETA exposure occurs through formal communication and training at current and past employers, social information sharing, and engagement with information security elements in the environment (Shillair et al., 2015). Environmental exposure can occur through such experiences as public service and private industry campaigns created by governmental or financial institutions, use of information security software such as malware and virus controls, and news events citing identity theft or data breaches (Posey et al., 2014).

Another limitation was that other motivators for information security compliance could be at play beyond those outlined in TPB and the theoretical framework of this study. Quantitative studies are limited in scope to investigating the variables stated in the research model (Turner, Balmer, & Coverdale, 2013). In this study, I did not employ exploratory research techniques investigating other factors that could affect the end computer users' intent to comply with information security. These facts limit a researcher to only showing correlation between independent and dependent variables and not demonstrating causation (Aguinis & Edwards, 2014; Charlwood et al., 2014; Vaidyanathan et al., 2016).

Methodology limitations existed in the study. A cross-sectional study is one where a researcher collects data at a single point in time (Lebo & Weber, 2015). This study was a cross-sectional study. This means that the findings are limited to the thoughts and actions of the individuals surveyed and the current information security culture in which they operate. Information security training and culture can change over time (Crossler et al., 2013) and the thoughts and actions of individuals can change as they progress in their career, gain further education, or as moral standards change (D'Arcy & Greene, 2014; Warkentin, Johnston, Shropshire, & Barnett, 2016). The study also utilized self-reported data. Self-reported data could be biased (Workman, Bommer, & Straub, 2008) toward socially desirable responses (Krumpal, 2013). This study's literature review presents an in-depth discussion of the socially desirable responses topic.

Study limitations existed in the researched population and sample. The study findings may not be generalizable due to a focus on the field of education, which may be different from corporations or other organizations. The study was also limited to the study of K-12 school administrators as opposed to other staff, faculty, or students. Other groups may hold differing information security thoughts and beliefs and may be more motivated to comply with or do not intend to violate information security (Crossler et al., 2013). The size of the school system studied is also significantly larger than most K-12 systems, thus findings may not be consistent in typical K-12 schools systems.

Delimitations

Delimitations outline the boundaries of a study by identifying what actions a researcher will not perform as part of the study and aids the reader in understanding the scope of the research (Newman, Hitchcock, & Newman, 2015). The scope of this study was to research the information security compliance intentions of staff leaders in K-12 educational institutions that are part of the Bigg County Public School system located in Northeast Georgia. I did not provide study participants with monetary incentives to participate. This study was limited in scope to the education industry and did not include studying the information security behavior of faculty or staff. This research was further limited to the use of the independent variables of TPB. I did not intend to identify newly discovered variables or motivational factors for information security compliance or develop a new theory or framework.

Significance of the Study

Contribution to Information Technology Practice

The computer end user has been established in the current literature as one of the most significant information security risks to the organization (Alaskar, Vodanovich, & Shen, 2015; Crossler et al., 2013). The development and deployment of security controls to mitigate information security risks, including those of human behavior, is a required function of IT security program managers as outlined in information security industry standards such as ISO 27001, NIST 800-53, and NIST SP800-50 (Disterer, 2013; Galvez, Shackman, Guzman, & Ho, 2015; NIST, 2015; Wilson & Hash, 2003). The primary information security control to address end user computer risks is SETA programs (Wilson & Hash, 2003).

This research may benefit K-12 IT security program managers by providing a better understanding of how certain motivational factors affect the information security behavior intentions of their target audience, thus aiding these security professionals in the development of more effective information security controls in the form of improved SETA programs. Such controls should support the needs and requirements of the end users (Thapa & Harnesk, 2014). K-12 computer end users may benefit from this understanding through the consideration of these motivational factors when information security professionals develop SETA campaigns that result in requirements that better enable them to perform their job functions. Lastly, this research contributed to the existing body of knowledge by studying information security from an end user human behavior viewpoint. Researchers have identified the need for this research and made the call for it in extant information security literature (Siponen, Mahmood, & Pahnila, 2014).

Implications for Social Change

The education sector is a high-risk target for information security breaches (Okpamen, 2013; Pardo & Siemens, 2014). This high risk is due to poor information security habits, practices, and motivation (Chou & Chou, 2016). This study has implications for social change through the potential improvement of SETA programs as a control to protect the private information of a school system, its employees, and the vulnerable student population (Aldridge, 2014) of K-12 schools. SETA programs can change the moral beliefs of individuals (Pfleeger, Sasse, & Furnham, 2014), affect individual intentions to comply (Choi, Levy, & Hovav, 2013), and shape the culture of an organization (Ashenden & Sasse, 2013; D'Arcy & Greene, 2014; Karlsson, Astrom, & Karlsson, 2015) in regards to information security. The secure handling of computer data affects social change in the form of increased freedoms and privacy for individuals (DHS Privacy Office and the Office for Civil Rights and Civil Liberties, 2015).

A Review of the Professional and Academic Literature

Performing a critical review and analysis of the existing literature in the topic area of this study provided a historical foundation for building new research, contributing to the academic knowledge in the field, and providing practical and applicable information that contributes to the improved practice of information technology. In this study, I sought to apply the framework and constructs of TPB (Ajzen, 1985) in a quantitative correlational data analysis process specifically to answer the RQ: To what extent does attitude toward the behavior, subjective norm, and perceived behavioral control affect the intention of computer end users in a K-12 environment in the Bigg County Public School System located in Northeast Georgia to follow information security policy?

Gathering a wide range of information resources in the form of peer-reviewed journal articles, industry reports, and scholarly texts provided for an exhaustive literature review. The execution of searches using Internet search engines such as Google.com and Google Scholar (scholar.google.com) as well as academic databases and publishers such as EBSCO Host, Science Direct, and Emerald Insight allowed for obtaining these resources. Searches regarding the applicable theory, methodology, design, and subject matter aided in obtaining the resources needed to cover the range of subject matter related to this study. Examples of such searches were various combinations of keywords such as *theory of planned behavior, information security, compliance, K-12, education, grade school administrators, secondary schools, behavioral theories, motivational factors, quantitative, qualitative, research design,* and more.

Citations in discovered resources provided additional article leads and additional keywords used in new searches. I performed reverse searches in Google Scholar to discover more recent articles that cited an article I was reviewing. Recommendations for similar documents made by scholarly databases after reviewing articles provided additional content. Tricco et al. (2016) recommend repeating these processes until the researcher achieved a point of saturation where the search results no longer provided new and interesting details that would contribute to a study. This process of searching and chaining articles reached this saturation level and allowed for the compilation of a rich and exhaustive database of resources in each desired discussion area of this literature review. In total, I studied 157 sources for the literature review section of this proposal; 92% of these articles were peer-reviewed, and 89% were published in the past five years since June 2017 (see Appendix D for reference counts by year and source).

The research question posed in this study served as the basis for the development of the following hypotheses:

> $H1_0$: Attitude toward the behavior, subjective norm, and perceived behavioral control does not affect the intention of computer end users in a K-12 environment to follow information security policy.
>
> $H1_a$: Attitude toward the behavior, subjective norm, and perceived behavioral control does affect the intention of computer end users in a K-12 environment to follow information security policy.

Through the analysis of data gathered, it was possible to answer the research question by rejection or acceptance of the null hypothesis and thus fulfill the purpose of the study. The stated purpose of this study was to provide sufficient knowledge and practical information to IT security program managers regarding how attitude toward the behavior, subjective norm, and perceived behavioral control affect the intention of computer end users in a K-12 environment to follow information security policy that can be applied to the development and improvement of SETA programs as a control to protect against human behavior risks. To accomplish this goal, it became necessary to discuss more than the theoretical framework of the study.

I documented the literature review as follows to provide a rich, complex picture with substantial detail and insight. The first sections establish the computer end user as an information security risk, the effectiveness of technical and nontechnical security controls, and the effectiveness of SETA programs as a security control. Next is a review regarding the use of behavioral theories in information security research including an exhaustive look at TPB in this context. The following sections present motivational factors contributing to information security compliance in relation to TPB and other competing behavioral theories to provide a context in which to define and measure the independent constructs of TPB. I then focus the discussion on measurement approaches and research methodologies used in existing studies. Later sections show how this study filled gaps in the extant literature. The final section closes the literature review with a summarization of the existing body of research as it relates to this study and the pertinent information presented.

Computer End Users as a Security Threat

Some may be led to believe that security incidents are the result of Internet hackers, organized crime, and cyberespionage groups (PricewaterhouseCoopers (PwC), 2013); however 54% of security incidents in 2014 were the result of human error, negligence by employees and contractors, and other malicious insiders (Ponemon Institute, 2015). Computer end users represent the “weakest link” in information security by regularly engaging in risky behaviors that can threaten the confidentiality, integrity, and availability of an organization's data and systems (Alaskar et al., 2015). This has become a major concern of both organizations and researchers. A survey of managers indicated that human behavior, particularly human error, is the largest security vulnerability in their organizations (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2014). The beliefs and concerns of management mimic the results of empirical studies as evidenced by the 113 journal and conference papers published in the last decade (Lebek et al., 2014) that combine the study of end user information security actions and behavioral theories.

It is the actions of privileged computer users inside the organization that account for the majority of information security incidents (Soomro, Shah, & Ahmed, 2016; Verizon, 2015). Here the term "privileged computer users" is used to reference end users who are authorized and able to perform functions related to information security that an ordinary end user may not be able to perform (National Institute of Standards and Technology, 2015). A partial list of negative user actions that contribute to noncompliance are being mischievous, neglecting to follow proper security protocols, being resistant to policies, not having proper awareness to recognize security events, lacking knowledge of proper behaviors or preventative actions, or having an attitude of apathy toward security compliance (Safa et al., 2015, 2016). Behind each of these actions are behavioral motivators that must be understood by information security program managers to implement security controls that address the vulnerabilities presented by computer end users (Furman, Theofanos, Choong, & Stanton, 2012). In later sections of this review, I discuss these motivators further.

To understand the security risk of the end user, one needs to understand the nature and intentions behind their security-related behavior. Guo (2013) suggests that end users engage in four types of information security behavior: security assurance behavior, security compliant behavior, security risk-taking behavior, and security damaging behavior. These actions may be passive, volitional, or nonvolitional (Willison & Warkentin, 2013), and the intentions of end users may or may not be malicious (Barlow, Warkentin, Ormond, & Dennis, 2013; Gundu & Flowerday, 2013). Researchers have further categorized dysfunctional information security behaviors as being either intentional destruction, detrimental misuse, dangerous tinkering, or naive mistake (Djajadikerta, Roni, & Trireksani, 2015). Understanding the motivators of these behaviors is necessary to develop an effective approach to protecting organizational data (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

Some researchers believe that nonmalicious human error caused by a lack of awareness or naivety that their actions as an end user could place the organization at risk poses some of the greatest security concerns for organizations (Barlow et al., 2013; Parsons, McCormac, Pattinson, et al., 2014; Soomro et al., 2016). Many computer end users have a perception that they understand information security and are security aware; however, research has shown that there is a significant gap between the accuracy of their beliefs, perceptions, and actual knowledge (Furman et al., 2012). End users often demonstrate a lack of understanding of information security communications, the inability to define and recognize risk, and have insufficient knowledge for decision making regarding information security protective strategies (Furman et al., 2012; Rashid, Zakaria, & Zulhemay, 2013). This is often referred to as the information security "knowing/doing" gap (Cox, 2012; Workman et al., 2008). Gaps also exist between information security program managers and end users in understanding the end user's role, responsibilities, and actions in regards to information security (Bartnes et al., 2016; Posey et al., 2014).

End user reasons and justifications for taking information security risks are varied. End users will circumvent information security if it interferes with work productivity, for convenience, or to achieve end goals (Posey et al., 2014). Many individuals employ coping mechanisms to address or avoid information security while others justify noncompliant security actions in their minds by using neutralization techniques (D'Arcy, Herath, & Shoss, 2014). Some of these techniques involve denial of responsibility, denial of injury, or denial of a real victim (Willison & Warkentin, 2013). Others use the "metaphor of the ledger" where they believe they have performed enough good deeds to offset bad behavior, a "defense of necessity" claiming the action is required to obtain a goal or achieve a higher purpose, or believe their actions are less damaging than what others do (Barlow et al., 2013). Some end users experience security-related stress that can lead to moral disengagement or claims of ignorance (D'Arcy et al., 2014; Pham, El-Den, & Richardson, 2016). Still others make misconceptions regarding social norms in the form of pluralistic ignorance and false consensus (H. Chen & Li, 2014).

Additional motivators for information security decision making include job performance outcomes, workgroup expectations, and a perceived match with their own beliefs (Dinev & Hu, 2007). Some users believe that it is the job of others to protect organizational data and that those people are performing those protective tasks sufficiently (Posey et al., 2014). Farahmand & Spafford (2013) summarized these justifications in a triangle model representing pressure, opportunity, and rationalization at the points of a "fraud triangle" to encompass the range of explanations for noncompliant security behavior and aid in the understanding of information security risk-taking behavior. Those engaged in deploying information security controls need to understand these elements in order to improve SETA (Parsons, McCormac, Pattinson, et al., 2014).

Nontechnical Security Controls

Historically information security has primarily focused on automated technical solutions such as virus scanners, firewalls, and intrusion detection and prevention systems (IDS/IPS) (Ben-Asher & Gonzalez, 2015; Soomro et al., 2016). However, organizations do not universally implement or utilize these solutions, nor are these solutions sufficient in securing the enterprise (Cavusoglu, Cavusoglu, Son, & Benbasat, 2013; Such, Gouglidis, Knowles, Misra, & Rashid, 2016). The reasons they are not universally implemented fall into the four categories of financial, situational, cultural, and technological (Workman et al., 2008). Technical solutions prove to be insufficient when end users are presented with a risk action or event and do not have the required knowledge and skills to interpret technology prompts, identify threats, or respond properly in a manner to mitigate the threat (Bartnes et al., 2016; Kirlappos & Sasse, 2012).

Thinking of information security as only a technical issue has been shown to be a flawed perspective as the correct approach requires addressing information security as both a technical and behavioral matter (Posey et al., 2014). Vulnerabilities are not only caused by technical factors such as programming errors, malicious code, and technical failures but also by flawed policies, individual practices, incorrect assumptions, and managerial decisions (Ahmad et al., 2014; Da Veiga & Martins, 2015a; Flores et al., 2014; Safa et al., 2016). Information security success depends on the actions and awareness of end users, regardless of strong technical controls (D'Arcy & Greene, 2014; Soomro et al., 2016). This has led to a multilayered research approach to control the risk posed by end users by addressing human perceptions, reactions, behaviors, and motivators (Ahmad et al., 2014; Soomro et al., 2016).

The complexities of users and organizations make the implementation of controls to mitigate end user risk behavior difficult (Safa et al., 2016). Most risk practices focus on protection of information assets from functionalist and interpretive paradigms (Dhillon & Backhouse, 2001) where organizations impose rules and enforce security compliance (Thapa & Harnesk, 2014). Organizations typically achieve this through the use of formal controls such as policies and sanctions in a deterrence model (Cheng, Li, Li, Holm, & Zhai, 2013). However, research has shown that end users will still violate security controls when the attempt is to enforce compliance with policy (Barlow et al., 2013; Willison & Warkentin, 2013). The problem with this approach is it does not address the humanist perspective (Thapa & Harnesk, 2014) where users can be positive change agents and perform protection related behaviors if properly educated, developed, and motivated (Cavusoglu et al., 2013; Posey, Roberts, Lowry, Bennett, & Courtney, 2013). This is achieved through the implementation of informal, nontechnical information security controls such as culture, social norms, values, traditions, and SETA (Da Veiga & Martins, 2015b; Kolkowska & Dhillon, 2013; Michie & West, 2013) which have shown to be more effective preventives even when deterrence factors existed such as certainty of detection and punishment for noncompliant behavior (Cheng et al., 2013).

Security education and awareness training. Correlations have been drawn between information security knowledge and end user attitude toward information security compliance (Al-Alawi, Al-Kandari, & Abdel-Razek, 2016; Flores & Ekstedt, 2016; Lee, Lee, & Kim, 2016; Öğütçü, Testik, & Chouseinoglou, 2016; Parsons, McCormac, Butavicius, et al., 2014; Safa et al., 2016). There is a significant body of IT literature addressing the need for SETA to increase end user knowledge (Alhogail, 2015; D'Arcy et al., 2014; Da Veiga & Martins, 2015a; Dinev & Hu, 2007; Kearney & Kruger, 2016; Posey et al., 2013; Rashid et al., 2013). Implementation of SETA is a nontechnical information security control (Posey et al., 2014). SETA is a core tenant of IT security standards such as those proposed by organizations such as the National Institute of Standards and Technology (NIST; Wilson & Hash, 2003) and the International Organization for Standardization (ISO; Disterer, 2013). NIST 800-53 (NIST, 2015) places SETA development responsibility specifically with the information security program manager.

SETA programs seek to educate computer end users regarding the risks of privileged network usage and how to defend against the various attacks that will be presented to them (Gundu & Flowerday, 2013). Another benefit of SETA is to develop conscious care behavior where the end user thinks about information security and the consequences of their actions when working with a system (Ahlan, Lubis, & Lubis, 2015; Safa et al., 2015). Awareness is a key component in developing end user appreciation of the need for security, importance of issues such as information security, and is central to forming attitudes and behavior toward protective technologies (Dinev & Hu, 2007; Flores & Ekstedt, 2016; Hanus & Wu, 2016; Kearney & Kruger, 2016; Montesdioca & Maçada, 2015). Studies have shown that SETA can change the moral beliefs of end users in regards to information security (Pfleeger et al., 2014; Posey et al., 2015; Reece & Stahl, 2015) and that awareness directly affects intentions to comply with information security (Arachchilage, Love, & Beznosov, 2016; Choi et al., 2013; Ngoqo & Flowerday, 2015).

Information security training should address why compliance is important in order to affect end user awareness (Öğütçü et al., 2016; Posey et al., 2015) and not just convey knowledge about the expected behavior or action of the end user (Parsons, McCormac, Butavicius, et al., 2014; Reece & Stahl, 2015; Tsohou, Karyda, & Kokolakis, 2015). It should be noted that SETA requirements are not the same for all organizations and all users (Kajzer, Darcy, Crowell, Striegel, & Van Bruggen, 2014; Soomro et al., 2016). Programs must be developed that align with business goals (Allam, Flowerday, & Flowerday, 2014; Soomro et al., 2016), complement the other components of a comprehensive security program (Disterer, 2013; National Institute of Standards and Technology, 2015; Wilson & Hash, 2003), meet the functional needs of the end users

(Kajzer et al., 2014), and is well maintained over time (Flores et al., 2014; Warkentin et al., 2016).

The extant research exposes problems with the effectiveness of some SETA campaigns. Individuals who have received such training have demonstrated that they will still engage in risky behaviors (Arachchilage & Love, 2014; Arachchilage et al., 2016; Caputo, Pfleeger, Freeman, & Johnson, 2014; Dang-Pham & Pittayachawan, 2015; Kearney & Kruger, 2016; Kirlappos & Sasse, 2012; Komatsu, Takagi, & Takemura, 2013; Ngoqo & Flowerday, 2015) if they cannot identify the information security risk or if they can achieve another gain. Historically information security professionals have taken a technocratic/technocentric approach (Ashenden & Sasse, 2013; Reece & Stahl, 2015) to SETA. This approach involves technical personnel evaluating the information security risk in the organization and then telling the computer end user how to react, respond, and execute safe computing practices to potential information security threats. Research has shown this to be a less than effective approach (Tsohou, Karyda, & Kokolakis, 2015).

Instead, end user education should focus on how the end user can recognize threats, understand the risks, and demonstrate to end users that they are empowered to have an effect (Arachchilage & Love, 2014; Komatsu et al., 2013; Öğütçü et al., 2016). Furman et al. (2012) believe organizations can accomplish this through the use of mental models where users can relate technical issues to life experiences. Another approach that has been forwarded in the extant research is to understand the motivating factors that influence the information security compliance behavior of the end user and use this information to develop improved information security policy and SETA (Dinev & Hu, 2007; Komatsu et al., 2013; Tsohou, Karyda, & Kokolakis, 2015). Posey et al. (2014) illustrated that end users make decisions based on motivational drivers that organizations need to address in SETA programs.

SETA programs face challenges in the ability to measure their effectiveness in terms of communications, building a security conscious culture, or impacting actual information security compliance (Alhogail, 2015; Da Veiga & Martins, 2015a; Montesdioca & Maçada, 2015; Öğütçü et al., 2016; Tsohou, Karyda, Kokolakis, et al., 2015). Many organizations recognize SETA as an important need (Siponen et al., 2014) however it remains poorly invested in by some organizations (Farahmand & Spafford, 2013; Montesdioca & Maçada, 2015; Posey et al., 2015; Tsohou, Karyda, Kokolakis, et al., 2015). SETA is regarded as being of sufficient importance that President Obama launched a nationwide awareness program in the United States (Furman et al., 2012). The education sector suffers from a lack of perceived vulnerability (Kirlappos & Sasse, 2012), attitude, intention, and behavior related to information security, and SETA is the primary path to resolving these issues (Chou & Chou, 2016).

The drivers, knowledge, understanding, constraints, and beliefs of those receiving information security messages must be considered when developing effective SETA programs (Allam et al., 2014; Furman et al., 2012; Tsohou, Karyda, & Kokolakis, 2015). Achieving this consideration and understanding is through applying social and behavioral science to information security (Crossler et al., 2013; Dhillon & Backhouse, 2001; Thapa & Harnesk, 2014). Galvez et al. (2015) summarized the benefits of understanding end user information security compliance motivational factors and nontechnical controls in their study by stating: "The findings of this study could be used to develop effective security policies and training. They could also be used to develop effective security audits and further recommendations for organizations that are looking to make significant improvements in their information security profiles."

Social and Behavioral Theories in Information Security Research

Previous sections of this review document a body of resources that demonstrate the concern over end users and their behavior as being a significant source of information security risks. Human behavior is in the center of the information security “Human Factor Diamond” influenced by preparedness, management, responsibility, society, and regulations (Alhogail, 2015). Presentation of research demonstrating how the application of sociobehavioral science can be influential in changing behaviors has also occurred. Dhillon and Backhouse (2001) made the call to the academic community to begin investigation of end user security related behavior from socioorganizational perspectives to predict and drive compliant behavior. The academic community responded, and has since produced a body of work “borrowing” theories from other disciplines and applying them to information security. This borrowing approach is known as translational research (Drouin & Jugdev, 2014). The use of behavioral science, as well as sociological and psychological theories, has proven applicable and valid in determining and measuring end user intentions for information security compliance (Lebek et al., 2014). It has become a common trend in information security research to apply human behavioral theories (Crossler et al., 2013; Silic & Back, 2014). By applying theories from other areas such as psychology, sociology, behavioral science, and criminology, as well as business and organizational science, there now exists knowledge that aids in explaining and understanding the end computer users' intention to comply with information security guidelines and policies (Lebek et al., 2014). This information is then used to develop and improve more relevant and effective SETA (Galvez et al., 2015). Improving these nontechnical controls has been shown to increase the security posture of the organization (Shepherd & Mejias, 2016).

Theories such as rational choice theory, theory of planned behavior, and protection motivation theory are popular examples of theories "borrowed" from other disciplines and applied to information security (Lebek et al., 2014). These sociobehavioral theories have independent variables and/or observed measures representing various motivational factors (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014) believed to influence the end user's intention (Ajzen, 1985, 1991) to comply with information security rules (Siponen et al., 2014). Through broad and repeated application of behavioral theories in the study of various organizations (Crossler et al., 2013), we gain evidence and understanding of how these motivational factors effect end user compliance (Hu, Dinev, Hart, & Cooke, 2012; Wall, Palvia, & Lowry, 2013). How end users will react and respond to information security policies and communications can be better predicted and applied to improve nontechnical security controls, such as SETA, to achieve the goals of the organization (Allam et al., 2014; Soomro et al., 2016) and the end user (Thapa & Harnesk, 2014). In the following sections, I review competing theories and demonstrate how research can draw upon the motivational factors present in these theories as measures for the independent variables of TPB.

Competing social and behavioral theories. Researchers have applied many sociobehavioral theories to the study of end user information security compliance behavior. These theories include general deterrence theory, theory of reasoned action, rational choice theory, protection motivation theory, technology acceptance model, social learning/cognitive/constructivism theory, social bond theory, neutralization theory, causal reasoning theory, cognitive evaluation theory, health belief model, habit theory, rival explanations, innovation diffusion theory, and theory of planned behavior (Alaskar et al., 2015; Lebek et al., 2014). In research, these theories are generally applied in the context of predicting the end users' likelihood or intention (Fishbein & Ajzen, 1975) to comply with information security directives (Siponen et al., 2014). Intention is often the target as it is difficult to observe end user security behaviors in real time (Workman et al., 2008) and studies support the concept that intention is a valid predictor of actual behavior (Ajzen, 1985, 1991; Alaskar et al., 2015; Armitage & Conner, 2001; Lebek et al., 2014; Siponen et al., 2014). The intention of citing this fact here is to address the relative concept of how researchers apply these theories in the context of information security research instead of repeating this information in the content of the following individual theory discussions. The next sections outline these theories along with the motivational factors that makeup their framework.

General deterrence theory. General deterrence theory (GDT) comes from the study of criminology and is the second most applied theory in the research of end user information security compliance (Lebek et al., 2014). This theory consists of two motivational factors focused on punishment for noncompliance. The two factors are certainty of punishment and severity of punishment (H. Chen & Li, 2014). This theory suggests that individuals consider if they are caught performing an undesirable act how likely it is that they will receive punishment and how severe the punishment would be (Cheng et al., 2013). The individual compares these factors to the potential benefits gained from performing the act and decides to stop or move forward with the act. There were more motivational factors to consider in the target study environment, thus GDT was not appropriate for this study due to the limited focus on punishment.

Theory of reasoned action. The theory of reasoned action (TRA) is a theory borrowed from the field of psychology. Attitude toward the behavior and subjective norm (Siponen et al., 2014) are the two variables representing motivational factors in this theory. When applied to information security, the variable of attitude reflects the individuals' attitude toward compliance with information security. Researchers provide support for the attitude toward the behavior variable in the extant literature (Arpaci & Baloglu, 2016; Chatterjee, Sarker, & Valacich, 2015; Cox, 2012). Subjective norm refers to beliefs held by the individual regarding what they think those important to them expect (H. Chen & Li, 2014; Yazdanmehr & Wang, 2015). TRA has been proceeded by TPB to include nonvolitional acts through the independent construct of perceived behavioral control (Ajzen, 1991). This inclusion improved the predictability of intention (Sommestad et al., 2015) and made TPB a more suitable theory for this study.

Rational choice theory. Rational choice theory (RCT) is another theory coming from the field of criminology research and draws from the core concepts of GDT (Paternoster, Bachman, Bushway, Kerrison, & O'Connell, 2015). This theory suggests that individuals weigh the risks and benefits of an action before taking it (Dietrich & List, 2013). The motivational factors here are formal sanctions and informal sanctions (Shepherd & Mejias, 2016). Formal sanctions include established and defined penalties for certain acts, such as would exists in law or policy. Informal sanctions are undefined penalties that may exist in society such as shunning or considering someone of low character (Paternoster et al., 2015). RCT posits that individuals consider each of these motivational factors before committing an act (Dietrich & List, 2013) such as an information security violation. Although RCT would have been a valuable theory for this study, it does not compensate for the influence of others on the beliefs of the individual as TPB does through the inclusion of subjective norm. The potential presence of this influence in the study environment made TPB a more suitable fit.

Protection motivation theory. Protection motivation theory (PMT) is another popular theory in the field of information security compliance research (Alaskar et al., 2015). This theory began as a theory regarding fear appeals (Boss, Galletta, Lowry, Moody, & Polak, 2015) and has grown to a more generalized theory regarding persuasion especially in health benefits studies (Sommestad et al., 2015). The theory is comprised of motivational factors that fall into the category of threat appraisals or coping appraisals (Posey et al., 2015; Tsai et al., 2016). In the threat appraisals category are the variables of perceived vulnerability and perceived severity (Crossler, Long, Loraas, & Trinkle, 2014; Ifinedo, 2012). These speak to the individual's perception of how susceptible they are to a vulnerability and how severe the results of the vulnerability should it be realized (Arachchilage et al., 2016). The other category of coping appraisals consists of response cost, response efficacy, and self-efficacy (Crossler et al., 2014; Ifinedo, 2012). This addresses the individual's ability to take preventive action, how effective the action will be, and what effort level will be required (Posey et al., 2015; Sommestad et al., 2015). The motivational factors here are very similar in terminology and meaning to like terms in the field of information security; thus the relevant application of this theory to the field.

PMT is a primary competitor to TPB in the extant research but is also complementary in practice, and researchers often combine the two (Sommestad et al., 2015). Some researchers have recently challenged PMT as being insufficient due to antiquated fear appeals and lacking in consideration of harm to the computer end user (Johnston, Warkentin, & Siponen, 2015). This consideration is addressed in TPB through the subjective norm construct and related informal sanctions (Cheng et al., 2013). This made TPB a better theory for application in this study.

Technology acceptance model. The technology acceptance model (TAM) is another theory closely related to TRA and widely applied in information technology research (Mortenson & Vidgen, 2016). This theory solely uses the independent variable of attitude as the predictor of behavior intention with the same definition and meaning as in TRA. The difference is the use of the observed measures of perceived usefulness and perceived ease of use as motivational factors that influence attitude (Bagozzi & Yi, 2012). TAM was an unacceptable base theory for this study as focusing solely on attitude would be a limitation.

Social learning/cognitive/constructivism theory. Social cognitive theory (SCT) (previously known as social learning theory) is a psychological learning theory largely applied in health and behavioral studies (Shillair et al., 2015). This theory has three categories of variables related to expectancies from the environment, expectations of outcomes, and expectations of self-efficacy (Font, Garay, & Jones, 2016; Young, Plotnikoff, Collins, Callister, & Morgan, 2014). The overriding concept is that individuals at least partially develop behaviors based on influences from their social environment (Johnston et al., 2015; Paternoster et al., 2015). These motivational factors are demonstrated in information security compliance studies in examples such as encouragement by others, information security practices by others, instrumental support, self-efficacy in information security, and outcome expectations in information security (Galvez et al., 2015).

Constructivism is included here as another relevant learning model that largely addresses how we learn from our environment as well. Constructivism has been applied to information security behavior research (Ifinedo, 2014) although it is not a theory per se as it has no defined framework and variables. As opposed to other theories that do not consider environmental influences, the fact that this is the sole focus of SCT/constructivism is limiting by not taking into account individual beliefs as TPB does, and thus they were not complete enough approaches for this study.

Social bond theory. Another theory from the study of criminology used in information security behavioral research is social bond theory (SBT). SBT, originally developed to explain delinquency in adolescents and then extended to the behavior of adults in and outside organizations, uses the motivational factors of attachment, commitment, involvement, and belief (Cheng et al., 2013). Attachment, commitment, and involvement all relate to the individual's relationship to others and to organizations with the thought that the greater of each of these variables, the less likely the individual is to commit malicious behavior (Ifinedo, 2014). A better definition for belief in this context is moral belief (Cheng et al., 2013), and represents one's own thoughts of right and wrong just as in other theories. SBT may have been a suitable theory for application to studying this study's population and the motivational factors may have provided additional insight into other motivational factors. However, the extant literature does not show SBT as well founded at predicting information security behavior as TPB and thus was not the right fit for this study.

Neutralization theory. Neutralization is not a defined framework but a theory of justification for human actions. Neutralization is a trending topic included in the discussion of a significant number of information security behavioral studies (Barlow et al., 2013; H. Chen & Li, 2014; Crossler et al., 2013; D'Arcy et al., 2014; Hu et al., 2012; Kolkowska & Dhillon, 2013; Siponen et al., 2014; Sommestad et al., 2014). Neutralization is the justification of an action, in this case performing an act not in line with information security policy, through rationalization. Willison & Warkentin (2013) established a substantial list of techniques of neutralization that are relevant motivational factors for end user noncompliant information security behavior. Examples are end users justifying their actions by citing that the action is less severe than the actions of others, that they have performed a sufficient number of positive actions that offset the negative action, or that they are performing the noncompliant act in order to achieve a goal that is substantially more beneficial than the damage caused (the "greater good" argument) (Barlow et al., 2013). Neutralization is an interesting theory but does not provide a sufficiently established framework for a correlational study.

Causal reasoning theory. Causal reasoning theory explains human behavior in direct response to change actions in the individual's environment. In an information security context, this theory explains the computer abuse behavior taken by someone as a reaction to a change event (Lowry, Posey, Bennett, & Roberts, 2015). Causal reasoning theory proposes that one action is responsible for another action and thus demonstrates causation. Causation is a simplistic model, but one that can be difficult to substantiate as other influencing factors can drive behaviors, and it can be a challenge to show that the behavior would not have occurred without the preceding event (Bagozzi & Yi, 2012). Here, as with other theories, there are not specific motivational factors established in a predefined framework, but instead, the motivational factors are the causing action. This is relevant as information security professionals must understand and be able to identify actions in the organization that can be potential triggers for noncompliant behavior by computer end users. Causation is an approach more appropriate for experimental study design (Charlwood et al., 2014). Causal reasoning theory was not a good fit for this study due to an acknowledgment that other factors could influence intent beyond those evaluated in this study's theoretical model.

Cognitive evaluation theory. Cognitive evaluation theory generally addresses the single motivational factor of reward (Siponen et al., 2014). However, reward can come in various forms and for differing reasons. For example, rewards can be tangible or intangible. Feedback can be considered a reward (Farahmand, Atallah, & Spafford, 2013). Cognitive evaluation theory has shown that reward can be a negative or positive motivational factor depending on the expectancy and perception of the reward and feedback by the end user (Siponen et al., 2014). From an information security perspective, the reward can be a direct result of compliant computer behavior, or end users can react to rewards given (or withheld) in the business environment by performing positive or negative information security related activities (Farahmand et al., 2013). Reward is a valid motivational factor and one that I included as a measure in this study. However, implementation of this study based solely on cognitive evaluation theory would have been a limitation when compared to the broader scope provided by TPB.

Health belief model. The health belief model is another theory borrowed from the field of psychology and first applied in the healthcare literature (Montanaro & Bryan, 2014) and now extended to end user information security behavioral studies (Davinson & Sillence, 2014). This model's framework content is very similar to the constructs that represent motivational factors in PMT. Motivational factors include perceived susceptibility, perceived severity, perceived benefits, perceived barriers, cues to action, and self-efficacy (Bishop, Baker, Boyle, & MacKinnon, 2015; Montanaro & Bryan,

2014) and these constructs have the same meaning relative to information security as applied in other theories previously discussed. The health belief model motivational factors differing from PMT are perceived barriers and cues to action and both are relevant to information security. Perceived barriers represent factors individuals may see that are in the way of performing positive information security behaviors such as lack of knowledge or training. Cues to action suggest that some event must cue the individual to perform information security related behaviors (Davinson & Sillence, 2014). This theory was not appropriate for this study, as I did not seek to understand information security barriers or cues to action in the target environment.

Habit theory. Habit (or habit theory) is another motivational factor that appears regularly in the information security behavioral study literature (Chatterjee et al., 2015; D'Arcy et al., 2014; Siponen et al., 2014; Wall et al., 2013; Yoon & Kim, 2013). This theory is again a single variable theory being that of habit, defined as the performing of behaviors unconsciously due to regular repetition (Moody & Siponen, 2013; Tsai et al., 2016). There are two information security perspectives from which to view habit. One can be the goal to have positive compliant behavior performed as habit. Alternatively, it can be that end users' perform negative computer behavior due to the formation of habit (Shropshire et al., 2015). The application of a single variable theory would not have provided the breadth of insight required to address the research question in this study.

Rival explanations. Rival explanations is not a framework theory, but instead a theoretical perspective that should be included and applied in any research study (R. K. Yin, 2013). Rival explanations are simply alternate explanations for events. Rival explanations are what must be overcome to show causation (Henry, Smith, Kershaw, & Zulli, 2013). Examples of rival explanations from an information security perspective are organizational commitment, job satisfaction, certainty of sanction, severity of sanction, incentives, and management support (Lowry et al., 2015). Rival explanations were recognized points for consideration in this correlational study. However, due to a lack of formal framework, this was not an acceptable theoretical basis for this study.

Innovation diffusion theory. Innovation diffusion theory is an acceptance theory similar to TAM (Yoon & Kim, 2013). This theory consists of five motivational factors that the end user moves through during the acceptance process: knowledge, persuasion, decision, implementation, and confirmation (Doyle, Garrett, & Currie, 2014). This theory is related to information security compliance as it defines the process the end user must go through before acceptance of information security policies (Kim & Ammeter, 2014; Silic & Back, 2014). This is a relevant framework for the information security program manager to understand in the creation and implementation of SETA programs as they can address all of the motivational factors of this model in these campaigns (Kim, 2014). Innovation diffusion theory was not a good fit for this study as my desire was to identify motivational factors for information security compliance, not the diffusion of information security practices in a culture over time.

Theory of planned behavior. The theory of planned behavior (TPB) is an extension of TRA and developed by Ajzen (1985) who is one of the same individuals involved in the creation of TRA (Fishbein & Ajzen, 1975). Ajzen (1991) determined that there was a need to reflect perceived behavior control in the theoretical model to account for nonvolitional behaviors. This motivational factor describes the belief of an individual in their ability to perform the action in question (Ajzen, 2002). This variable is often defined as consisting of two observed measures, locus of control and self-efficacy (Ifinedo, 2014; Wall et al., 2013). These describe the individual's belief that they are in a position to perform the action and that they have the technical ability to do so (Cox, 2012). TPB has been shown to be an effective predictor of information security compliance intention (Sommestad et al., 2015) and is the most prevalent theory applied to the information security field (Lebek et al., 2014).

Theory review summary and selection for the proposed study. During preparation for performing research on what variables affect the information security behavioral intention of individuals it becomes necessary to develop a theoretical perspective. TPB (Ajzen, 1991) stands as an appropriate research framework for this subject. This theory is relevant as it focuses on the intent of the individual to perform a behavior as a predictor of the likelihood that they will enact the behavior (Ajzen, 1985). This theory goes beyond the incomplete TRA framework that only centers on perspective to account for behaviors (Ajzen, 1991; Fishbein & Ajzen, 1975). Other theories used to predict behavior such as PMT or TAM focus only on attitude and/or personality traits to determine if an individual would be likely to act in a particular manner and this too is incomplete. TPB posits intent to act in a certain manner may not be completely determined by an actor's attitude, perceptions, expectations, or traits but goes further to include perceived behavior control to account for situations that are beyond the volition of the actor (Ajzen, 1991). TPB comprises independent variables that can be defined and measured by motivational factors that may have a direct effect on the dependent construct of intention (Ajzen, 1991). The independent variables represented in TPB matched well with the research question and population of this study. TPB is also a well-established theory applied in many areas of study such as: accident analysis and prediction (Efrat & Shoham, 2013), environmental psychology (Chan & Bishop, 2013; de Leeuw, Valois, Ajzen, & Schmidt, 2015; Donald, Cooper, & Conchie, 2014; Greaves, Zibarras, & Stride, 2013), dietary nutrition (Dawson, Mullan, & Sainsbury, 2014; Mullan, Allom, Sainsbury, & Monds, 2015), health psychology (Michie & West, 2013), hospitality management (M. F. Chen & Tung, 2014), human behavior (I Ajzen & Klobas, 2013), nursing (Tipton, 2014), social psychology (Icek Ajzen & Sheikh, 2013), sports and exercise (Prapavessis, Gaston, & DeJesus, 2015), substance abuse (Zemore & Ajzen, 2014), and transportation (Castanier, Deroche, & Woodman, 2013). Discussion of the relevant findings of these studies occurs in following sections.

TPB is also a popular theory in studies that have the purpose of providing information for the development of interventions such as training or education programs (Ajzen & Klobas, 2013; Chan & Bishop, 2013; de Leeuw, Valois, Ajzen, & Schmidt, 2015; Greaves, Zibarras, & Stride, 2013; Mullan, Allom, Sainsbury, & Monds, 2015; Tipton, 2014). This intent fit well with this study, as the application was to provide information for SETA development. Based on the above arguments, recognition of TPB as a well-established predictor of behavioral intention (Sommestad et al., 2015), and consideration of the research question and study population I determined that the study topic variables were most similar to TPB and TPB was the more suitable theory for this study.

The constructs of TPB. The purpose of this section is to provide in-depth discussion and definition for the constructs of TPB as per the existing literature. Development of a clear understanding of these constructs both in general and their application in this study aims to aid in fully understanding the framework for the study. In the next sections, I discuss each independent and dependent variable from the perspective of the extant literature, followed by definitions of the constructs as specifically related to and applied in this study.

Attitude toward the behavior. Attitude toward the behavior (ATT) is the first of two constructs carried over from TRA. Ajzen (1991) defined this construct as the favorable or unfavorable appraisal an individual holds regarding a particular behavior. Salient behavioral beliefs of the individual influence this construct (Armitage & Conner, 2001). Individuals link these beliefs to particular outcomes of performing a behavior. The individual perceives these outcomes as positive or negative, and thus an attitude toward the behavior is established (Lee et al., 2016). Attitude has been shown to explain a significant amount of intended behavior (Arpaci & Baloglu, 2016; Flores & Ekstedt, 2016; Herath et al., 2014; Jafarkarimi, Saadatdoost, Sim, & Hee, 2016; Moody & Siponen, 2013; Safa et al., 2016) and can be influenced by training that seeks to modify this trait (Parsons, McCormac, Butavicius, et al., 2014) .

Attitude has a strong influence on intention in TPB (Ajzen, 1991). Ajzen supported this position well in his work, and the position is supported further by the fact that other theories center on this construct such as TAM (Bagozzi & Yi, 2012) and TRA (Fishbein & Ajzen, 1975). Lebek (2014) showed that eight of ten IT studies applying TPB demonstrated significant correlations between attitude and intention with six of those studies showing strong relationships at the $p < 0.01$ level. In contrast, two of the studies reviewed by Lebek did not show the significance of this correlation. In the non-IT related studies reviewed, attitude has been shown to be the most significant predictor of intention in eight cases (Ajzen & Klobas, 2013; Ajzen & Sheikh, 2013; Castanier, Deroche, & Woodman, 2013; Dawson, Mullan, & Sainsbury, 2014; Efrat & Shoham, 2013; Greaves et al., 2013; Tipton, 2014; Zemore & Ajzen, 2014). Similar to IT studies, contrasting findings in five other studies found attitude to be the least significant predictor of intention (Chan & Bishop, 2013; M. F. Chen & Tung, 2014; de Leeuw et al., 2015; Donald, Cooper, & Conchie, 2014; Mullan et al., 2015).

Subjective norm. Subjective norm (SN), the second of the two constructs taken from TRA, represents the social pressure perceived by the individual to perform or not perform a particular behavior (Ajzen, 1991; Yazdanmehr & Wang, 2015). Salient normative beliefs of the individual influence this construct (Armitage & Conner, 2001). Here the individual is concerned with whether or not those individuals or groups important to the individual approve or disapprove of performing a particular behavior (Yoon & Kim, 2013). Individuals can convey this information in the knowledge sharing process inside an organization (Dang-Pham, Pittayachawan, & Bruno, 2017; Flores et al., 2014) and even in the information security policies and control measures of the organization (Allam et al., 2014; Soomro et al., 2016). If the individual holds the belief that others think they should or should not perform an action it will have a positive or negative effect on the individual's intention to perform the behavior (Armitage & Conner, 2001; Yazdanmehr & Wang, 2015).

Subjective norm has been a subject of contention in the literature with various studies showing that it is either a weak (Dinev & Hu, 2007; Jafarkarimi et al., 2016), strong (Hu et al., 2012; Yazdanmehr & Wang, 2015), or insignificant (Yoon & Kim, 2013) predictor/motivator for information security compliance. Non-IT studies reviewed that apply TPB mimic this pattern. Two studies found subjective norm the most significant predictor of intention (Greaves et al., 2013; Prapavessis, Gaston, & DeJesus, 2015). Ten studies identifying the construct as the second most significant (Ajzen & Klobas, 2013; Ajzen & Sheikh, 2013; Castanier et al., 2013; Chan & Bishop, 2013; M. F. Chen & Tung, 2014; de Leeuw et al., 2015; Donald et al., 2014; Greaves et al., 2013; Mullan et al., 2015; Tipton, 2014). Three found subjective norm the lowest predictor (Dawson et al., 2014; Donald et al., 2014; Efrat & Shoham, 2013). One study found the construct insignificant (Zemore & Ajzen, 2014).

The importance of subjective norm on determining intended behavior is also a point of contention in the literature. In a review of 161 studies applying TPB, Armitage & Conner (2001) found subjective norm to be the weakest of predictors overall, but still concluded the construct to be relevant if multiple measures were used for the construct while also citing the need for additional empirical evidence. Dinev & Hu (2007) also found subjective norm a weak predictor which contrasts with the findings of Randall & Gibson (1991) that show this construct to be the second most important predictor of TPB.

Cox (2012) found subjective norm to be the most significant construct impacting intended behavior. Lebek (2014) stated that subjective norm showed a statistical influence on intention in six out of the eight IT studies reviewed that applied TPB. Other studies not fully based on TPB have applied subjective norm in their models and found the construct a significant (Tsai et al., 2016) or weak predictor of intention (Arpaci & Baloglu, 2016; Cheng et al., 2013).

There is also some conflict in the application of this construct. Siponen et al. (2014) applied normative beliefs directly as a predictor instead of as a measure for subjective norm as was proposed in the original TPB development (Ajzen, 1991). All of these conflicts are acceptable as they meet the expectations established by Ajzen and confirmed by Randall & Gibson (1991) that each independent variable in TPB would demonstrate a different level of significance across studies depending on the subject matter, environment, and sample population.

Perceived behavioral control. Perceived behavioral control (PCB) is the independent construct that differentiates TPB from TRA (Ajzen, 1991). Lebek (2014) determined that 92% of the correlations in existing literature between PBC and intention to be significant at the $p < 0.05$ level. In contrast, many studies find this construct to be the weakest predictor of intention (Ajzen & Klobas, 2013; Ajzen & Sheikh, 2013; Castanier et al., 2013; Greaves et al., 2013; Prapavessis et al., 2015) or insignificant (Greaves et al., 2013; Tipton, 2014).

Salient control beliefs held by the individual influence this construct (Ajzen, 2002). Ajzen (1991) compared and contrasted this construct with other conceptions of control, specifically locus of control and self-efficacy. The definition of locus of control is the belief one can control events affecting them (Ajzen, 2002). Perceived behavior control is different from locus of control as it takes into account not only the actor's belief that they can control the behavior but to what extent exercising this control will be easy or difficult through consideration of self-efficacy (Ajzen, 2002). The individual's belief in their ability to perform behaviors in a manner that achieves a desired goal defines self-efficacy (Ajzen, 1991). An argument exists that both locus of control and self-efficacy should be factors that define perceived behavioral control (Ajzen, 2002) and has been implemented this way in existing studies (Cox, 2012; Ifinedo, 2014). PCB posits the more an individual believes that they have the resources and opportunities to execute a behavior successfully, the greater their intention will be to perform the behavior (Ajzen, 2002). This construct not only effects the dependent variable of intention but has shown some correlational role in the actor exhibiting the actual behavior (Ajzen, 1991).

Intention. Intention is the dependent variable of TPB. Intention is of interest as TPB contends that intention to perform a behavior determines the actual behavior of the individual (Dinev & Hu, 2007). Intention provides an indicator as to how much effort an individual will put forward to perform a behavior (Ajzen, 1991). As applied in TPB, intention is meant to capture the motivational factors that will influence an individual's behavior (Ajzen, 1991). These motivational factors are represented by the three independent constructs (Randall & Gibson, 1991) previously discussed. Research performed during the validation of TRA and TPB and studies that have utilized these theories has provided empirical evidence that intention does have a strong correlation to actual behavior (Ajzen, 2002; Fishbein & Ajzen, 1975; Siponen et al., 2014). Note that there is some contention that theories such as TPB may be a better interpreter of desires than intention and thus may not lead to predicting objective behavior (Armitage & Conner, 2001). Intention is the dependent variable in this study due to the practical difficulties of collecting actual behavior data related to information security and applying intention in this manner is a well-established and accepted practice in the extant literature (Hu et al., 2012; Lebek et al., 2014).

Construct definitions in the proposed study. Definitions drawn from the literature for the three independent constructs of TPB as applied to this study are:

1. Attitude toward the behavior is the actor's internally developed thinking, feeling, and understanding of their self, their work motivations, and perceptions regarding information security in their workplace (Ajzen, 1991). TPB strongly associates attitude with intention (Ajzen, 1991; Chatterjee et al., 2015). This allows proposal of the argument that a strong attitude toward information security compliance correlates with a stronger intention toward information security compliance.
2. Subjective norm refers to the social evaluation of a behavior by the individual based on how they believe those important to them think the individual should act (Ajzen, 1991; Yazdanmehr & Wang, 2015). TPB posits that this can influence intention in regards to engaging in a particular behavior (Chatterjee et al., 2015). From the perspective of this study, the suggestion was that if an individual perceives that their engaging in information security compliance

behavior is important to those whom they value, this perception results in a stronger intention toward information security compliance behavior.

3. An individual's belief in his ability to perform a particular behavior drives perceived behavioral control (Ajzen, 2002). This belief is the result of considering if performing the behavior is in the control of the individual and if the individual has the skills to be successful in performing the behavior to the extent that it will produce the desired result (Ajzen, 1991). If the individual believes that he is able to facilitate information security compliant behaviors, there is a likelihood that the individual will have a stronger intention toward performing information security compliant behavior (Chatterjee et al., 2015). This was the rationale applied in this study.

Definition drawn from the literature for the dependent variable of TPB as applied to this study was:

1. Intention in this study represented the desire and likelihood of the individual to perform information security compliant behavior. Fishbein & Ajzen (1975) established in the development of TRA that intention is a strong predictor of actual behavior. In this study, I suggested that an individual's attitude toward the behavior, subjective norm, and perceived behavioral control have a correlational relationship to the individual's intention to perform information security related behavior.

Support for the use of TPB in the existing literature. TPB has been applied and empirically validated in a range of existing studies. In an article intended to review

TPB, challenge its constructs, and provide quantitative evidence of the ability of TPB to predict behaviors, Armitage & Conner (2001) reviewed 161 studies that apply TPB to determine the accuracy and effectiveness of each construct of TPB as well as the overall theory itself. Their study found TPB well supported as a theory by which to predict behaviors in a wide number of domains. Recent literature continued to support this stance (Dawson et al., 2014; Donald et al., 2014; Mahmood, Dahlan, Hussin, & Ahmad, 2016; Mullan et al., 2015; Prapavessis et al., 2015; Zemore & Ajzen, 2014).

Ajzen (1991, 2002) provided two follow-up articles to address challenges made to the theory and provide evidence of the theory's continued effectiveness. Randall & Gibson (1991) provided validation for the use of social theories in predicting intended and actual behaviors and made the call to apply TPB across ethical and decision-based studies. Dinev & Hu (2007) were the first to apply TPB to the study of information security. Since that time, Lebek (2014) showed TPB to be the theory of choice in 27 of 60 information security behavioral studies. Similarly, Alaskar et al. (2015) showed TPB to be the theory applied to 7 of 39 information security studies reviewed. Sommestad et al. (2015) challenged TPB as being a sufficient theory for explaining and predicting information security related behaviors and found TPB proved to be relevant to predicting such behaviors. However, sociobehavioral information security research is still in its early stages and researchers continue to provide validation and practical application for the integration of behavioral science and information security and make the call for continued research applying theories such as TPB (Crossler et al., 2013; Lebek et al., 2014).

Application of TPB in the existing information security literature. Dinev & Hu (2007) applied the constructs of TPB and TAM in a study investigating the effects of technology awareness on the use of protective software such as antivirus software. The authors well established the extensive application of sociobehavioral theories in technology acceptance studies and this provided the underlying support for extending the use of such theories in information security studies. Their study showed significant support for the use of social/behavioral theories in information security and validation of TPB specifically in information security research. Here the attitude and perceived behavior control constructs showed significant in predicting behavioral intention while subjective norm was weak.

Ifinedo (2012) applied TPB in a study determining the information security compliance drivers for end users. Similar to Dinev & Hu (2007), Ifinedo found the attitude construct significant in predicting intended behavior, but contrasted Dinev & Hu by showing subjective norm to be relevant in the same prediction. Ifinedo (2014) confirmed these findings in a subsequent study applying TPB to determine information security policy compliance. Ifinedo does not use the construct of perceived behavioral control directly in both of his studies, but instead the construct is broken down into the factors that define the independent construct as previously outlined. Although Ifinedo confirmed these factors to be significant in each study, it was not possible to contrast his findings directly with studies that apply the independent perceived behavioral control construct specifically.

Two additional information security studies performed in 2012 applied TPB. Hu et al. (2012) applied TPB to determine how organizational culture and the influence of management effects the information security related intentions of computer end users. In this study, Hu et al. found subjective norm to be the most significant construct although only slightly more than PCB. Here the finding was still that attitude is a significant predictor. However, it is the lesser of the three constructs. Cox (2012) mimicked the findings of Hu et al. in a study determining how the knowing-doing gap related to end user information security knowledge effected intentions to comply with information security policy by again showing subjective norm to be the most significant construct followed by perceived behavioral control and lastly attitude. These findings vary substantially from studies applying TPB in other subject areas where subjective norm was typically found to be the weaker predictive construct (Armitage & Conner, 2001).

Siponen et al. (2014) applied TPB to study various factors that lead to employees' intention to comply with information security to provide information to develop training and awareness campaigns that address the influencing motivational factors. Like previous studies, Siponen et al. found attitude to be the most significant construct in the model. Siponen et al. followed a similar approach as other studies by applying observable factors that define subjective norm and perceived behavioral control in the form of normative beliefs and self-efficacy respectively. The findings showed subjective norm to be the second most significant construct, supporting the findings of Ifinedo (2012). It was not possible to draw correlations for perceived behavioral control between the Siponen et al. study and others due to the incomplete use of all the factors forming this independent construct.

Three information security studies completed in 2015 apply TPB. Safa et al. (2015) provided research into the formation of information security conscious care behavior and thus changed the dependent variable of the TPB model to reflect this measurement point. This study agrees with the findings of Cox (2012) and Hu et al. (2012) in citing subjective norm as the most significant construct. Safa et al. also found attitude to be a sound predictor. However, they found perceived behavior control insignificant. A study by Chatterjee et al. (2015) applied TPB to determine key factors related to the unethical use of information technology. Here all independent constructs were determined to be significant predictors of intent in the order of attitude, perceived behavioral control, and lastly subjective norm matching most closely with the original findings of Dinev & Hu (2007). Djajadikerta et al. (2015) found when applying TPB to the study of dysfunctional information system behaviors that the attitude construct was significant in all scenarios tested with subjective norm being significant in three out of four scenarios. However, perceived behavioral control was of significance in only one out of four scenarios in their study.

Two information security studies completed in 2016 and one in 2017 applied TPB. Jafarkarimi et al. (2016) applied TPB to ethics in social networking, and again attitude was found to be the most significant followed in order by subjective norm and perceived behavioral control. Gurung & Raja (2016) found attitude to be the most significant followed by perceived behavioral control and subjective norm in their study applying TPB to online privacy and security concerns. Attitude showed significant in a study by Dang-Pham et al. (2017) on information security knowledge sharing followed by subjective norm. However, perceived behavioral control showed no relevance.

It was possible to make a couple of conclusions when reviewing these studies. First, they support the suggestion forwarded by Ajzen (1991) that the significance of each independent construct in the TPB framework will depend on the subject matter and sample population. Next, a recognizable pattern exists where subjective norm appears to be more significantly relevant in information security scenarios. This suggests that individuals value the opinions of others who are important to them when making decisions regarding information security compliance.

Challenges to TPB in the existing information security literature. TPB is not without challenge nor are the independent constructs of the theory. TPB was developed specifically to address challenges made to TRA (Fishbein & Ajzen, 1975) that it did not address the volitional aspect of user behavior leading to the addition of the perceived behavioral control construct (Ajzen, 1985). It was the further definition of this construct along with justification for the use of intention and self-reported data that served as the primary focus of Ajzen's (1991) follow-up paper to address challenges to these areas made by the academic community. Additional challenges to the theory have been made suggesting lack of consideration for items such as alternate actions (Sniehotta, Presseau, & Araújo-Soares, 2014) but have been defended on the basis of poor understanding or implementation of TPB (Ajzen, 2014) and validated through research (Ajzen & Sheikh, 2013).

Researchers have also challenged TPB from an information security perspective for not accounting for certain characteristics of the individual, clarity and scope of information security policies, and cultural dimensions (Al-Mukahal & Alshare, 2015). Other areas of consideration are individual knowledge of policy, trust relationships with management, and how well developed and effective security policies are in the environment. Culture is also an area frequently discussed by researchers as an important motivational factor in information security research (Al-Mukahal & Alshare, 2015; Arpaci & Baloglu, 2016; Ashenden & Sasse, 2013; Crossler et al., 2013; D'Arcy & Greene, 2014; Da Veiga & Martins, 2015a, 2015b; Flores et al., 2014; Hu et al., 2012; Karlsson et al., 2015; Kolkowska & Dhillon, 2013).

Use of self-reported data for behavioral intention. It is difficult to observe actual information security compliance behavior in a natural setting as it cannot be determined when the individual will be presented with a situation where information security related behavior is required (Hu et al., 2012). However, the use of self-reporting data has been challenged as being an accurate predictor of actual behavior (Workman et al., 2008). It is possible to manifest a live scenario, but behaviors can vary when the individual knows they are being tested and observed resulting in a socially desirable behavior instead of exhibiting what actual behavior may be in a real situation (Crossler et al., 2013). The literature has shown that intention can be measured via self-reported data (Parsons, McCormac, Butavicius, et al., 2014) and that TPB is effective in accounting for variance between self-reported and actual behavior (Armitage & Conner, 2001). Assessing intention via the independent constructs of TPB has been shown to be grounded both theoretically and technically (Lebek et al., 2014). Thus intention and the use of self-reported behavior has been established as having sufficient predictability of actual behavior (Ajzen, 1991; Moody & Siponen, 2013) in order to be applied practically in determining if an individual would perform information security compliant behavior.

The use of motivational factors as measures. Researchers have applied all the theories outlined in previous sections to information security behavioral studies in the extant literature. Most of these theories have a defined set of motivational factors that serve as the independent variables (Bagozzi & Yi, 2012) in their respective theoretical framework. Often the goal of these studies is identifying motivational factors and determining if they are indeed relevant in predicting information security compliant behavior (Chatterjee et al., 2015; Galvez et al., 2015; Sommestad et al., 2014; Willison & Warkentin, 2013). Researchers have called for the identification of these motivational factors as part of a need to drive change from thinking about information security technically to socially (Kirlappos & Sasse, 2012). TPB categorizes these motivational factors by identifying them as being based on the behavioral, normative, or control beliefs of the individual (Ajzen, 1991). In TPB the dependent variable of intention has been defined as indicating the level of effort an individual is willing to exert to perform a behavior and is assumed to capture the motivational factors that influence such behavior (Ajzen, 1991).

A current trend in sociobehavioral information security research is the combining of theories and variables. This practice, known as theory integration, combines variables from multiple theories in order to provide a more rich and complex picture and has been stated to be necessary to provide this perspective and extend behavioral information security research beyond the current literature (Siponen et al., 2014). Research approaches the combining of variables and motivational factors in one of two ways. The first method takes the independent variables from multiple theories and makes them all independent variables directly correlated with the framework's dependent variable. Examples include using independent variables from TRA, PMT, and behaviorism theory (Gundu & Flowerday, 2013), TRA, moral obligation, PMT, and organizational context factors (Yoon & Kim, 2013), or PMT and TPB (Ifinedo, 2012; Safa et al., 2015; Sommestad et al., 2015) all to predict behavioral intention. Another example uses PMT and SCT to assess information security intervention strategies (Shillair et al., 2015).

The second method is using observable motivational factors as measures to define independent constructs. Here factors that are measurable and provide definition are correlated with independent constructs (M. I. Aguirre-Urreta, Marakas, & Ellis, 2013). For example, researchers have applied the independent variables that makeup PMT such as perceived severity and perceived vulnerability as measures that define the "attitude towards the behavior" independent construct of TPB (Cox, 2012; Yoon & Kim, 2013). Likewise, researchers have applied the SCT variables of locus of control and self-efficacy as measures that define the perceived behavioral control construct of TPB (Cox, 2012).

In a quantitative research design, the researcher will commonly develop survey questions that represent and measure motivational factors demonstrated in the environment (Bagozzi & Yi, 2012; Mahmood et al., 2016). Correlational analysis techniques are then applied to verify relationships in the theoretical model between the independent constructs and the dependent variable(s) (Bagozzi & Yi, 2012). Several sociobehavioral information security studies that apply TPB use this approach.

One example is research into the information security "knowing-doing gap" that looks at individuals' understanding of information security and how other factors can affect their intentional or unintentional actions related to following security guidelines (Cox, 2012). Cox mapped observable measures to the independent constructs of TPB to relate and apply the theory to the research topic at hand. Another research example combined TPB and PMT measures in a similar study of predicting information security compliance (Ifinedo, 2012). The addition of PMT in this study example added the overarching theme of self-protection into the prediction model.

The approach of combining theories in a research model is robust; however, this practice establishes new frameworks and theories that must be empirically verified several times before credibility and generalization of the framework can be achieved (Venkatesh et al., 2013). This study took a lesser approach to avoid creating a new framework but still provide accurate definition and measurement of the independent constructs. This study specifically used the framework and variables of TPB. The application of observable measures established in existing literature provided for the definition of the independent constructs.

TPB and the theoretical framework for this study. This section provides substantiation of the constructs of TPB in relation to this study and discussion on how drawing on other behavioral theories and the application of their independent variables as measures to explain and define the constructs of TPB provides a rich and complex view of the study topic. The combining of theories and/or the inclusion of a large number of variables or measures is supported by a trend in existing literature as technology grows and scenarios become more complex (Siponen et al., 2014). Most research that limits to a single theory or limited constructs no longer provides enough insight to make a valid conclusion, and this is a limitation toward generalized knowledge in the subject area (Cox, 2012; Ifinedo, 2012). In this study, definition for each of the independent constructs came from one or more observable measures related to the target population.

Sommestad et al. (2015) challenged TPB as being a sufficient theory for explaining and predicting information security related behaviors with the base premise that although research shows TPB an accurate predictor of intended behavior, it is typically combined with elements from other theories and not applied strictly by its original constructs. Sommestad et al. continued in this trend and tested if elements of PMT could improve the outcomes of research that applies TPB. Their study found that all the elements of TPB proved to be relevant at predicting behaviors on their own; however, the addition of elements from other theories such as PMT improved the predictive results. Cox (2012) extended the TPB framework by adding motivational factors specific to the study environment which in that case was a corporate environment. Cox, like Ifinedo (2012), also included elements of other theories in his research such as organizational narcissism and threat control (Cox, 2012; Ifinedo, 2012). This study used the same or similar theories and motivational factors to develop explanatory measures for the independent constructs of TPB.

The framework for this study used the specific independent constructs of attitude towards the behavior, subjective norm, and perceived behavior control as presented originally in TPB (Ajzen, 1985). However, it was necessary to define how to measure each independent construct. A selection of motivational factors served as the observable measures for the independent constructs and basis for survey questions for the study. Combining the values of measures related to a particular construct provided a value for each of the independent constructs in the study's model. I intuitively selected these measures, drawing on extant literature and identified psychological targets needing understanding in areas of human motivation (Michie & West, 2013), as representing salient beliefs of the study population. Through this focus on salient beliefs (Ajzen, 1991) it was proposed that relevant and significant correlations may exist.

The measures for this study were organizational narcissism, reward, perceived vulnerability, perceived severity, normative beliefs, locus of control, and self-efficacy. As previously discussed in this review, this study did not create a new theory or framework. Substantiation for the correlation of the selected measures already existed in the extant research (See Table 1) and I used these measures as a method to define the independent constructs of TPB. Many of these measures were similar to Cox (2012) where he relates organizational narcissism, perceived vulnerability, and perceived severity to the construct of attitude towards the behavior. This study went further to consider reward as another factor effecting attitude towards the behavior, and a following section provides validation for its inclusion. Salient normative beliefs form subjective norm (Armitage & Conner, 2001). These normative beliefs represent how the individual perceives the opinions of those important to the individual in regard to the expected behavior (Ajzen, 2002; Yazdanmehr & Wang, 2015) which in this case was information security compliance. Normative beliefs served as the measure for subjective norms in this study. The measures related to perceived behavioral control were locus of control and self-efficacy (Ajzen, 2002; Cox, 2012).

Table 1

Construct Operationalization

Description	Source
Organizational narcissism - > Attitude toward the behavior	J. Cox (2012), inclusion of personality traits Ajzen (1991), Kajzer et al. (2014), Shropshire, Warkentin, & Sharma (2015), Wall et al. (2013)
Perceived vulnerability - > Attitude toward the behavior	J. Cox (2012), Yoon & Kim (2013)
Perceived severity - > Attitude toward the behavior	J. Cox (2012), Yoon & Kim (2013)
Reward - > Attitude toward the behavior	Current study (derived from discussions and applications in Chatterjee et al. (2015), Farahmand, Atallah, & Spafford (2013), Posey et al. (2014), Sommestad et al. (2015))
Normative beliefs -> Subjective norm	Ajzen (1991), Armitage & Conner (2001), J. Cox (2012), Ifinedo (Ifinedo, 2012), Sommestad e al. (2015), Yoon & Kim (2013)
Locus of control - > Perceived behavioral control	Ajzen (Ajzen, 2002), J. Cox (2012)
Self-efficacy - > Perceived behavioral control	Ajzen (Ajzen, 2002), Chatterjee et al. (2015), J. Cox (2012)

Note. Provides a summary of previously established measure relationships.

Measures for attitude toward the behavior. This study used four factors to define and measure the attitude toward the behavior independent construct. These factors were organizational narcissism, perceived vulnerability, perceived severity, and reward. This section discusses each of these factors to further define the measure, identify the source of the factor, and provide justification for the use of the factor based on existing literature.

Ajzen (1991) specifically discusses personality traits impacting attitude and being influential in predicting behavior, yet the use of this type of factor is lacking in the existing information security TPB literature, and only limited examples exist across all domains (Ajzen & Klobas, 2013; de Leeuw et al., 2015; Efrat & Shoham, 2013). Personal norms, of which organizational narcissism would be an example, have been shown to be the most significant factors influencing attitude toward the behavior of information security compliance and researchers suggest inclusion in such studies (Ifinedo, 2014). The only literature example known is a corporate study in which the organizational narcissism factor was applied but did not show significance (Cox, 2012).

Control-related motivations and personality traits have been shown to have a significant effect on information security behavioral intention supporting the inclusion of psychological theory in sociobehavioral studies (Kajzer et al., 2014; Shropshire et al., 2015; Wall et al., 2013). Autonomy, control, influence, ownership, external perceptions, and identity are all factors that contribute to organizational narcissism (Galvin, Lange, & Ashforth, 2015; Wall et al., 2013). Narcissism is a personality trait comprised of a collection of views and emotions (Vater et al., 2013) that has been identified as a primary trait to drive risk behavior (Crysel, Crosier, & Webster, 2013). Organizational narcissism can manifest when an individual identifies themselves as being core to the identity of the organization, and it can have an influence on behavioral decisions (Galvin et al., 2015).

Perceived vulnerability, perceived severity, and reward are motivational factors established in PMT (Dang-Pham & Pittayachawan, 2015; Posey et al., 2015). PMT is comprised of two classifications of motivational factors, that of threat appraisal factors and coping appraisal factors (Ifinedo, 2014; Tsai et al., 2016). The three motivational factors discussed here are threat appraisal factors. Perceived vulnerability addresses the individual's perception regarding the likelihood of a negative event (Gundu & Flowerday, 2013). Perceived severity addresses the individual's perception regarding the degree of harm that would come from such a negative event (Gundu & Flowerday, 2013). Both influence attitude toward compliance (Herath et al., 2014; Lee et al., 2016) and protective behavior (Crossler et al., 2014; Herath et al., 2014; Öğütçü et al., 2016). Information security studies based on TPB have demonstrated the correlation between perceived vulnerability and perceived severity and the attitude towards the behavior independent construct (Cox, 2012; Yoon & Kim, 2013).

Reward is defined by the intrinsic or extrinsic benefits gained or kept through performing or not performing a behavior (Moody & Siponen, 2013; Posey et al., 2015; Siponen et al., 2014) and has been shown to be a relevant motivational factor in information security behavior (Kajzer et al., 2014; Moody & Siponen, 2013; Posey et al., 2015, 2014). The use of reward as a measure has been absent in information security related TPB studies. This could be because reward is also an incentive motivational factor in GDT and SCT and there is some conflict on the value of these theories in predicting information security behavior (Yoon & Kim, 2013). However, researchers have called for the inclusion of this factor in future studies (Boss et al., 2015; Ifinedo, 2012; Parsons, McCormac, Butavicius, et al., 2014; Posey et al., 2015). The inclusion of reward was a unique factor in the proposed study. Coercion or deterrent factors (Barton, Tejay, Lane, & Terrell, 2016) have been used in the past to represent similar motivational factors. Reward has been used as a manifest variable in at least one PMT-based information security study for predicting intention (Siponen et al., 2014).

A supervisor can reward individuals at work through a performance appraisal process. A supervisor may reward an employee in this process for achieving an operational goal that may have required the individual to not comply with information security policies. Literature has stated that this type of reward has a relationship to the attitude of the individual (Cheng et al., 2013; Parsons, McCormac, Butavicius, et al., 2014; Zhai, Lindorff, & Cooper, 2013) and can influence behavior intention (Farahmand et al., 2013; Shillair et al., 2015). Literature also shows that damage to ego through poor performance appraisal (lack of reward) leads to riskier behavior for those with narcissistic traits (Crysel et al., 2013). This demonstrates a relationship between the reward and organizational narcissism factors and supported their inclusion in a singular study. Information security behavioral intention can also be altered when reward exceeds inconvenience (Workman et al., 2008) showing that given proper return end users will ignore known information security policies and training (Kirlappos & Sasse, 2012).

Measure for subjective norm. In this study, I included normative beliefs as the single measure for subjective norm. Existing studies have established that subjective norm is influenced by normative beliefs (Cox, 2012; Lebek et al., 2014). Normative beliefs are understandings of perceived behavior developed by the individual through the observation of their peers and others in their environment (Barton et al., 2016; Yoon & Kim, 2013). Sometimes normative beliefs are also defined as being similar to the moral obligations felt by an individual to perform in a particular manner (Jafarkarimi et al., 2016; Kajzer et al., 2014; Yazdanmehr & Wang, 2015). Based on these normative beliefs, the individual develops thoughts of how they believe those important to them expect them to behave, and this becomes their subjective norm (Armitage & Conner, 2001). There is a close relationship between normative beliefs and subjective norm in both definition and intent and are often used interchangeably in the literature even though they are distinct in definition.

Some studies apply normative beliefs directly as an independent variable toward the dependent variable of intention and have found normative beliefs to be both a significant (Siponen et al., 2014) and weak (Flores & Ekstedt, 2016) predicting factor. However, in this type of application the representation is still that normative beliefs affect the intentions of the individual, and a conclusion is drawn that these normative beliefs influence the thoughts of the individual in regards to their actions (Barton et al., 2016; Safa et al., 2016), which becomes their subjective norm (Ajzen, 1991; Ifinedo, 2012). Others combine these concepts of norms into a single construct described as perceived norms (Sommestad et al., 2015).

Measures for perceived behavioral control. The addition of the perceived behavioral control construct is what differs TPB from TRA (Ajzen, 1991). This construct accounts for elements of behavioral processes that are outside the volition of the individual. The lack of which researchers have cited as a limitation of TRA (Ajzen, 1985). Ifinedo (2014) defined perceived behavior control as being influenced by the two factors of locus of control and self-efficacy, both borrowed from the expectancy theory of SCT. Locus of control addresses if executing a particular behavior is in the control of the individual or another entity and represents an outcome expectation. Self-efficacy addresses the ability of the individual to execute a behavior and exemplifies an efficacy expectation (Ajzen, 2002).

Ajzen (1991) closely related these two factors in the development of the perceived behavioral control construct in the formation of TPB. However, the blending of these two factors into a single measure has been challenged as they represent two distinct factors and should be measured independently (Workman et al., 2008). These two factors are also represented in PMT as coping assessment measures and have both shown significance in predicting security omissive behavior when applied in that framework (Siponen et al., 2014; Workman et al., 2008). Self-efficacy is prevalent as an independent variable in the information security studies reviewed, and although it is a valuable predictor of compliant behavior (Crossler et al., 2014; Galvez et al., 2015; Herath et al., 2014), other studies have shown it not to be a significant predicting factor for information security compliance (Choi et al., 2013; Flores & Ekstedt, 2016; Wall et al., 2013).

Intention in the proposed study. Intention, as applied in TPB, is meant to capture the motivational factors that will influence an individual's behavior in the form of the independent constructs of attitude toward the behavior, subjective norm, and perceived behavioral control (Ajzen, 1991). Measurement of intention occurred through self-reported data as discussed previously in this review. Seven information security studies applying TPB reviewed by Lebek (2014) follow the approach of evaluating the independent variables of the theory against this dependent variable. This study followed the same approach.

Methodologies Used in Extant Literature

Researchers apply a number of differing research methodologies in the extant information security literature to measure the dependent variable of intention. For the studies that researchers wholly or mostly base on TPB, the predominant approach is quantitative correlational methods with the only varying aspect being the framework and/or study population. Previous sections of this study discussed the topic of varying frameworks via differing methods of combining theories, variables, and measurement factors. Varying of study population can be seen in studies utilizing college students (Chatterjee et al., 2015; Dinev & Hu, 2007; Hu et al., 2012), corporate computer end users (Cox, 2012; Ifinedo, 2012, 2014; Siponen et al., 2014), and IT professionals (Ifinedo, 2012, 2014). This approach is the same as can be seen in studies that apply TPB but are not information security related (Randall & Gibson, 1991). The only TPB-based information security study reviewed that deviates from this approach is Gundu & Flowerday's (2013) quasi-experimental study where they applied TPB in evaluating information security knowledge after repeated training exercises. I did not locate any experimental information security studies applying TPB. The review of extant literature also exposed one information security study that applied the independent constructs of

TPB but utilized a modified dependent variable of conscious care behavior (Safa et al., 2015). However, it still employed a quantitative correlational methodology.

A number of information security related studies use the same dependent variable of intention, yet they apply independent constructs from different theories. Example theories providing these independent constructs include RCT (Cheng et al., 2013; Willison & Warkentin, 2013), PMT and habit theory (Boss et al., 2015), TRA/moral obligation/PMT/organizational context (Yoon & Kim, 2013), SBT/DT (Cheng et al., 2013), self-determination/psychological reactance theories (Wall et al., 2013), coping/moral disengagement/security related stress (D'Arcy et al., 2014), and culture/social exchange theory (D'Arcy & Greene, 2014). All of these studies follow the dominant model of a quantitative correlational method. However, one can find variation in this realm. One study applied a 3x3x3 factorial experiment design (Barlow et al., 2013). That study utilized random selection and achieved treatment control through the manipulation of scenarios. It would be proper to consider that study quasi-experimental as statistical variables were not controlled that could introduce rival hypotheses (R. K. Yin, 2013). Another study utilized the same dependent variable of intended behavior in a quasi-experimental 2x2x2 factorial design while applying the theories of PMT/SCT (Shillair et al., 2015).

Measurement Instruments Used in Extant Literature

For all the studies cited in the methodologies section above, regardless of theory or method, the single measurement instrument was that of a survey. When applying a survey for data collection the researcher develops survey questions based on the independent variables or observed factors (motivational factors demonstrated in the environment) that comprise the applied theory (Fetters et al., 2013). The only variation for the surveys in the reviewed literature is in the delivery method, which ranged from electronic and Web-based surveys to paper surveys distributed in person or via the postal system.

The use of surveys in quantitative research is popular for effective, efficient, affordable, and anonymous broad scale data gathering and is well supported (Mahmood et al., 2016; Venkatesh et al., 2013). The development and implementation of written or oral survey questions is the data gathering technique in the survey model. The responses to the survey questions represent data relevant to the variables or measures of the proposed theory and thus are analyzed to accept or reject the hypotheses forwarded by the researcher (Fetters et al., 2013). The survey design is time and cost effective and efficient (Weigold, Weigold, & Russell, 2013), provides data that are generally ready for analysis without further interpretation, and is convenient for both the researcher and study participant (Yoshikawa et al., 2013).

Contention in the Literature

The studies reviewed attempt to develop a method to measure intention to comply with information security (Sommestad et al., 2015), information security culture (Da Veiga & Martins, 2015a, 2015b; Flores et al., 2014), determine effectiveness of information security policy (Parsons, McCormac, Pattinson, et al., 2014), and/or intention to evade policy (Barlow et al., 2013). However, many seem to differ in the right theory or methodology to perform these measurements as evident by the diverse approaches noted in preceding sections of this paper. In regards to theory, Lebek et al. (2014) documented 54 theories that researchers have applied in sociobehavioral information security studies. The prevailing theory is TPB (Lebek et al., 2014) but it has not been established to be the standard. This contention stems from conflicts in the interpretation of the theories themselves. For example, TPB has had conflicting conclusions in various studies regarding which is the prevailing of the three constructs of attitude toward the behavior, subjective norm, and perceived behavior control (Chatterjee et al., 2015; Safa et al., 2015; Sommestad et al., 2015). Further contention happens in defining the individual constructs (Ajzen, 1991). Perceived behavior control is an example in terms of its definition being more about self-efficacy, locus of control, or both (Ajzen, 2002; Workman et al., 2008). The range of approaches in the preceding methodologies and measurement sections further demonstrate the lack of a standard practice for gathering and analyzing data to predict intended behavior related to information security. Sampling is also a point of contention noted in the review of these works. Some studies focus on data collected from populations such as IT professionals or college students (Crossler et al., 2013; Safa et al., 2015) which does not necessarily reflect a population of interest.

Relationship of Proposed Study to Extant Research

More study is needed in end user information security behavior (Dhillon & Backhouse, 2001) and there is a need for more empirical studies to validate behavior research theories (Siponen et al., 2014). This study answered both of these calls. Of the 41 studies in this literature review that focus on the application of sociobehavioral theories in information security research, only one samples non-IT end user employees in the educational sector. The remaining studies survey corporate employees, college students, IT personnel, noneducation government employees, the general public, or a combination of these populations. Most studies reviewed that do enter the realm of academia do so at the university level (Ahlan et al., 2015; Al-Alawi et al., 2016; Dang-Pham & Pittayachawan, 2015; Kim, 2014; Misenheimer, 2014; Öğütçü et al., 2016; Shropshire et al., 2015). The educational sector is largely nonexistent in the extant behavioral information security literature; however, this area is at high risk (Okpamen, 2013; Pardo & Siemens, 2014). Research has shown that the educational sector experiences high information security risks due to bad information security habits, lack of communications, feedback, and motivation (Chou & Chou, 2016). Lack of belief, attitude, intention, behavior, training, awareness, and norms adoption also contribute to the information security exposure in educational environments (Chou & Chou, 2016). K-12 educational environments especially should be addressed as these issues can be more prevalent due to organizational scale and mindset (Moyo, 2013). This study aided in filling this gap.

Herath & Rao's (2009) research showed that intrinsic motivators such as morals, purpose, end goals, and understanding of information security as well as extrinsic motivators such as social influence or the fear of detection effect understanding and attitudes towards information security compliance. This study adds to this discussion. However, Herath & Rao executed their study broadly across different types of entities to draw generalized findings. Focusing on a single entity/industry will show if generalized theoretical concepts (Sandelowski, 2014; Tsang, 2014) apply to that environment. There is a need to study more about what factors motivate behaviors in different environments (Crossler et al., 2013). The K-12 environment in this study may differ in motivators when compared to corporate or higher learning environments.

The scope of information security motivational factors needs to be expanded from existing literature, extending to factors beyond maliciousness and productivity/convenience (Crossler et al., 2013). Much of the existing information security literature is also limited to using questions and/or scenarios such as writing down or sharing passwords, failing to log out of systems, or copying data to external devices (D'Arcy et al., 2014). There is a need to look at broader motivators of organizational managers, such as school administrators, that change organization operations and results in potential major data exposure (Hu et al., 2012). At a broader level, the IT landscape is more complex today and there is a need to take in many more factors than the limited ones of most studies (Ifinedo, 2012). Cox (2012) cites changes in technology results in changes in attitudes and ethics over time furthering support for ongoing research in this area. Again, this study adds to the conversation in these target areas.

Aspects for Further Research Cited in Extant Literature

End user study in regards to information security is still young overall (Herath & Rao, 2009) allowing for many avenues of further research. Much of the existing research is at a high level identifying factors and correlations of human behavior that effect information security. These individual factors, such as the independent constructs of TPB, can be studied deeper on a per factor level to provide greater insight. Since sociobehavioral information security research is relatively new, most all studies need the findings to be applied to more groups and/or specific industries (Crossler et al., 2013) for generalization.

Research into end user security behavior may no longer be in its infancy, but the vast number of areas that remain for future research shows this field to be in its adolescent years at best. Crossler et al. (2013) list a range of topics needing research in the categorization of behaviors, improving security compliance, and cross-cultural research. D'Arcy & Greene (2014) echo the call for studying behaviors from a cultural perspective, while researchers like Cox (2012) advocate research into personality traits of end users to understand security behavior. Some researchers see information security from an organizational perspective and are extending study deeper into this realm (Hu et al., 2012; Kolkowska & Dhillon, 2013). At the base of each of these suggestions is the continuation to integrate findings from psychological and behavioral research in the application of information security. This study addressed many of these issues.

Transition and Summary

The development of effective IT security controls is a requirement for information security program managers (Disterer, 2013; Galvez et al., 2015; NIST, 2015; Wilson & Hash, 2003). The existing research has established both in concept and empirically that end user behavior effects information security compliance in the organization and ultimately the security level of an entity overall (Alaskar et al., 2015). With computer end users representing potentially the largest information security risk to the organization (Alaskar et al., 2015; Crossler et al., 2013), information security program managers must implement effective nontechnical controls in the form of SETA programs (NIST, 2015).

Information security program managers may benefit from having an understanding of the motivational factors that drive compliant and noncompliant behaviors in order to develop and improve such campaigns.

In the literature review, I provided an examination of the existing literature from the perspective of applying behavioral theories to end user information security research and discussing the variables in these theories that establish the motivational factors for compliance. The literature indicated TPB provided the correct theoretical fit for this study. The independent constructs of the theory allow focussing on salient beliefs of the study population (Ajzen, 1991) that influence their intention to perform information security related behaviors (Sommestad et al., 2015). These constructs are attitude toward the behavior, subjective norm, and perceived behavioral control (Ajzen, 1985). It has been determined to be likely that persuasive messages, such as those provided in SETA programs, can influence and change the salient beliefs of individuals and thus influence their information security compliance intentions (Ajzen, 1991). Trends in this field were also identified such as the combining of theories to provide a richer, more complex picture relevant to the current IT landscape (Siponen et al., 2014).

In the extant literature, researchers discussed the risk that end user behavior poses to an organization and provided justification for the need to understand this behavior (Parsons, McCormac, Pattinson, et al., 2014). Arguments have been presented and substantially supported that the key to understanding this behavior is through the application of sociobehavioral (Dhillon & Backhouse, 2001) theories. An analysis of common applications of these theories in existing research has been provided as well as a look into future trends (Crossler et al., 2013) in this same area.

The existing literature in the field of information security and end user behavior research indicated that study in the area is valid and trending, but still new and requires the support of further studies (Crossler et al., 2013; D'Arcy & Greene, 2014). This same literature presented support for the concepts of applying behavior theories to determine end user intention to follow or evade information security (Lebek et al., 2014). These studies showed the benefit of such research to the IT field through increased knowledge and awareness of information security effectiveness and culture and presented how the research findings are applicable to improving information security efforts.

The literature review showed that extending this research into the K-12 educational environment has not occurred. This study proposed that the K-12 environment might present unique motivational factors that may expand the study of information security compliance drivers and variables and add to the existing body of knowledge in this subject area. The literature review concluded with suggestions for future research in the hope that continued study in this field will improve the application of nontechnical security controls. The goal of these improvements is to bring better security to the organization and effect social change in the form of increased freedoms and privacy through the secure handling of computer data (DHS Privacy Office and the Office for Civil Rights and Civil Liberties, 2015).

Section 1 of this paper presented details on the study problem, background, and a detailed review of the existing literature related to the subject. This segment concludes

Section 1, with Sections 2 and 3 to follow. Section 2 provides a detailed outline regarding the approach and execution of the research project including research method and design, population and sampling, measurement instrumentation, and data gathering and analysis. Section 3 presents the findings of the study along with information regarding practical application in the IT profession as well as implications for social change. Section 3 also includes recommendations for useful action based on the study results as well as for future research in the subject area. Section 3 concludes with reflections on the study.

Section 2: The Project

There are academic studies that apply sociobehavioral theories to predict information security compliance intentions in order to improve SETA programs (Lebek et al., 2014). The literature review in Section 1 provided evidence that the majority of these studies focus on the private business sector. This quantitative study extended this research into the K-12 education sector in order to determine if the variables of TPB were applicable in this environment for consideration during SETA program improvement.

This section begins with restating the study's purpose and provides details of the researcher's role in the study as well as that of the study participants. Section 2 also contains specifics regarding the study's research methodology and design along with information on population sampling, measurement instrumentation, data gathering, and analysis. The section closes with a discussion of study validity and a transition to Section 3.

Purpose Statement

The purpose of this quantitative correlational study was to examine how attitude toward the behavior, subjective norm, and perceived behavioral control affect the intention of computer end users in a K-12 environment to follow information security policy to provide IT security program managers sufficient knowledge to develop effective security controls in the form of SETA to protect against human behavior risks. Surveying computer end users in the Bigg County Public School System located in Northeast Georgia provided data collection. For this study, I applied TPB (Sommestad et al., 2015) to provide sufficient knowledge of how the constructs of this theory affected the information security behavior intentions of computer end users so that IT security program managers can develop effective SETA programs as a security control. Applying sociobehavioral theories to information security research is a current trend with researchers calling for further academic study (Crossler et al., 2013). The independent constructs of this theory are attitude toward the behavior, subjective norm, and perceived behavioral control. The dependent variable is intention. The implications for social change include the possibility for development of effective information security controls and improvement of data security protections for the employees and vulnerable student population of K-12 schools.

Role of the Researcher

In quantitative research the role of the researcher is to be as detached from the data gathering process as possible with the goal of providing an impartial and objective view (Yilmaz, 2013; Yoshikawa et al., 2013). However, researchers still have influence on the data collected in that the researcher selects the theory to be tested, is able to manipulate the independent variables in the criteria that will define them and how they will be measured, determines the analysis technique, and selects the population and sampling process (Tavakol & Sandars, 2014a). For example, in this study, I selected the factors (based on the extant literature) that defined the independent constructs of TPB. Likewise, I chose to use a survey for data collection, acquired established measurement questions, and developed the instrument to measure these factors.

I have obtained a formal education in information security and work professionally in the IT field. I was formerly an active participant as an IT worker located in some of the same K-12 schools in this study. In an organization, a conflict can arise between IT functionality, ease of use, and security (Kohlborn, 2014). I often dealt with this conflict as school administrators challenged that information security impeded the operations and goals attainment of the school. I often observed school administrators desiring to take actions to reach technology goals and objectives through methods that may circumvent information security intentionally or unintentionally. This led to consideration of what motivational factors effected K-12 administrators' intentions to comply with information security and how this information could improve SETA campaigns, thus the formation of the topic for this study. To mitigate subjective bias (Tavakol & Sandars, 2014a), I used an Internet-based survey that provided direct contact separation from the sample and that contained properly formed survey questions focused on measuring the intended constructs. Another mitigation was the use of the quantitative method deploying statistical analysis in order to draw conclusions based only on the data presented.

Ethical research was paramount, and this study complied with the guidelines and requirements for respect, beneficence, and justice as prescribed in the Belmont Report (Tavakol & Sandars, 2014b). Allowing participants free will to participate in the study showed respect. Ensuring identity protections to participants, holding participants free from harm due to participation or lack thereof, and providing research findings back to the participant organization for the benefit of developing improved information security protections for the participants (should they so choose) provided beneficence and justice.

The upcoming “Ethical Research” and “Data Collection Technique” sections provide a complete discussion on methods for addressing these ethical concerns specifically.

Participants

Eligible participants for the study were required to be computer end users operating in the K-12 school environment of the Bigg County Public School System located in Northeast Georgia. The targeted population for the study was the K-12 school administrators, thus participants were required to be over the age of 18 and be employees of the school system in a principal, assistant principal, or associate principal role. Participants were required to provide consent to participate in the study to demonstrate their voluntary participation and document that I had informed them regarding the purpose and procedures of the study, of their rights and protections, and any risks or benefits to participation.

As noted in the preceding “Limitations” section of this paper, this research was limited to the study of K-12 school administrators as opposed to other faculty, staff, or students. Other groups than those studied may hold differing information security thoughts and beliefs and may be more motivated to comply with or do not intend to violate information security (Crossler et al., 2013). I acknowledge that study results may not be generalizable to the entire population of K-12 computer end users. The following “Population and Sampling” section provides discussion and justification for focusing on this population along with generalization discussion as it applies to other K-12 computer user groups. The upcoming “Study Validity” section of this paper presents a discussion of concerns related to study generalizability, transferability, and selection bias.

Convenience sampling occurs when study participants are easily accessible by the researcher and conveniently available for study participation (Acharya, Prakash, Saxena, & Nigam, 2013; Bornstein, Jager, & Putnick, 2013; Landers & Behrend, 2015). This was the case for this study. The target school system's institutional review board (IRB) granted access to the population. Internal employees have access to the list of K-12 administrators via provided directories and thus this list was available for this research.

IRB evaluation by the sponsoring university and the internal IRB of the participant location is intended to ensure that the researcher follows ethical research practices (Johnson et al., 2013; Lange, Rogers, & Dodds, 2013; Spurlin & Garven, 2016). Examples of ethical practices to be followed include allowing voluntary participation and withdrawal in the study, protection of participants' identity, and holding participants harmless from participation (Mahon, 2014; Rhodes, 2014; Whicher et al., 2015). The following "Ethical Research" section of this paper discusses ethical practices for this study in detail. Email communication that explained the purpose of the study and the protections afforded through participation established a working relationship with the participants.

Research Method and Design

A research methodology defines the conceptual approach that a researcher will take in the investigation of a topic (Yoshikawa et al., 2013). These methods shape the type of data gathered, how data are gathered and analyzed (Turner et al., 2013), and are driven by a study's research question(s) (Fetters et al., 2013) as well as the perspective of the researcher (Sparkes, 2015). The two primary methodologies are quantitative and qualitative (Turner et al., 2013) with a third being mixed methods which combines the two primary methods (Heyvaert et al., 2013). With each methodology lies research designs that outline how the researcher will execute a study and how the findings of the study address the research question (Turner et al., 2013). A broad range of methods and designs have become available due to changes in globalization and access to data; however, research methods should not be developed for the sake of invention but instead only be driven by being the proper means by which to answer a study's research question (Tavakol & Sandars, 2014a, 2014b).

This study used a quantitative methodology and a correlational design. It was important for this study to use a design similar to extant literature to be relevant and comparable in order to add further empirical and statistical evidence to the existing conversation. Due to the primary difference in this study when compared to existing studies was the addition of factors to measure and a change in population, if the methodology was also deviated, comparison to extant literature would be difficult. The following sections provide further discussion and justification of the methodology and design selected as well as evaluation of alternative approaches.

Method

The epistemological and ontological perspective of the researcher is one driver for method section (Sparkes, 2015; Yilmaz, 2013). Quantitative research is a method that approaches studies from the worldview of the postpositivist where the researcher approaches the subject matter from the viewpoint that there is a singular reality and phenomena in that reality can be objectively measured by applying statistics to empirically gathered data (Tavakol & Sandars, 2014a). This is in contrast to the naturalistic worldview associated with qualitative research where the viewpoint is that multiple realities exist and the researcher can only observe phenomena, not predict it (Tavakol & Sandars, 2014a). Holding a postpositivist worldview represents one criterion that supported the selection of a quantitative methodology for this study.

Beyond the worldview of the researcher, the research question of the proposed study informs the research methodology (DeLyser & Sui, 2013). If a research question is asking *how* or *why* phenomena occur in order to obtain understanding, a qualitative methodology is appropriate (Hales, Lesher-Trevino, Ford, Maher, & Tran, 2016; Tavakol & Sandars, 2014b; Yilmaz, 2013). If a research question concerns obtaining a measurement by asking *how many*, *how often*, or to *what level* particular independent variables influence a dependent variable, a quantitative methodology is appropriate (Turner et al., 2013). In this study, I desired to understand to what extent attitude toward the behavior, subjective norm, and perceived behavioral control affected the intention of computer end users in a K-12 environment in the Bigg County Public School System located in Northeast Georgia to follow information security policy. Applying a quantitative methodology achieved the proper evaluation of this research question.

From a theoretical perspective, sociobehavioral studies often apply an existing theory as their guiding foundation (Lebek et al., 2014). Studies designed to approach a subject through the application of existing theories generally use a quantitative methodology (Turner et al., 2013). A theory comprises independent and dependent variables. Theorists propose that the independent variables of the theory affect the dependent variable(s) in some manner. The researcher gathers data relative to the independent variables in a situation. Statistical analysis of the gathered data then establishes the affect the independent variable(s) have on the dependent variable(s) and becomes the foundation of discussion for the study. Alaskar et al. (2015) confirmed the most popular methodology for information security studies applying sociobehavioral theories as quantitative.

Methodology represented a significant gap identified in the current information security behavior literature. The quantitative approach limits the researcher to quantifying if the independent variables identified in the proposed theoretical framework do or do not exist as factors that influence intentions to comply with information security policy (Crossler et al., 2013). This approach limits the researcher from identifying other factors that may be influencing noncompliant behaviors (Crossler et al., 2013) or integrating other factors into the model as suggested in the rival explanations theory discussed in a previous section of this paper. Research methodologies other than quantitative would be required to address this gap.

Since the mid-1980s, the qualitative research method has seen increased use in the extant literature while the quantitative has decreased (DeLyser & Sui, 2013). Qualitative research would allow for exploratory investigations in identifying motivational factors that exist in an organization in regards to complying with information security policies (Flores et al., 2014). This research could be performed as a case study (R. K. Yin, 2013) limited to identifying motivational factors based on established theories, or a grounded theory (Turner et al., 2013) approach could be implemented to identify motivational factors in the development of new frameworks. These qualitative approaches could serve to identify motivational factors relevant to particular cultures, industries, or geographical regions (Crossler et al., 2013). These approaches were not appropriate for this study as the desire was not to identify motivational factors (independent variables) but to measure the affect of those in TPB; thus, there was an epistemic misalignment with the qualitative approach. Other qualitative methodologies do exist such as ethnography, phenomenology, and narrative (Hales et al., 2016; Turner et al., 2013), but these are exploratory in nature and represented a worldview misalignment at an ontological level.

Mixed methods research involves the combination of quantitative and qualitative disciplines (Fetters et al., 2013). This design intends to provide a rich and complex perspective to a problem and deliver validity and reliability of the study through the use of multiple data sources and analysis (Heyvaert et al., 2013; Tricco et al., 2016). The epistemological perspective here is that information can be described and identified by both descriptive and analytical approaches that support each other and provide equal status (Yoshikawa et al., 2013). Although not necessarily a disagreeable mindset, mixed method research is both time and resource intensive (Venkatesh et al., 2013). Mixed method also extends beyond the scope and scale of the inaugural doctoral study of a new researcher in terms of mixing of ontological perspectives, conceptualization (Heyvaert et al., 2013), and proper synthesis of epistemologically diverse and diverging data (Tricco et al., 2016; Venkatesh et al., 2013; Yoshikawa et al., 2013). Based on these points, the mixed method approach was determined not to be a proper fit for this study.

Research Design

Each research methodology has associated research designs (Turner et al., 2013). The selection of a research design is informed by the sample selection and data gathering and analysis processes required to answer the study research question (Yoshikawa et al., 2013). Designs aligned with the quantitative methodology include experimental, quasi-experimental, survey (Tavakol & Sandars, 2014a), and correlational (Turner et al., 2013). This study employed a cross-sectional correlational design.

The primary drivers to select a correlational design for this study lied in the sample selection process and lack of conditional treatment. One criterion for the experimental design requires random sample selection (Charlwood et al., 2014; Tavakol & Sandars, 2014a) in order to prevent selection bias (Henry et al., 2013). Sample selection in this study focused on a nonrandomly selected population in a singular school system, thus making the experimental design unavailable. Another criteria requirement for both experimental and quasi-experimental designs is the application of a treatment across equally divided samples that a researcher can manipulate between test groups in order to measure effect (Bettany-Saltikov & Whittaker, 2014; Tavakol & Sandars, 2014a). In this study, there was no treatment to apply to the study population upon which to draw measurements thereby rendering both the experimental and quasi-experimental designs inappropriate.

Another consideration in design selection is if the research question seeks to show causation or correlation. Demonstrating causation is the goal of experimental designs as the desire is to show that statistical differences between controlled population samples are the direct result of manipulating a treatment (Aguinis & Edwards, 2014; Charlwood et al., 2014; Vaidyanathan et al., 2016). Correlation is a statistical measurement of how much of the statistical change in a dependent variable maps to the statistical change in an independent variable (Bettany-Saltikov & Whittaker, 2014). Correlation does not rule out the possibility that factors other than the measured independent variable(s) could be the cause for variations in the dependent variable (Turner et al., 2013).

From an epistemological perspective, correlational studies have the ability to well reject a hypothesis but do not definitively identify the only variables present affecting a dependent variable (Charlwood et al., 2014). However, correlations can be considered sufficient in showing significance between the theory variables (Aguinis & Edwards, 2014; Charlwood et al., 2014; Vaidyanathan et al., 2016). Correlation is an appropriate statistical approach for many research designs and studies (Bettany-Saltikov & Whittaker, 2014). Correlation was a good fit for this study as I desired to answer to what extent the independent constructs of TPB effected the dependent variable of TPB in the context of information security behavioral intention in the study's target population.

The extant literature often uses the research design terms of correlational (Turner et al., 2013) and survey (Tavakol & Sandars, 2014a) interchangeably. However, they are distinctly different designs. It is common that correlational studies do deploy surveys as data gathering techniques, but a correlational design can be applied to data gathered in other manners such as observation or testing (Turner et al., 2013). Similarly, studies designed around survey-collected data typically have the data analyzed in a manner to show correlation. However, there is the possibility to seek causation if proper control factors are in place (Vaidyanathan et al., 2016).

In the survey design data are gathered through the development and delivery of written or oral survey questions that represent the independent variables of a theory in a relevant way to the study's topic and research question(s) (Turner et al., 2013). The responses to the survey questions are then analyzed statistically to accept or reject the study hypotheses (Bettany-Saltikov & Whittaker, 2014). Less common in the existing literature, but a more appropriate term for survey and correlational designs, is the term descriptive design which defines studies seeking to describe the way conditions are in the world (Turner et al., 2013). This term is also often interchanged with survey design as many descriptive design studies use surveys to collect data (Turner et al., 2013). For this study, the term survey described the data collection technique, and the term correlational described the research design. The lack of experimental design implies the fact that this study was descriptive in nature and does not require explicit statement of this fact.

Research design can also reference the timeframe for data collection (Yoshikawa et al., 2013). Studies can be cross-sectional where a researcher gathers data at a singular point in time (Tavakol & Sandars, 2014a) or longitudinal where data are gathered at multiple intervals over a period of time (Turner et al., 2013). Longitudinal studies provide the ability to analyze changes over time. However, this was not the desired goal of this study. The desired goal was to capture the effect of the theory variables on information security behavioral intentions at a singular point in time with a specific population in order to provide current, relevant, and actionable data to information security program managers for the development and improvement of effective security controls in the form of SETA programs.

Population and Sampling

In this study, I sought to contribute to the existing body of knowledge regarding independent constructs of TPB that may influence intentions to comply with information security in order to improve SETA programs. The literature review exposed a gap regarding the participants of existing studies being limited largely to corporate environments and some academia at the university level (Cox, 2012; Herath & Rao, 2009; Ifinedo, 2014; Safa et al., 2015; Siponen et al., 2014). However, research of this topic in the K-12 school environment had not occurred. This study filled this gap by performing this research in the previously unexplored K-12 academic environment.

The K-12 environment may offer motivations at the peer, societal, and performance levels that may be unique from other environments (Kim, Kim, Lee, Spector, & DeMeester, 2013; Metcalf, 2012; Misenheimer, 2014; Raman, Don, & Kasim, 2014) making this research relevant and valuable as it adds to the existing literature. Factors such as organizational narcissism and reward were applied in the study to determine if they influenced the independent variables of TPB in the K-12 educational environment as opposed to the corporate environment researched by Cox (2012) and I sought to add this knowledge to the findings of previous research. The logic that underlain the factors in this study were as follows:

a. The existence of an organizational narcissistic attitude, perceptions of information security risks, and/or the existence of rewards for following information security are significant to forming an attitude toward information security compliant behavior intentions.

b. Influence of various internal and external forces is significant to forming subjective norm toward information security compliant behavior intentions.

c. The level of feeling responsible and capable of complying with information security is significant to forming perceived behavioral control toward information security compliant behavior intentions.

The population for this study was the 699 K-12 school administrators of the Bigg County Public School System located in Northeast Georgia. The definition of K-12 school administrators for this study was individuals currently employed in principal, assistant principal, and/or associate principal roles. These participants aligned with the study research question, as they were all computer end users currently operating in a K-12 school environment. I recognized in this study that other types of computer end users exist in the K-12 environment including other faculty, staff, and students.

K-12 administrators represent the leaders and decision makers for technology implementation and information security at the individual school level (Blau & Presser, 2013; Metcalf, 2012; Raman et al., 2014; Weng & Tang, 2014) much as senior management in corporations (Barton et al., 2016). For K-12 faculty and staff, this means that exposure and guidance for technology and policy is largely disseminated through the K-12 administration (Metcalf, 2012). In observations of the environment, both populations are similar in use case as they have largely independent and unencumbered usage of technology, have exposure to the same or similar information security policies, are under indirect supervision, and are largely the target of SETA programs developed by information security program managers. Generalizability of information systems research can happen at four different levels: Generalizing from data to description, generalizing from description to theory, generalizing theory to description, and generalizing from concepts to theory (Lee & Baskerville, 2003). In this study, generalization from data to description was possible as the findings of the study sample could generalize to the unstudied population of K-12 faculty and staff due to the similarity in use case.

Regarding the K-12 student population, based on observation of the environment, the use case for K-12 student computer users is different in that they use computers in this environment under limited access, strict direction, and direct supervision. There is also an expectation that the measures for the independent variables of TPB may be different for the adolescent student population. This is in line with Ajzen's (2002) expectation of measures to differ between populations when applying TPB. Observation has also shown this group can be the target of SETA programs, but exposure is not direct from the information security program managers but passed down through administration and faculty. It is possible for the results of this study to generalize from description to theory (Lee & Baskerville, 2003). This suggests that the findings support the application of the chosen theory (TPB) to this larger population. However, this would require empirical validation.

The target organization was a single, large urban school system in the state of Georgia in which I maintained employment. The school system is one of the largest in the U.S. and the recipient of several national awards. The size and reputation of this school system makes it a desirable research environment for both internal and external researchers and it provided a rich setting for this study.

Convenience sampling occurs when study participants are easily accessible by the researcher and conveniently available for study participation (Acharya et al., 2013; Bornstein et al., 2013; Landers & Behrend, 2015). This was the case for this study. The convenience sampling method for this study involved sending a study participation invitation to all members of the population and accepting the responses of whoever in the population decided to participate until reaching or exceeding the minimum sample size described below. There was no application of an exclusion process or exclusion criteria to identify whom in the study population received an invitation to participate. Sending of invitations occurred across all grade levels (elementary, middle, and high) and included all demographic groups in the organization. The organization provided the sampling frame (Acharya et al., 2013) in the form of email and directory listings available to all internal personnel in the target organization.

Convenience sampling is nonprobabilistic as the sample does not consist of a predetermined selection of participants from the population but instead consists of those volunteering to participate (Acharya et al., 2013; Landers & Behrend, 2015; Palinkas et al., 2015). Nonprobabilistic sampling has the issue of only being generalizable to the study sample (Bornstein et al., 2013; Jafarkarimi et al., 2016; Landers & Behrend, 2015). However, this approach is time and cost efficient (Acharya et al., 2013; Bornstein et al., 2013; Weinberg, Freese, & McElhattan, 2014).

Stratification of a target population is performed when demographic variables are considered major influences of the study variables (Acharya et al., 2013; Bornstein et al., 2013). Stratification in this study did not occur, as there was no consideration or expectation for demographic variables being major influencers of the study variables. However, some demographic information was gathered and reported for extending the discussion and held out as a basis for future research. Lack of stratification does have the disadvantage of not exposing differences in sociodemographic subgroups (Bornstein et al., 2013). However, there was an assumption in this study that the sample had exposure to similar levels of SETA balancing differences between subgroups.

An *a priori* sample size calculation was performed using the statistical software package G*Power version 3.1.9.2 (Faul, Erdfelder, Buchner, & Lang, 2009). This calculation required input values for probability of error, effect size, and number of predictors. Probability of error was set at a = 0.05. A researcher can estimate effect size by reviewing the findings of existing research (Lakens, 2013). A mean effect size of f^2 = .30 was calculated across eight studies most closely related to the proposed study represented in the literature review (Chatterjee et al., 2015; Cox, 2012; Dinev & Hu, 2007; Hu et al., 2012; Ifinedo, 2012, 2014; Safa et al., 2015; Siponen et al., 2014) where intended behavior was the dependent variable. The number of predictors in TPB is three (Ajzen, 1991). The result was a sample size of 41 to achieve a power of .80 and 62 to achieve a power of .95 (Figure 2).

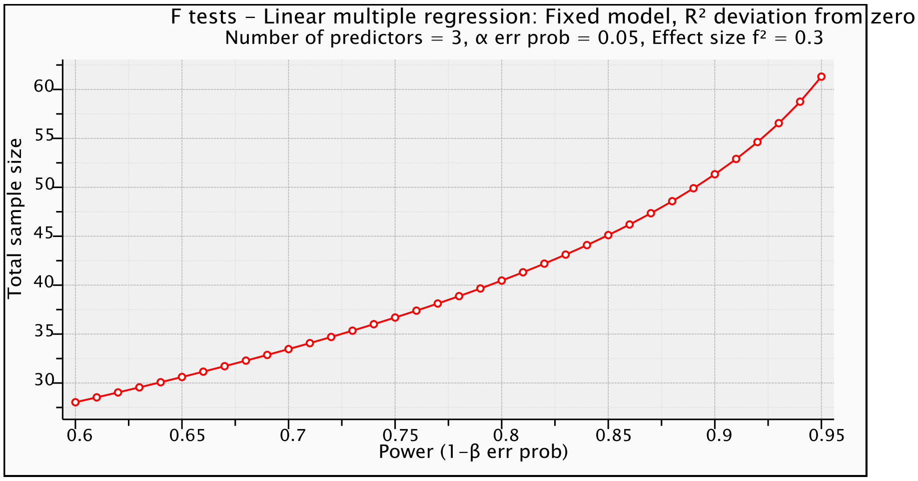

Figure 2. Power represented as a function of sample size.

Ethical Research

Researchers must perform human participation research ethically, and the U.S. federal government regulates such research requiring the minimization of participant risks, performing research where the risk and benefits are fairly balanced, where the researcher appropriately recruits human subjects, participants provide consent for participating, have their privacy protected, and safety monitored (Johnson et al., 2013; Mahon, 2014). A currently held Certificate of Completion from the National Institutes of Health (NIH) Office of Extramural Research provided evidence of training in protecting human research participants. Submission to and approval by the Walden University IRB of this study was a requirement prior to performing any research (approval number 04-19-17-0488547). IRB review is intended to verify systematic interventions are in place to protect human research subjects (Whicher et al., 2015). The target organization for this study had their own IRB process and this study gained their review and approval as well prior to commencing (see Appendix C).

All individuals in the research population meeting the job position criteria outlined in the “Participants” section of this paper received invitations to participate in this study via email. There were no other criteria for receiving this invitation. A list of contacts made available by being an employee in the same organization provided a frame for sending the email. This same communication contained an informed consent form that outlined the study purpose, role of the researcher, role of the participant, and methods of ethical practice and research. No participant received any monetary or other valuable incentives to participate. Participants could withdraw from the study at any time without harm or penalty by not completing and submitting the study survey. Participants received contact information for me as well as the university in order to ask questions about the research or their rights. The participant provided consent by clicking an Internet link to access the study survey and submitting a completed survey.

The participants completed a Web-based survey that did not gather any individually identifying information providing privacy and confidentiality. Submission of the completed survey was anonymous; thus, no one was aware of the identity of any participant. The reporting process provided further identity protection by not reporting the participating organization, and not reporting individual information but only cumulative and statistical information derived through the data analysis process. Notification in the consent form advised participants that study data retention occurs in electronic format and is securely stored in a locked cabinet for five years as required by Walden University.

Instrumentation

Measurements

In this study, measurement of the independent constructs of TPB (attitude, subjective norm, and perceived behavioral control) was by measurable factors that extant literature showed to be relevant to the formation of that construct. These factors were organizational narcissism, perceived vulnerability, perceived severity, reward, normative beliefs, locus of control, and self-efficacy. School systems often promote school administrators as being the central element of the organization and grant them sole governance of their school, staff, and faculty in the system (Blau & Presser, 2013; Metcalf, 2012; Raman et al., 2014; Weng & Tang, 2014). This provides the opportunity to drive organizational culture which has been shown to have a significant influence on individual beliefs (Ashenden & Sasse, 2013; Hu et al., 2012). Given that the population in this study largely has autonomous control of their environment, this factor merited consideration. Based on the above arguments, I included organizational narcissism as a factor influencing the attitude toward the behavior independent construct.

As discussed in the literature review, it has been shown that the inclusion of motivational factors from PMT increase the predictive effectiveness of TPB (Sommestad et al., 2015). Existing literature has demonstrated correlations between the perceived vulnerability, perceived severity, and reward factors and the independent construct of attitude toward the behavior. Based on these points these factors were included in this study.

In this study, I suggested that in the K-12 educational environment the study population develops normative beliefs from a wide range of sources such as senior management, peers, students, parents, and community. This range of influential sources may be significantly different from those of corporate environments and may represent a meaningful distinction compared to similar extant research. The inclusion of this factor may add to this conversation and be significant in this research study.

The use of locus of control and self-efficacy factors has been substantiated in existing literature as being applied in the same manner as the proposed study and showing existing correlation (Cox, 2012; Ifinedo, 2014; Lebek et al., 2014). Literature has shown that understanding the current measures of these factors in an environment is important to the development of quality SETA programs (Posey et al., 2014). The established value of these factors and their established correlation to the perceived behavioral control independent construct justified these factors as important for inclusion in this study. The reader should review the "TPB and the theoretical framework for this study" section and summary Table 1 of the literature review for complete extant literature discussion and justification of these measures.

Measurement Instrument

A Web-based survey using previously validated instruments present in existing research using the same or similar theory and subject matter provided data collection for this study. The close alignment to existing related research and established collection methods supported this approach as being appropriate for this study. Content validity and reliability was established by performing an extensive literature review that validated and supported measurement factors used and by using instruments and survey questions validated in previous research that provided direct relevance to the theory being tested (Cook, Zendejas, Hamstra, Hatala, & Brydges, 2014; Finn & Wang, 2014; Jorg Henseler, Ringle, & Sarstedt, 2014). The literature review in this paper provided sufficient data to meet these criteria and this study utilized survey questions validated in prior research. Testing for multicollinearity as described in the upcoming "Data Analysis" section provided discriminant validity. The survey contained 34 total questions (7 demographic, 11 factor measurements, and 16 personality test) and pretesting showed the study participant could complete the survey in approximately ten minutes.

The 11 factor measurement questions were directly from a previous study applying TPB to information security behavior intention in a corporate environment of computer end users (Cox, 2012) and were used by permission (see Appendix A). Cox addressed validity of the questions via a thorough literature review, using questions from established research (Workman et al., 2008), citing multiple sources that support the context of the questions in terms of the construct they were intended to measure, and minimally editing questions to fit the context of the survey and meet participation understanding. Research into the root source for these questions determined some come directly from Workman et al. without edit and were also used by permission (see Appendix A). All other questions were determined to be unique to Cox and thus the permissions granted were sufficient for use. Cox established construct reliability through partial least squared (PLS) analysis of path coefficients and testing significance of those paths. An additional question measuring the added factor of reward (related to the attitude independent construct) was added based on existing research (Cox, 2012; Posey et al., 2014) and edited to match other factor measurement questions.

The 16 personality questions were taken from the Narcissistic Personality Inventory-16 (NPI-16; Ames, Rose, & Anderson, 2006) and were used by permission (see Appendix A). The survey respondents selected which of the two statements in each selection best matched how they viewed themselves. Researchers established the validity of the NPI-16 through administering five separate studies using well-established instruments to measure various NPI-16 target areas and the NPI-16 itself. Analysis showed the NPI-16 to be valid at measuring the desired indicators using a shortened format (Ames et al., 2006). Reliability was established through test-retest cycles (Ames et al., 2006). The NPI-16 has been used in previous IT research with corporate computer users (Cox, 2012) to measure the same attitude factors as applied in this study. Researchers have also used it in a number of diverse studies where using a longer personality test may have distracted from the study intentions (Ames et al., 2006) including job satisfaction among public sector employees (Mathieu, 2013), comparison of personality trait scales among university students (Austin, Saklofske, Smith, & Tohver, 2014), and bullying on Facebook among university students (Kokkinos, Baltzidis, & Xynogala, 2016). A graphical mapping of survey questions to the variables they measure is in Figure 3. Appendix B contains a complete list of survey questions.

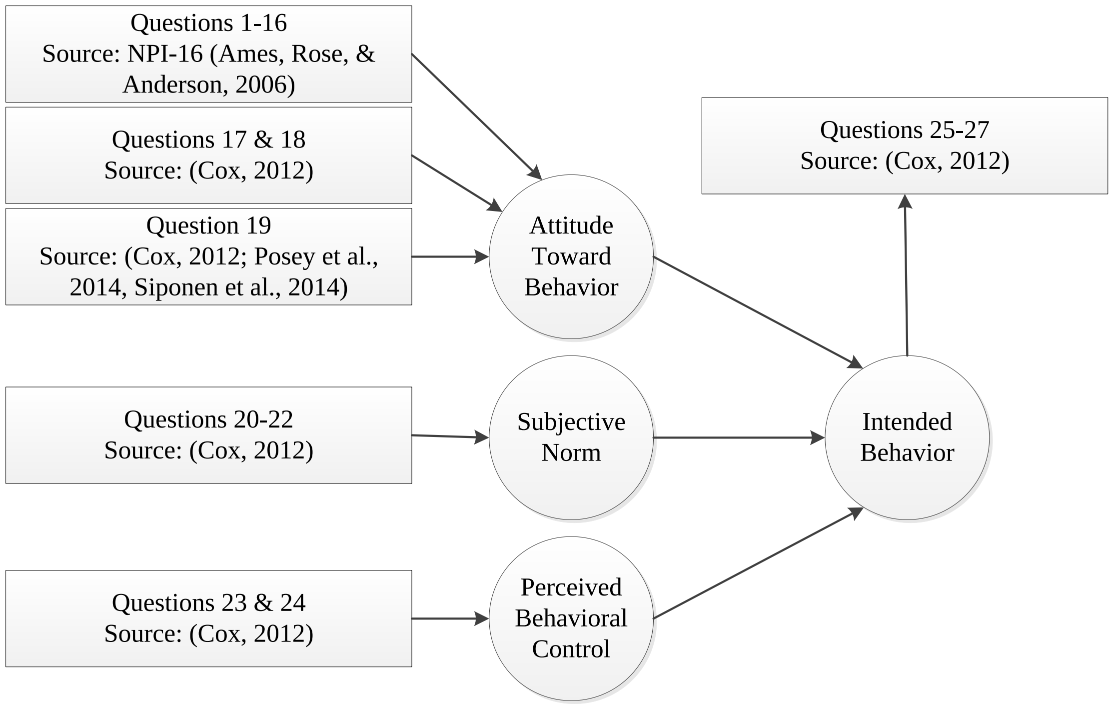

Figure 3. A mapping of survey questions to the research model. Identifies the questions that measure for each variable with the question sources. Theory variables are in circles; survey question information is in squares.

Appendix B does not list the survey questions in the order that they were in the actual survey. Appendix B lists the questions in order of relation to the constructs in the research framework and contains reference citations (where applicable). In the actual survey, demographic and qualification questions were first, followed by a randomization of all measurement questions. Randomization of measurement questions is intended to reduce method and response biases by separating constructs (Jakobsen & Jensen, 2015; Navarro-Gonzalez, Lorenzo-seva, & Vigil-colet, 2016). Questions in the personality test were last and remained in nonrandomized order to maintain the integrity of the test (Ames et al., 2006). Creation and administration of the survey instrument was via

SoGoSurvey (https://www.sogosurvey.com), a secure Web-based survey management portal. As a further protection to study participants' and organization anonymity, publishing of raw survey data did not occur and are only available through direct request.

Survey questions represented and provided a measure of each factor that defined a related construct. Usage of one question for each factor (except organizational narcissism and normative beliefs, which result in a single value) prevented any factor from having a greater weight in the formation of the final value of any independent construct. The factor measurement questions used Likert or semantic differential scales to determine an ordinal value for each question. The Likert scale questions measured a range of agreement with the presented question with values ranging from 1-5. The semantic differential questions used adjectives to represent the respondent's attitude or belief toward the proposed question and had a value range of 1-5. This approach was similar to that used by Ajzen (1991). The assigned values indicated where a respondent's attitude or belief fits on a scale of most (highest value) to least (lowest value) desirable from an information security perspective. Table 2 provides a detailed breakdown of these measurement relationships.

Table 2

Survey Question Value Assignments

Question	Factor	Theory construct	Response range	Value
1-16	Organizational narcissism (NAR)	Attitude	Cumulative	0 - 16
17	Perceived vulnerability (PVUL)	Attitude	Unlikely - Likely	1 - 5
18	Perceived severity (PSEV)	Attitude	Harmless - Severe	1 - 5
19	Reward (REW)	Attitude	Unlikely - Likely	5 - 1
20	Normative beliefs (NB1)	Subjective norm	Agree - Disagree	5 - 1
21	Normative beliefs (NB2)	Subjective norm	Agree - Disagree	5 - 1
22	Normative beliefs (NB3)	Subjective norm	Agree - Disagree	5 - 1
23	Locus of control (LOC)	Perceived behavioral control	My employer - Myself	1 - 5
24	Self-efficacy (SE)	Perceived behavioral control	Agree - Disagree	5 - 1
25	Intended behavior (IB1)	Intention	Agree - Disagree	5 - 1
26	Intended behavior (IB2)	Intention	Agree - Disagree	5 - 1
27	Intended behavior (IB3)	Intention	Agree - Disagree	5 - 1

Note. Response range values for each survey question in relation to the factor measured and the related theory construct.

The independent variables of TPB are composite variables. The organizational narcissism, perceived vulnerability, perceived severity, and reward measures determined the attitude independent variable. Organizational narcissism was determined in the study through the use of the NPI-16 (Ames et al., 2006) personality test. Each question in the personality test where the selected element does not represent narcissism scored a value of one (see Appendix B). All other personality test responses scored a value of zero. Summation of the values determined a measurement value for this factor. Determination of the values for perceived vulnerability, perceived severity, and reward was by the ordinal value of the response for each survey question related to the factor. Summation of all factor values determined a value for the attitude toward the behavior independent construct.

Values for the normative beliefs factor that comprises the subjective norm construct was by the ordinal value of the response for each survey question related to the factor and summation of these values determined a value for the subjective norm independent construct. The same applied to the locus of control and self-efficacy measures that comprised the perceived behavioral control independent construct. Determination of values for the intended behavior factors was in the same manner and summed to represent the intention dependent variable.

Data Collection Technique

As mentioned in an earlier section, data collection in this study took place via the use of an Internet survey. The use of Web-based surveys are common in data collection due to convenience, low cost, and quick turnaround (Ansolabehere & Schaffner, 2014;

Mlikotic, Parker, & Rajapakshe, 2016). Support exists in the extant literature for the use of Web-based surveys for anonymous broad scale data gathering (Herath & Rao, 2009; McCormack, Friedrich, Fahrenwald, & Specker, 2014; Mlikotic et al., 2016; Tavakol & Sandars, 2014b). This method aids in providing anonymity for the survey participants as actions related to information security can be sensitive in nature and can result in more accurate self-reporting (Albaum, Roster, Smith, Albaum, & Smith, 2014; Gnambs & Kaspar, 2014; Weigold et al., 2013). If respondents perceive a risk of recognition they could try to give socially desirable answers that may introduce response bias into the study reducing validity (Krumpal, 2013). Data gathered via Web-based survey are generally ready for analysis without further interpretation and is convenient for both the researcher and study participant (Weigold et al., 2013). Disadvantages of Internet surveys include a lack of motivation to participate or complete a survey that may not exist with direct personal contact (Ansolabehere & Schaffner, 2014; Gnambs & Kaspar, 2014; McCormack et al., 2014; Mlikotic et al., 2016).

Alternatively, I could have performed the survey in person, via pencil and paper, or through postal mail. However, this would have negated the benefits cited for an anonymous method and literature showed that response results would not necessarily improve (Ansolabehere & Schaffner, 2014; McCormack et al., 2014; Mlikotic et al., 2016; Weigold et al., 2013). In lieu of a survey, I could have subjected the study population to a live scenario and observed reactions. However, this was not practical due to time, cost, and high potential for ethical issues if I did not handle the scenario properly and the population perceived it as deceptive or manipulative (Mahon, 2014). Randall

(1991) and Efrat (2013) suggest that direct questions may be superior to scenarios further supporting the survey method.

The creation of a Web-based survey using the questions in Appendix B and entering them into an Internet survey tool under a private account was the first data collection step. The survey tool generated a link to the web survey. Next was the generation of an email containing the study consent form and survey link. Distribution of the email occurred to a small group of nonstudy participants in the target organization to verify functionality, but retention of data gathered did not take place. A pilot study was not required as the survey used questions and measures already validated in extant research (see "Instruments" section for detail). Upon confirmation of email and survey functionality, distribution of the email to the study population followed. Monitoring for response rate happened over one week. In the case of low response rate, the sample population was to receive a reminder request via email, and this did happen. Once data gathering via the web survey was complete, an export provided the data for analysis.

Data Analysis

The following two sections are restatements of the research question and hypotheses from Section 1:

Quantitative Research Question

> RQ: To what extent does attitude toward the behavior, subjective norm, and perceived behavioral control affect the intention of computer end users in a K-12 environment in the Bigg County Public School System located in Northeast Georgia to follow information security policy?

Hypotheses

Formation of the hypotheses for this study occurred based on the constructs exhibited in the study framework and research model. Data analysis determined the correlation of these constructs in order to accept or reject the null hypothesis. The specific hypotheses for this study were:

$H1_0$: Attitude toward the behavior, subjective norm, and perceived behavioral control does not affect the intention of computer end users in a K-12 environment to follow information security policy.

$H1_a$: Attitude toward the behavior, subjective norm, and perceived behavioral control does affect the intention of computer end users in a K-12 environment to follow information security policy.

Data Analysis Approach

Researchers use correlation and regression data analysis techniques to demonstrate the relationship of one or more independent variables to one or more dependent variables (Y. Chen, Li, Wu, & Liang, 2014; Halfens & Meijers, 2013; Lowry & Gaskin, 2014) which was the goal of this study. Several bivariate and multivariate techniques exist to perform such analysis. Bivariate statistics involve a single independent and dependent variable (Tavakol & Sandars, 2014b). TPB contains multiple independent variables, thus bivariate approaches were not appropriate. Multivariate approaches are needed for models containing multiple independent variables and/or multiple dependent variables and utilize regression, path analysis, factor analysis, or principal components analysis (Mertler & Reinhart, 2017).

Factor analysis and principal component analysis techniques utilize latent factors (Astrachan, Patel, & Wanzenried, 2014; Chou & Chou, 2016; Hair, Ringle, & Sarstedt, 2013; Lowry & Gaskin, 2014; Ringle & Sarstedt, 2016) and are generally used for theory development or testing (Mertler & Reinhart, 2017) which was not a goal of this study. Path analysis estimates causal relations (Skorek, Song, & Dunham, 2014) and this was inappropriate for this study as I acknowledged that other factors might affect the dependent variable of TPB other than the interdependent variables included in the theory. Some researchers use different regression techniques to show the significance of differences between groups. This includes techniques such as *t*-tests, ANOVA, ANCOVA, MANOVA, and MANCOVA (Ord, Ripley, Hook, & Erspamer, 2016; Tonidandel & LeBreton, 2013). This study did not involve the comparison of multiple groups rendering comparison-oriented regression approaches inappropriate as well.

Data analysis in this study was via multiple linear regression. There were several justifications for the multiple linear regression approach. Multiple linear regression is a multivariate regression process intended to measure multiple predictors in order to account for the variance of a single dependent variable (Y. Chen et al., 2014; Granato, de Araújo Calado, & Jarvis, 2014; Jung & Kim, 2014; Mertler & Reinhart, 2017). This description matched the theoretical model and intention of this study. Researchers regularly use multiple linear regression in information systems studies in general (Ayatollahi et al., 2013; Y. Chen et al., 2014; van Deursen & van Dijk, 2013) and they recommend its use in studies applying TPB (Beville et al., 2014; Hankins, French, & Horne, 2000; MacFarlane & Woolfson, 2013; Sommestad et al., 2015; Tipton, 2014).

Multiple linear regression is also a common data analysis approach in similar existing studies applying sociobehavioral theories to information security (Al-Mukahal & Alshare, 2015; John Opala, Rahman, & Alelaiwi, 2015; Klein & Luciano, 2016; Said, Abdullah, Uli, & Mohamed, 2014).

Data Screening

Data screening is a necessary process that a researcher must perform before data analysis in order to provide accurate statistical analysis and draw valid conclusions (Mertler & Reinhart, 2017; Rutkowski & Zhou, 2015; Williams, Grajales, & Kurkiewicz, 2013). The data screening process involves verifying the accuracy of data collected, addressing missing data, checking for outliers, and validating that the basic data assumptions for multiple linear regression are met (Casson & Farmer, 2014; Flores & Ekstedt, 2016; Lowry & Gaskin, 2014). The basic data assumptions are normality, linearity, homoscedasticity, and multicollinearity (Berenson, 2013; Hannigan & Lynch, 2013; Tipton, 2014; Williams et al., 2013). Meeting data assumptions lends to the "robustness" of parametric tests such as multiple linear regression (Wiedermann & Von Eye, 2013).

IBM SPSS software version 23.0 (IBM Corp., 2015) was used to provide all data analysis. Demographic statistics provided number and percentage of respondents, demographic characteristics, and answers to qualification questions. Descriptive statistics exist for each factor measurement reporting median scores and standard deviations. Review of the raw data and descriptive statistics aids in verifying the accuracy of data collected and locating missing quantitative data (Mertler & Reinhart, 2017). Accuracy of data also means ensuring that all data properly represents the concept of each measure. Some measures may require inversion of values to represent the correction direction of intent as identified in Table 2.

Missing data can lead to inaccurate statistical results and may identify data collection issues (Mertler & Reinhart, 2017). Discarding controlled for surveys where the participant skipped the qualification questions or answers to the qualification questions regarding age, professional role, and/or computer use disqualified the participant from the study. Cases with demographic questions skipped still had quantitative data included in the study. Discarding occurred for single cases missing over 50% quantitative data. A guideline for how to address measures missing data is determining if 15% or more of data are missing (Mertler & Reinhart, 2017). Measures missing less than 15% quantitative data had the data replaced with the mean score for the measure. If 15% or more of data were missing for a particular measure, removal occurred for that measure during calculation of the related independent variable's value.

After final calculation of composite variable values as described in the above "Measurements" section, the next step was to identify outliers. Outliers are cases where the value for one or more variables differs to an extreme at either end of a sample distribution enough to distort statistical results (Mertler & Reinhart, 2017; S. Yin, Wang, & Yang, 2014). Univariate outliers are cases where a single variable is far from the mean. Multivariate outlier cases have more than one variable with an extreme value. Creation of box plots identify univariate outliers (Mertler & Reinhart, 2017) and were used for this purpose in this study. Review of univariate outliers identifies reason and aids in determining whether to drop the case(s). Mahalanobis distance calculation determined cases far from the centroid of all variables (Mertler & Reinhart, 2017). After identification of univariate outliers, execution of the Mahalanobis distance process determined multivariate outliers. Discarding occurred for cases with multivariate outliers.

Meeting the assumptions of normality, linearity, homoscedasticity, and multicollinearity is a requirement when performing multiple linear regression (Casson & Farmer, 2014). Normality refers to a sample distribution being spread across a range starting from central tendency by a measure of standard deviation (Mertler & Reinhart, 2017). Assessment of univariate normality was through the review of histograms, normal Q-Q plots, skewness and kurtosis values, and results of Kolmogorov-Smirnov tests of normality (Mertler & Reinhart, 2017) and represented the assessment approach for each variable in this study. Variables should plot along a linear line of expected values, have skewness/kurtosis values near zero, and show a strong significance level of normality (Mertler & Reinhart, 2017). A scatterplot matrix provides an initial analysis of the linear relationship between the independent and dependent variables and provides a check for multivariate normality (Casson & Farmer, 2014) and I used one as such in this analysis process. Data are expected to present in an elliptical shape (Mertler & Reinhart, 2017).

Linearity refers to the assumption that straight line relationships existing between variables (Harry Yang, Novick, & LeBlond, 2015). A residual plot will validate linearity among model variables (Mertler & Reinhart, 2017) and I used one in this study for this purpose. Residuals represent prediction errors between expected and obtained variable values (Lowry & Gaskin, 2014) and should fall in a linear pattern (Bennett et al., 2013; Casson & Farmer, 2014; Lee, 2014; Prapavessis et al., 2015). The expectation is for a rectangular pattern and clustering of values would represent nonlinearity (Mertler & Reinhart, 2017).

Homoscedasticity is the assumption that the variance in scores for one variable is close to the same for other variables in the model (Williams et al., 2013). Initial checking for homoscedasticity can occur through the review of scatterplots (Berenson, 2013; Grabemann, Mette, Zimmermann, Wiltfang, & Kis, 2014) and occurred during the review of the scatterplot generated during normality testing. Bivariate plots between the independent and dependent variables should be of similar width throughout with bulging in the middle (Mertler & Reinhart, 2017). Levene’s test is another check for homoscedasticity (Bettany-Saltikov & Whittaker, 2014) and I performed this test as the final check for homoscedasticity. A nonsignificant result indicates homogeneity of variance (Mertler & Reinhart, 2017).

Multicollinearity is a condition where intercorrelations exist between independent variables (Astrachan et al., 2014; Hannigan & Lynch, 2013; Williams et al., 2013). If two variables are highly correlated, it means they essentially contain the same information and are measuring the same concept (Hair, Ringle, & Sarstedt, 2011; Ingenhoff & Buhmann, 2016; Mertler & Reinhart, 2017). The calculation of collinearity statistics measuring for tolerance and variance inflation factor (VIF) determines multicollinearity (Chou & Chou, 2016; Klein & Luciano, 2016; Moody & Siponen, 2013) and was the approach for this study. Tolerance at or above 0.1 and a VIF of 10 or less will demonstrate lack of multicollinearity (Hazen, Overstreet, & Boone, 2015; Ingenhoff & Buhmann, 2016; Mertler & Reinhart, 2017).

In the case of assumption violations, several corrective measures are available to allow the analysis of data to continue. Corrective measures include omission of measures and/or variables, bootstrapping, or application of a mathematical correction such as a square root, logarithm, or z-score transformation (Bennett et al., 2013; Berenson, 2013; Hannigan & Lynch, 2013; MacFarlane & Woolfson, 2013; Mertler & Reinhart, 2017; Tipton, 2014; Weigold et al., 2013; Zemore & Ajzen, 2014). These corrective actions may occur at any of the above stages to the dependent and/or independent variables as required to meet assumptions.

Data Analysis Technique

Multiple linear regression focuses on describing and testing the predictable relationships between independent (predictor) variables and dependent (criterion/response) variables (Nathans, Oswald, & Nimon, 2012). The purpose of applying multiple linear regression is to establish a method of predicting values for the dependent variable for all members of a population (Nimon & Oswald, 2013). Multiple linear regression establishes the correlation between the independent and dependent variables in order to predict how much the independent variables explain the variance of the dependent variable (Mertler & Reinhart, 2017). As related to TPB and this study, multiple linear regression determined how much the independent variables of attitude, subjective norm, and perceived behavioral control predicted the intended information security behavior of the study population.

The analysis of data loaded into IBM SPSS software version 23.0 (IBM Corp., 2015) provided hypothesis testing applying a standard multiple linear regression analysis. The enter method (Mertler & Reinhart, 2017; Nathans et al., 2012) was utilized as it best aligned with the study's research question. Model summary, ANOVA, and coefficients tables provided the information needed for analysis and interpretation. The model summary provided *R*, *R* squared (R^2), and *R* squared adjusted (R^2_{adj}) values. These values, measuring for variance, determined how well the combination of independent variables predicted the dependent variable (Nathans et al., 2012). R^2 values should be high (Lowry & Gaskin, 2014) with values around .75 being substantial, .50 moderate, and around .25 weak (Hair, Hult, Ringle, & Sarstedt, 2016; Sarstedt, Ringle, Smith, Reams, & Hair, 2014).

The ANOVA table provides *F* test and significance values that aid in interpreting the degree of linearity of the model and how significantly the model predicts the dependent variable (Mertler & Reinhart, 2017). Significance should be $p <= .05$ (Said et al., 2014; Sommestad et al., 2015). The coefficients table provided the unstandardized regression coefficient (*B*) weights that represented the slope direction between variables (Nathans et al., 2012; Nimon & Oswald, 2013). This table also provides *t* and *p* values supplying significance values for the provided coefficients allowing interpretation for the contribution of each independent variable to the model (Mertler & Reinhart, 2017). Coefficients should be substantial and significant as determined by having values $t >= 1.96$, $p <= .05$ (Lowry & Gaskin, 2014; Said et al., 2014; Sommestad et al., 2015).

Analysis results included a description of any transformations, case discarding, and/or measurement factor removals and summarization of statistical findings. Reporting occurred in both graphics and descriptive table formats followed by scholarly discussion and interpretation of the results and their implications. The results of the data analysis and interpretation described in this section provided for the acceptance or rejection of the study hypotheses.

Study Validity

Quantitative studies of experimental or quasi-experimental design need to address external and internal threats to validity (Lancsar & Swait, 2014; Marcellesi, 2015; Tavakol & Sandars, 2014b; Yilmaz, 2013). This study was neither of these designs and as such did not need to address these topics. However, all quantitative studies need to address statistical conclusion validity (Aguinis & Edwards, 2014; Lowry & Gaskin, 2014; Venkatesh et al., 2013). Areas addressed here were those of instrument reliability, data assumptions, and sample size.

This study addressed instrument reliability through the use of instruments validated in prior research that focused on same or similar subject matter and where established alignment with the applied theory existed. Extant literature was used to provide a basis for any additions or modifications (Cook et al., 2014; Finn & Wang, 2014; Jorg Henseler et al., 2014). Statistical conclusion validity is aided by performing proper validation of instrumentation (Flores et al., 2014) and applying proper analytical techniques (Aguinis & Edwards, 2014; Hair et al., 2013; Lowry & Gaskin, 2014). Proper instrumentation also strengthens generalization of a study (Drouin & Jugdev, 2014).

Discussion of these qualities for this study exists extensively in the preceding "Instruments" and "Data Analysis" sections.

Performing screening and analysis for the data assumptions of ordinary least squares (OLS) regression techniques (M. I. Aguirre-Urreta et al., 2013; Astrachan et al., 2014; Hair et al., 2016; Ingenhoff & Buhmann, 2016; Schubring, Lorscheid, Meyer, & Ringle, 2016) in this study provided exposure of data conditions and aided in making corrective decisions as needed. Discussion of the approach for this process exists in detail in the preceding "Data Analysis" section. Establishing a requirement for a significance level of .05 for hypothesis testing (Bettany-Saltikov & Whittaker, 2014; Halfens & Meijers, 2013; Lakens, 2013) and meeting the data assumptions requirements of multiple linear regression analysis aids in avoiding Type I errors (Granato et al., 2014; Lowry & Gaskin, 2014; Mertler & Reinhart, 2017; Wiedermann & Von Eye, 2013).

Although some "rule of thumb" formulas exist for determining sample size (Mertler & Reinhart, 2017), the recommended modern approach for linear regression studies is to establish an *a priori* sample size (M. Aguirre-Urreta & Ronkko, 2015; Hair et al., 2016; Lowry & Gaskin, 2014). The preceding "Population & Sampling" section provides a detailed discussion of this topic. Proper sample sizing by applying literature-supported effect size estimations is also a defense against Type I & Type II errors (M. Aguirre-Urreta & Ronkko, 2015; Lakens, 2013; Wolf, Harrington, Clark, & Miller, 2013) and aids generalizability (Bornstein et al., 2013).

Academia well accepts quantitative studies as providing generalizable results (Bettany-Saltikov & Whittaker, 2014; Halfens & Meijers, 2013; Tavakol & Sandars, 2014a). One of the differentiating factors of this research was the study of a sample population not yet addressed in the extant literature. Statistical generalizability is when the results of a study can be generalized through inferential statistics to similar populations (Tavakol & Sandars, 2014a; Tsang, 2014). The expectation was that this study would provide statistical generalizability to the K-12 administration population.

Sample selection bias is a concern (Acharya et al., 2013) as individuals cannot be mandated to participate in a study and those motivated to participate may not fully represent the greater population (Landers & Behrend, 2015; Pearl, 2015). Addressing this bias is by studying large representative samples (Lee & Baskerville, 2003; Yilmaz, 2013). This study occurred in an environment where a larger than normal population existed and the extension of the population included the largest number of qualified participants through the inclusion of associate and assistant K-12 leadership. However, a larger population when gathered under convenience sampling, as in this study, may not support generalizability (Aguinis & Edwards, 2014; Landers & Behrend, 2015). Researchers offset this argument by performing research in natural settings (Aguinis & Edwards, 2014) as in this study. Still results may not be generalizable beyond the sample (Acharya et al., 2013).

In this research, I applied measures established in the extant literature. Establishing analytical generalizability (Lee & Baskerville, 2003; Sandelowski, 2014; Tsang, 2014) occurs if the study results provide confirmation that the measured factors are applicable descriptors for the independent constructs of TPB by supporting the concept that these same factors are valid when TPB is applied to study other populations.

Researchers could establish transferability (Venkatesh et al., 2013; Yilmaz, 2013) to the larger computer end user population through the review and analysis of multiple studies of similar design, theory, and topic as research shows motivational factors for information security compliance would vary across populations. This is in line with the theoretical assumptions made by Ajzen (2002) regarding TPB. Additional detailed discussion of generalization exists in the preceding “Limitations” and “Population and Sampling” sections.

Transition and Summary

Section 2 of this proposal provided detail regarding the study project. To summarize, the role and relationship of the researcher and participants was organizationally in-house but objective and arms-length. Participant selection occurred through substantive convenience sampling. Proper study oversight, participant recruiting, and data handling addressed ethical concerns.

Discussion of the research method and design in this section provided details for the quantitative correlational approach with support and justification from extant literature. Section 2 also provided information and validation for the measurement instrumentation as well as details and defense of the data collection and analysis processes for this study. The provided information supports the goal of providing valid and reliable statistical study results.

The following section provides the findings of this study and relates those findings in terms of professional IT practice and social change. Discussion includes recommendations for action based on the study findings as well as pathways for future research. The section and paper concludes with reflections on the study project including closing perspectives on the study overall.

Section 3: Application to Professional Practice and Implications for Change

This section presents details of findings and discussion for this study based on quantitative analysis of the collected study data. Organization of this section is as follows. First, I provide an overview of the study recapping the purpose of the study and present a high-level overview of the study findings. Next is a detailed presentation of the quantitative data analysis and results. Subsequent sections present discussion on the application of the findings to professional practice, implications for social change, recommendations for action, and recommendations for further study. The final sections contain a reflection on the study along with summary conclusions.

Overview of Study

The purpose of this quantitative correlational study was to examine how attitude toward the behavior, subjective norm, and perceived behavioral control affect the intention of computer end users in a K-12 environment to follow information security policy to provide IT security program managers sufficient knowledge to develop effective security controls in the form of SETA to protect against human behavior risks. The quantitative method is appropriate when the desire is to measure to what level particular independent variables influence a dependent variable (Turner et al., 2013) which was the intent of this study. TPB (Ajzen, 1985) served as the theoretical basis for the study.

A population of 699 K-12 school administrators in Bigg County Public Schools were invited to participate in an anonymous Web-based survey regarding factors shown in the study literature review to represent the variables of TPB in order to answer the RQ:

To what extent does attitude toward the behavior, subjective norm, and perceived behavioral control affect the intention of computer end users in a K-12 environment in the Bigg County Public School System located in Northeast Georgia to follow information security policy? An *a priori* analysis for sample size was performed using G*Power (Faul et al., 2009). The result was a required sample size of 41 to achieve a power of .80 and 62 to achieve a power of .95 (see Figure 2). Study participants submitted 165 individual surveys. Data screening resulted in 163 valid surveys for a 23.3% response rate.

The general IT problem addressed by this study was that some IT security program managers lack knowledge of what motivational factors affect intention to follow information security policy in order to develop a SETA program to mitigate human behavior risks. Multiple linear regression and logistic regression analysis of the study model and data resulted in the rejection of the study's null hypothesis. The statistics indicated that the independent variables of TPB do affect the information security intentions of computer end users in a K-12 environment with subjective norm being the single significant predictor. Results of the study did not find attitude and perceived behavioral control to be significant. Findings suggest that IT security program managers working in the K-12 environment should consider these motivational factors when developing improved SETA programs for their organization.

Presentation of the Findings

Attitude (ATT), subjective norm (SN), and perceived behavioral control (PBC) represent the three independent variables of TPB that affect the dependent variable of intention (represented as IB for intended behavior in the study findings). I used multiple linear regression as the analytical method for the study data. Multiple linear regression is a multivariate regression process intended to analyze multiple predictors in order to account for the variance of a response variable (Y. Chen et al., 2014; Granato et al., 2014; Jung & Kim, 2014; Mertler & Reinhart, 2017). This description matched the theoretical model and intention of this study.

A population of 699 K-12 administrators received study participation invitations via email. The same population received a participation reminder email after one week. Collection of study data occurred over a period of two weeks. Study participants submitted 165 individual survey responses. Entering of coded values for study measures based on Table 2 occurred in the web survey export tool making the exported data ready for analysis in SPSS without any further processing.

Data Screening

Data screening provides for accurate statistical analysis and drawing valid conclusions (Mertler & Reinhart, 2017; Rutkowski & Zhou, 2015; Williams et al., 2013). Data screening involves verifying the accuracy of data collected, addressing missing data, checking for outliers, and validating that data assumptions are met (Casson & Farmer, 2014; Flores & Ekstedt, 2016; Lowry & Gaskin, 2014). This description reflects the process followed for this study and the following contains details of each step taken in the data screening process.

Study participants answered qualification questions regarding their job role, age, and use of a computer for work. Frequency tables identified cases to remove based on invalid responses to qualification questions. Two participants responded “No” in regards to being in the required job role for the study (see Table 3). I deleted these cases. No disqualification of cases occurred based on responses to age or usage of a computer at work questions (see Tables 4 & 5). This left 163 cases for analysis.

Table 3

Job Role

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Yes	163	98.8	98.8	98.8
	No	2	1.2	1.2	100.0
	Total	165	100.0	100.0	

Table 4

Age Qualification

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Yes	165	100.0	100.0	100.0

Table 5

Computer Use Qualification

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Yes	165	100.0	100.0	100.0

Throughout this paper, the use of acronyms provides abbreviated references for the quantitative measures used in this study. Table 2 provides the introduction of the acronyms used. Table 6 provides a recap of these acronyms for reference.

Table 6

Acronyms for Quantitative Measures

	Quantitative Measure Referenced
PVUL	Perceived vulnerability
PSEV	Perceived severity
REW	Reward
NB1	Normative behavior, question 1
NB2	Normative behavior, question 2
NB3	Normative behavior, question 3
LOC	Locus of control
SE	Self-efficacy
IB1	Intended behavior, question 1
IB2	Intended behavior, question 2
IB3	Intended behavior, question 3

A count of missing responses for the quantitative measure questions for each case revealed no case was missing more than 1 of 27 responses, thus discarding did not occur for any cases based on stated criteria in Section 2 of missing 50% or more responses. A review of frequency tables to identify the number of missing values per quantitative measure showed no measure was missing over 15% of response data (highest count was 5 missing for PSEV = 2.9%; see Table 7); thus, no discarding occurred for any quantitative measures.

Table 7

Response Counts

		PVUL	PSEV	REW	NB1	NB2	NB3	LOC	SE	IB1	IB2	IB3
N	Valid	160	158	159	162	162	163	162	162	163	160	163
	Missing	3	5	4	1	1	0	1	1	0	3	0

Note. Quantitative measure questions NAR1-NAR16 were not optional in the survey and thus had no missing values.

Participants answered questions regarding their knowledge of existing organizational information security policies at work. Of the 163 cases analyzed, 162 respondents stated their organization did have such policies. Only one respondent stated that they did not know if their organization had information security policies (see Table 8). No discarding of cases occurred based on these responses.

Table 8

Organizational Information Security Policies Exist

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Yes	162	99.4	99.4	99.4
	I don't know	1	.6	.6	100.0
	Total	163	100.0	100.0	

Response Demographics

Survey participants answered questions regarding their age, gender, and the number of years they had been with their employer. One respondent did not reveal their age, and two did not reveal their gender. Tables 9-11 provide frequency and percentage values for these questions.

Table 9

Age Range

		Frequency	Percent	Valid percent	Cumulative percent
Valid	25 to 34 years	6	3.7	3.7	3.7
	35 to 44 years	71	43.6	43.8	47.5
	45 to 54 years	64	39.3	39.5	87.0
	55 years or older	21	12.9	13.0	100.0
	Total	162	99.4	100.0	
Missing	System	1	.6		
Total		163	100.0		

Table 10

Gender

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Male	50	30.7	31.1	31.1
	Female	111	68.1	68.9	100.0
	Total	161	98.8	100.0	
Missing	System	2	1.2		
Total		163	100.0		

Table 11

Years with Employer

		Frequency	Percent	Valid percent	Cumulative percent
Valid	Less than 1 year	2	1.2	1.2	1.2
	Between 1 and 5 years	13	8.0	8.0	9.2
	Between 6 and 10 years	16	9.8	9.8	19.0
	Between 11 and 15 years	45	27.6	27.6	46.6
	More than 15 years	87	53.4	53.4	100.0
	Total	163	100.0	100.0	

Factor Calculation and Descriptive Statistics

Replacement occurred for missing values of quantitative measures with the mean for that measure. Summing of these measures provided the value for the independent and dependent variables as follows:

ATT = (NAR = (N1-N16 Summed)) + PVUL + PSEV + REW

SN = NB1 + NB2 + NB3

PBC = LOC + SE

IB = IB1 + IB2 + IB3

Tables 12-15 provide summary descriptive statistics for each of the mean-imputed quantitative measures as well as the summed value for the related variable.

Table 12

Descriptive Statistics for Attitude

		NAR	PVUL	PSEV	REW	ATT
N	Valid	163	163	163	163	163
	Missing	0	0	0	0	0
Mean		11.9693	2.225	3.076	4.654	21.9244
Median		12.0000	2.000	3.000	5.000	22.0000
Std. deviation		2.55174	1.0940	1.2300	.8748	3.48359
Skewness		-.498	.569	-.067	-2.780	-.370
Std. error of skewness		.190	.190	.190	.190	.190
Kurtosis		-.214	-.645	-.964	7.310	-.170
Std. error of kurtosis		.378	.378	.378	.378	.378
Minimum		5.00	1.0	1.0	1.0	12.00
Maximum		16.00	5.0	5.0	5.0	29.00

Table 13

Descriptive Statistics for Subjective Norm

		NB1	NB2	NB3	SN
N	Valid	163	163	163	163
	Missing	0	0	0	0
Mean		4.580	4.735	4.902	14.2167
Median		5.000	5.000	5.000	15.0000
Std. deviation		.6259	.5643	.4039	1.31756
Skewness		-1.379	-2.257	-4.748	-2.573
Std. error of skewness		.190	.190	.190	.190
Kurtosis		1.496	4.998	24.573	9.734
Std. error of kurtosis		.378	.378	.378	.378
Minimum		2.0	2.0	2.0	6.00
Maximum		5.0	5.0	5.0	15.00

Table 14

Descriptive Statistics for Perceived Behavioral Control

		LOC	SE	PBC
N	Valid	163	163	163
	Missing	0	0	0
Mean		3.136	4.247	7.3827
Median		3.000	4.000	7.0000
Std. deviation		.8643	.9497	1.40867
Skewness		.080	-1.566	-.698
Std. error of skewness		.190	.190	.190
Kurtosis		1.743	2.439	1.503
Std. error of kurtosis		.378	.378	.378
Minimum		1.0	1.0	2.00
Maximum		5.0	5.0	10.00

Table 15

Descriptive Statistics for Intended Behavior

		IB1	IB2	IB3	IB
N	Valid	163	163	163	163
	Missing	0	0	0	0
Mean		4.963	4.938	4.951	14.8516
Std. error of mean		.0259	.0257	.0243	.07240
Median		5.000	5.000	5.000	15.0000
Std. deviation		.3313	.3275	.3104	.92437
Skewness		-8.943	-6.530	-7.457	-8.149
Std. error of skewness		.190	.190	.190	.190
Kurtosis		78.950	48.406	60.967	70.366
Std. error of kurtosis		.378	.378	.378	.378
Minimum		2.0	2.0	2.0	6.00
Maximum		5.0	5.0	5.0	15.00

Data Assumptions

Meeting the assumptions of normality, linearity, homoscedasticity, and multicollinearity is a requirement when performing multiple linear regression (Casson & Farmer, 2014). Preliminary assessments determined if variables met these assumptions prior to analysis. A scatterplot provided for initial review of linearity, multivariate normality, and homoscedasticity (see Figure 4). Data are expected to present in an elliptical shape (Mertler & Reinhart, 2017) and bivariate plots between the independent and dependent variables should be of similar width throughout with bulging in the middle (Mertler & Reinhart, 2017). The study data overall did not present in the manner described. The scatterplot shows the majority of data clustered and skewed in a single direction demonstrating a lack of normality. The bivariate plots between the independent and dependent variables present in a clustered line as opposed to an elliptical shape demonstrating a lack of linearity. Further analysis of the data condition occurs in the following sections.

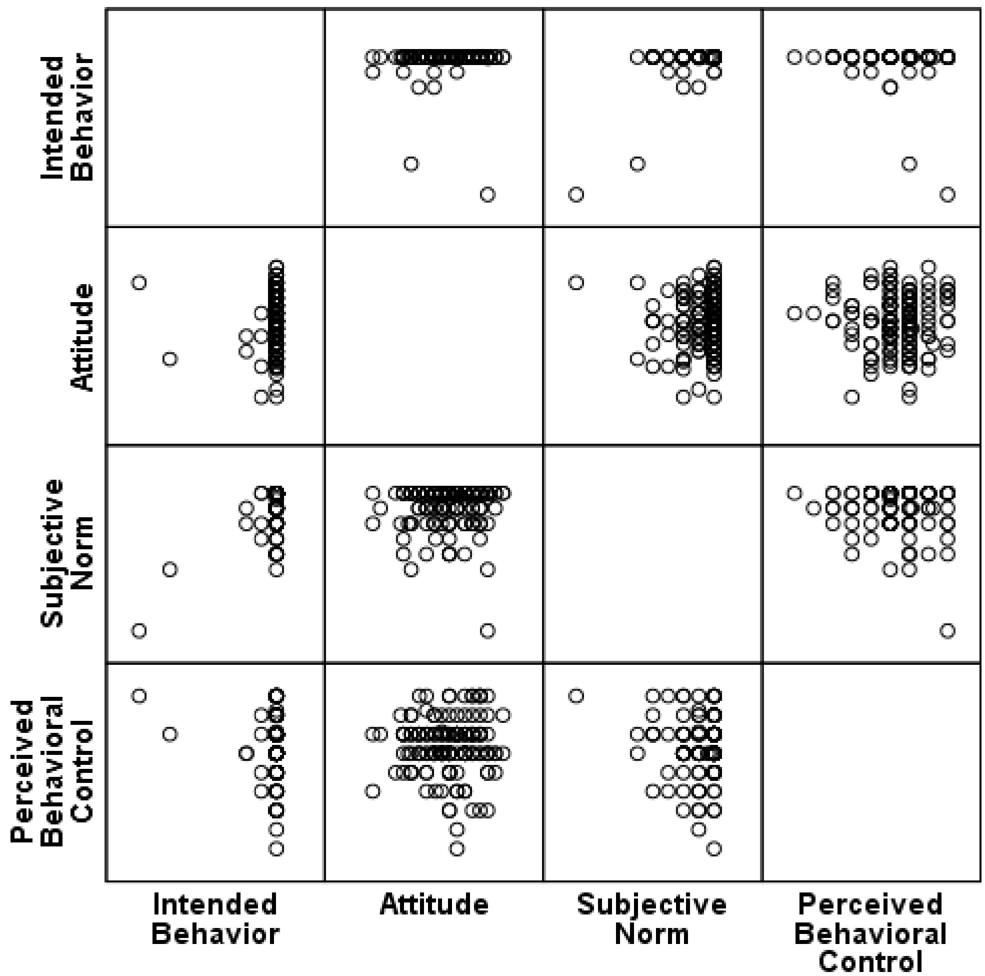

Figure 4. Scatterplot representing the relationship between study variables.

Normality. Further analysis assessed the normality of each study variable. This assessment was through the execution of Kolmogorov-Smirnov (K-S) tests and a review of skewness and kurtosis values, histograms, and normal Q-Q plots. The following sections provide discussion regarding the normality condition for each variable.

Attitude. The K-S test results for the ATT variable (Table 16) show a strong significance level ($p < .05$) and skewness and kurtosis values of -.370/-.170 (Table 12) are significantly different than 0. Both of these findings indicate a nonnormal distribution. The accompanying histogram (Figure 5) and normal Q-Q plot (Figure 6) reflect this finding. A box plot shows that the ATT variable (Figure 7) had some univariate outliers. However, it was determined removal would not occur for any cases due to these outliers providing the primary variability for some of the constructs in the study model.

Table 16

Tests of Normality for ATT

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
ATT	.091	163	.002	.979	163	.014

a. Lilliefors significance correction

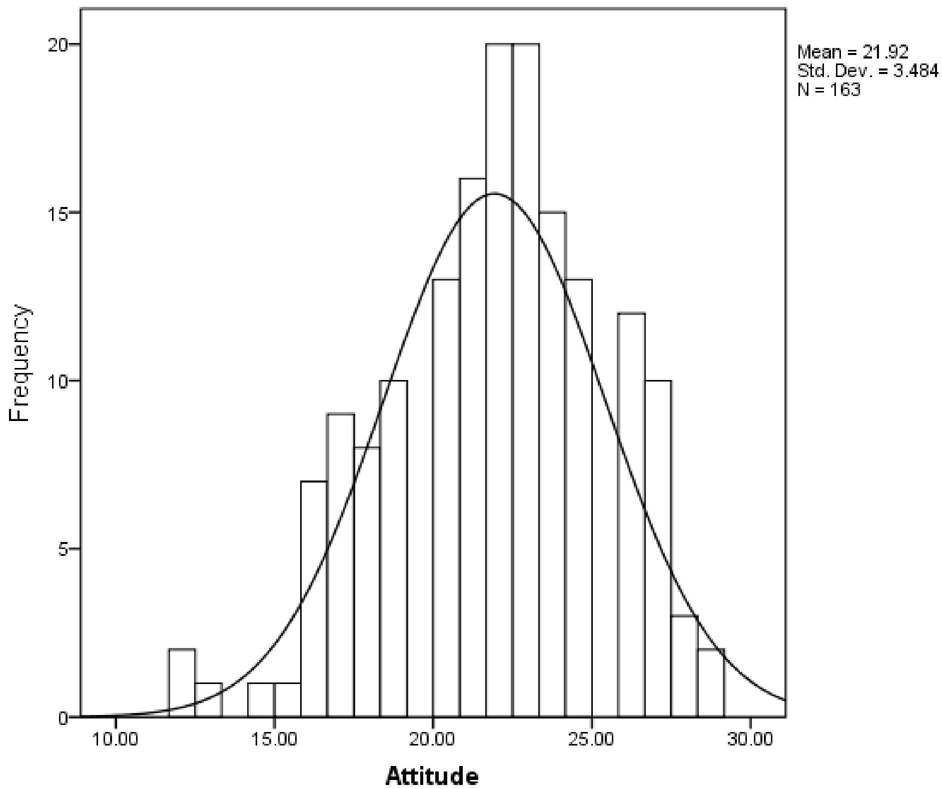

Figure 5. Histogram for ATT variable.

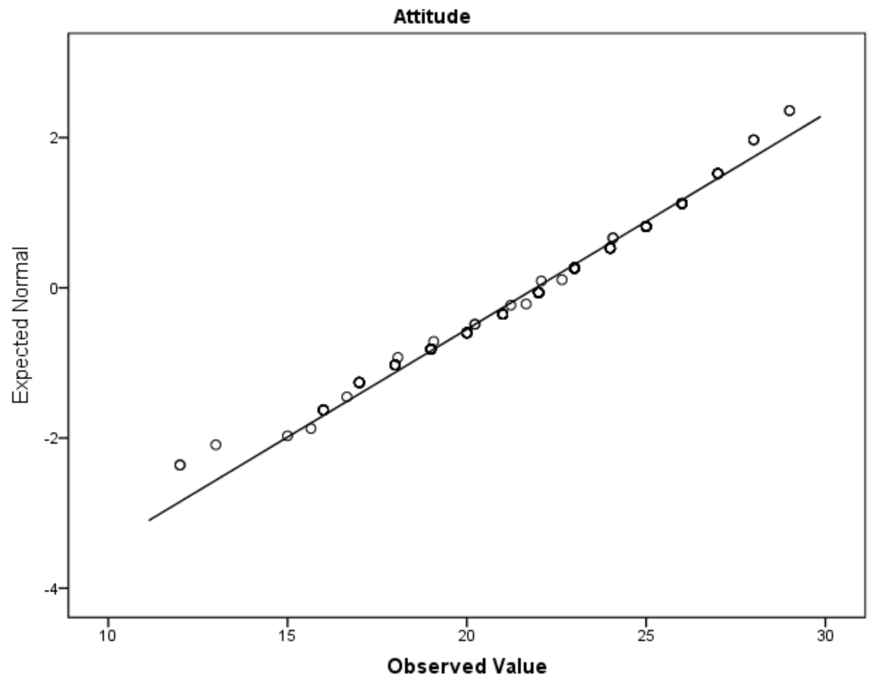

Figure 6. Normal Q-Q plot for ATT variable.

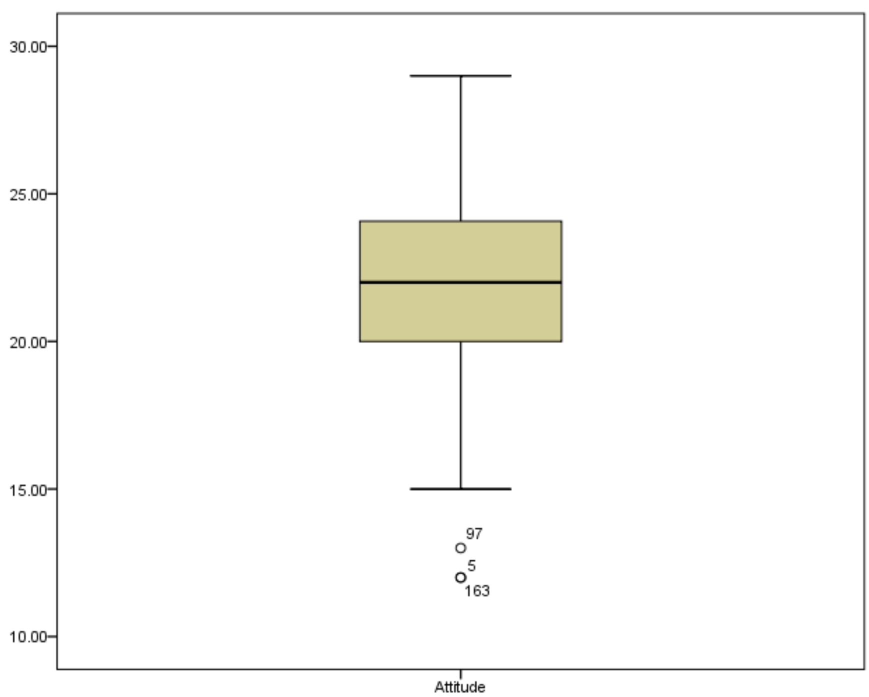

Figure 7. Box plot for ATT variable.

Subjective norm. The K-S test results for the SN variable (Table 17) show a very strong significance level ($p < .001$) and skewness and kurtosis values of -2.573/9.734 (Table 13) are significantly different than 0. Both of these findings indicate a nonnormal distribution. The accompanying histogram (Figure 8) and normal Q-Q plot (Figure 9) reflect this finding. A box plot shows that for the SN variable (Figure 10) several univariate outliers exist. However, it was determined removal would not occur for any cases due to these outliers providing the primary variability for some of the constructs in the study model.

Table 17

Tests of Normality for SN

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
SN	.331	163	.000	.645	163	.000

a. Lilliefors significance correction

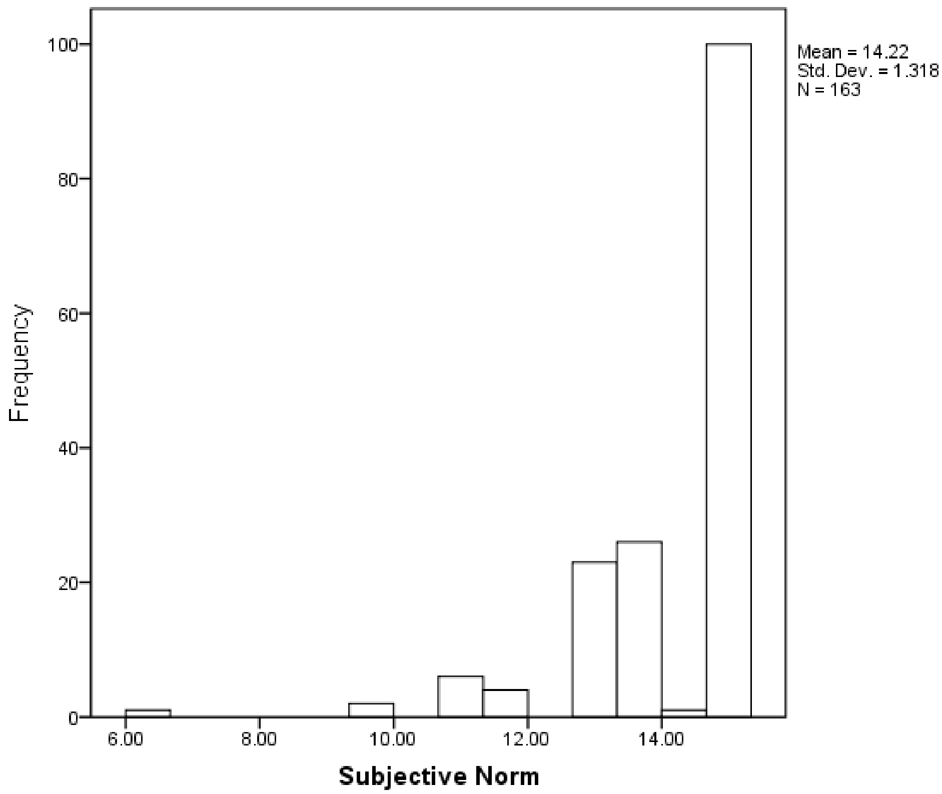

Figure 8. Histogram for SN variable.

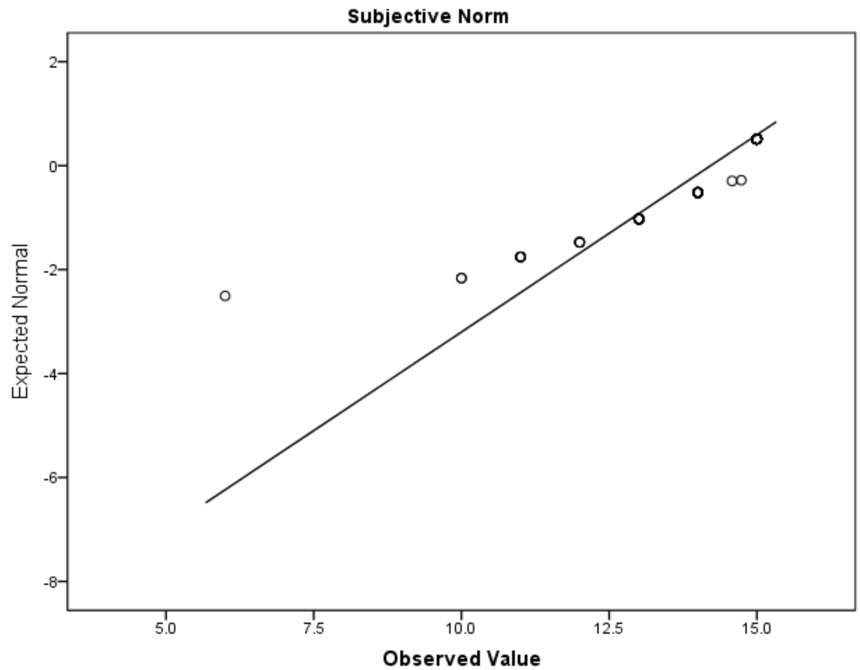

Figure 9. Normal Q-Q plot for SN variable.

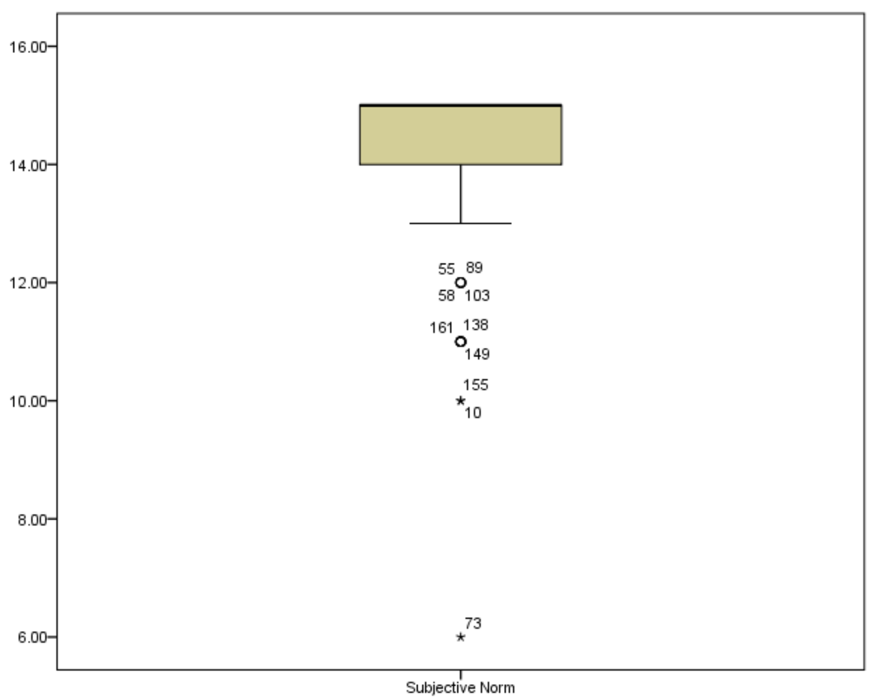

Figure 10. Box plot for SN variable.

Perceived behavioral control. The K-S test results for the PBC variable (Table 18) show a very strong significance level ($p < .001$) and skewness and kurtosis values of -.698/1.503 (Table 14) are significantly different than 0. Both of these findings indicate a nonnormal distribution. The accompanying histogram (Figure 11) and normal Q-Q plot (Figure 12) reflect this finding. A box plot shows that for the PBC variable (Figure 13) many univariate outliers exist. However, it was determined removal would not occur for any cases due to these outliers providing the primary variability for some of the constructs in the study model.

Table 18

Tests of Normality for PBC

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
PBC	.209	163	.000	.913	163	.000

a. Lilliefors significance correction

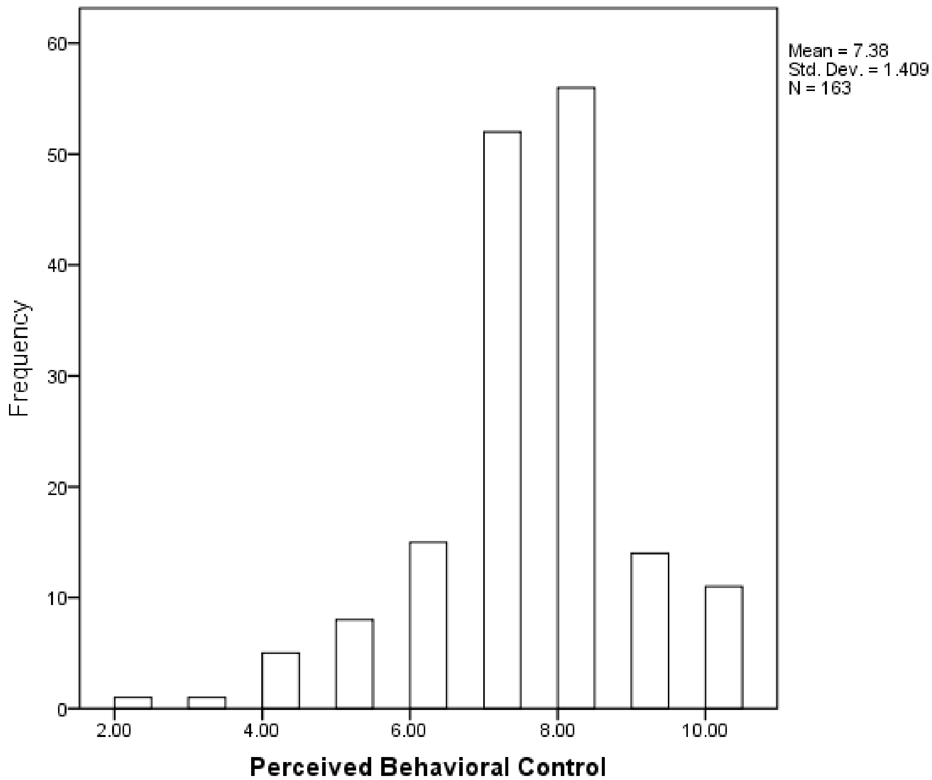

Figure 11. Histogram for PBC variable.

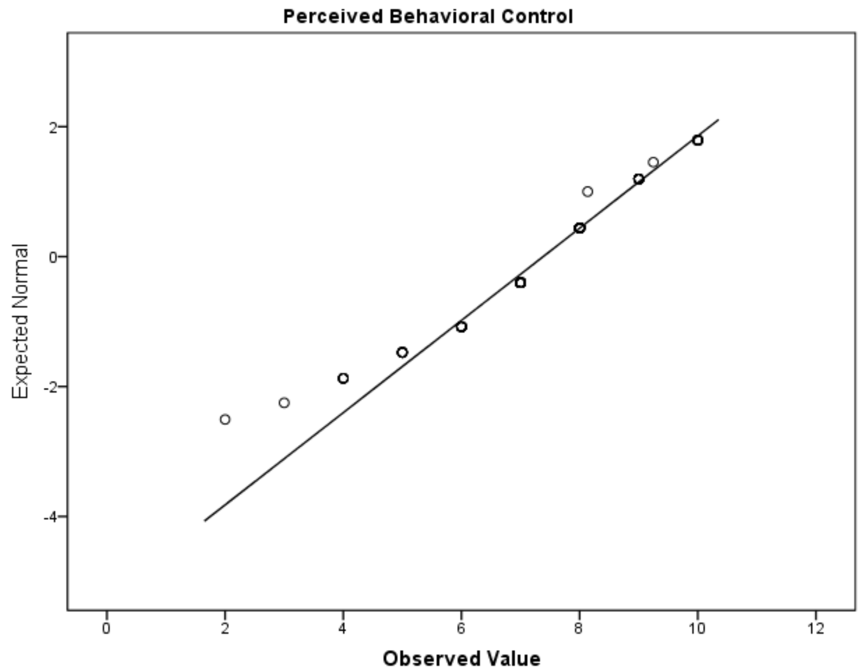

Figure 12. Normal Q-Q plot for PBC variable.

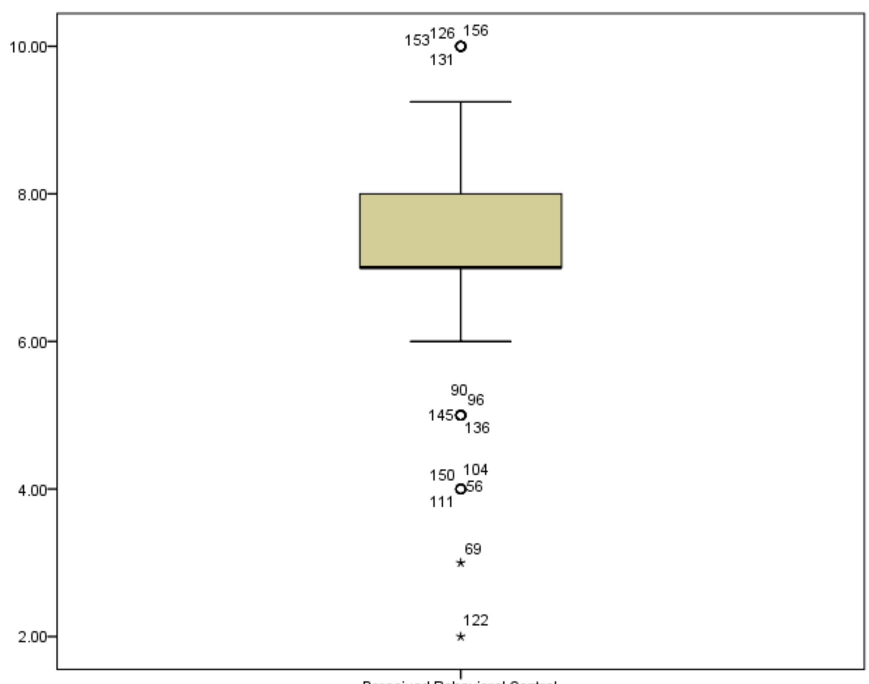

Figure 13. Box plot for PBC variable.

Intended behavior. The K-S test results for the IB variable (Table 19) show a very strong significance level ($p < .001$) and skewness and kurtosis values of -8.149/70.366 (Table 15) are significantly different than 0. Both of these findings indicate a nonnormal distribution. The accompanying histogram (Figure 14) and normal Q-Q plot (Figure 15) reflect this finding. A box plot shows that for the IB variable (Figure 16) several univariate outliers exist. However, it was determined removal would not occur for any cases due to these outliers providing the primary variability for some of the constructs in the study model.

Table 19

Tests of Normality for IB

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
IB	.496	163	.000	.151	163	.000

a. Lilliefors significance correction

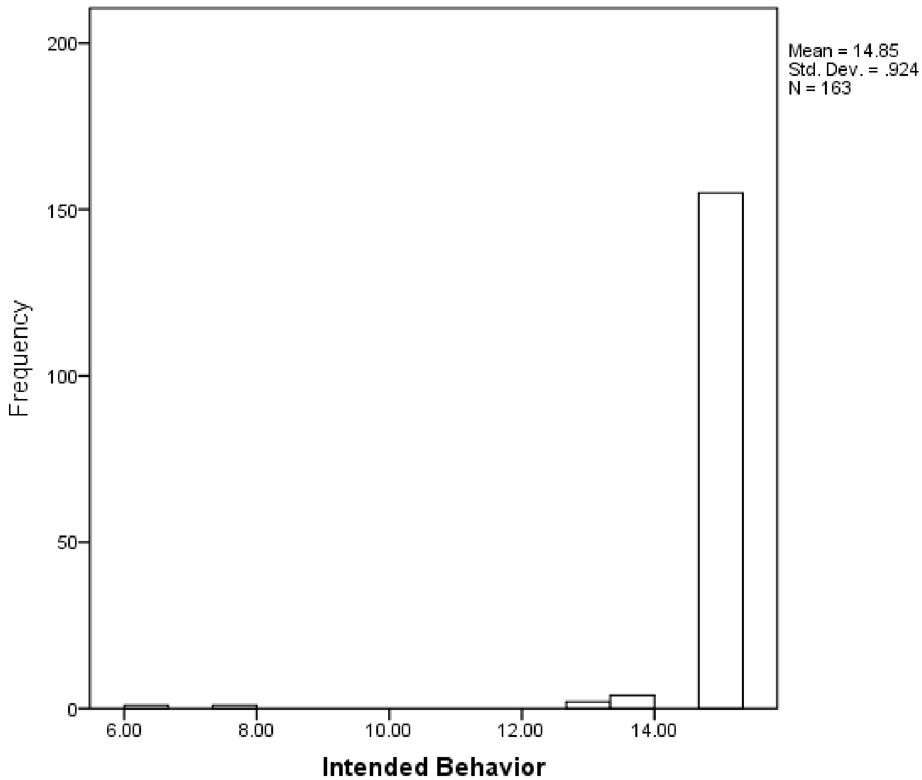

Figure 14. Histogram for IB variable.

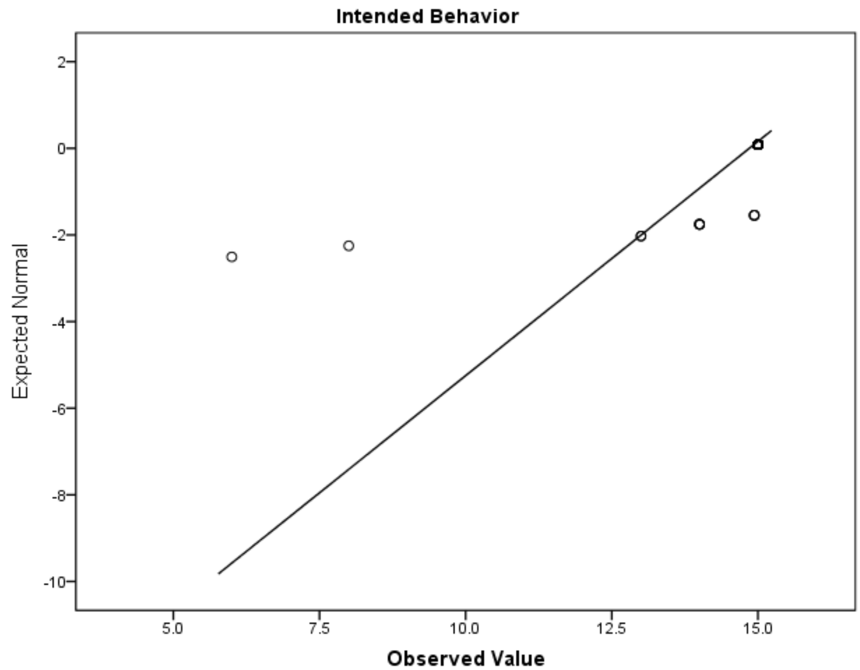

Figure 15. Normal Q-Q plot for IB variable.

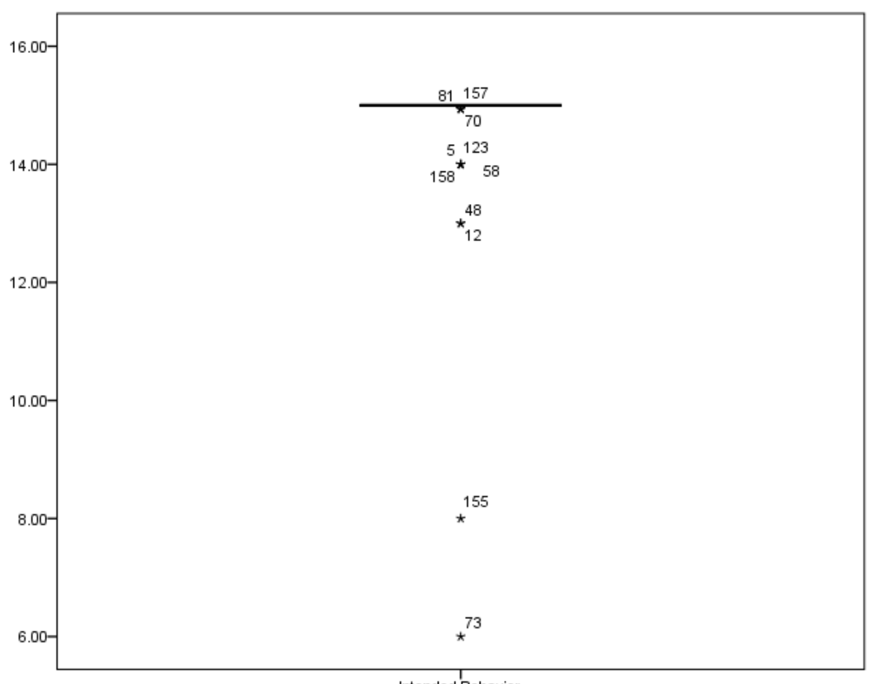

Figure 16. Box plot for IB variable.

Homoscedasticity. Bivariate scatterplots between independent and dependent variables should be of similar width throughout with bulging in the middle to demonstrate homoscedasticity (Mertler & Reinhart, 2017). Review of the scatterplot (Figure 4) did not show the study data in this condition. Levene's test is another analysis for homoscedasticity. Although intended for analysis of grouped data, application occurred as an additional check. Results should not be significant at $p < .05$. The mixed results presented in Table 20 made determining homoscedasticity difficult. This is largely due to the violations of normality cited in the previous section. A further check for homoscedasticity of residuals occurred after initial multiple linear regression analysis and discussion for that test exists in a following section.

Table 20

Test of Homogeneity of Variance

		Levene statistic	df1	df2	Sig.
IB	Based on mean	5.089	5	148	.000
	Based on median	1.192	5	148	.316
	Based on median and with adjusted df	1.192	5	30.034	.337
	Based on trimmed mean	2.777	5	148	.020

Linearity and multicollinearity. Determination of linearity beyond an initial review of scatterplots is through analysis of residuals. An initial multiple linear regression analysis must occur to generate residual data. Determining multicollinearity also occurs during the multiple linear regression analysis process. Further discussion of both of these assumptions occurs in the following multiple linear regression data analysis section.

Summary. All variables in the study data violate the normality data assumption. This is most evident with the IB variable. Out of the 163 respondents to the study survey, all but eight participants provided the same response. Three more respondents skipped one of the IB related questions; resulting in their IB score containing mean values that provided only minor variation of their IB score (see Table 21). My belief is that the survey responses for IB are valid and not socially desirable responses due to the anonymity provided through the Web-based survey. The IB measures question intent to follow information security policies. It is possible to assume that most people do intend to follow policies. However, the data condition of the dependent variable results in many of the issues seen in assumption testing.

Table 21

Frequency Table for Intended Behavior

		Frequency	Percent	Valid percent	Cumulative percent
Valid	6.00	1	.6	.6	.6
	8.00	1	.6	.6	1.2
	13.00	2	1.2	1.2	2.5
	14.00	4	2.5	2.5	4.9
	14.94	3	1.8	1.8	6.7
	15.00	152	93.3	93.3	100.0
	Total	163	100.0	100.0	

Multiple Linear Regression Data Analysis

As stated in previous sections, an initial multiple linear regression analysis was required to generate residuals for linearity analysis as well as perform other tests for data assumptions such as multicollinearity. I performed the first multiple linear regression analysis with the data "as is" with no transformations or corrective actions in order to complete these tests and gain preliminary insight into the data. This section provides analysis and discussion of the initial multiple linear regression results.

Multiple linear regression was performed using the enter method to determine how much the independent variables of TPB (Attitude [ATT]; Subjective Norm [SN]; Perceived Behavioral Control [PBC]) predict the intended information security behavior [IB] of the study population. Data screening led to the elimination of two cases due to study qualification responses. Regression results indicate that the study model significantly predicts intended behavior (R^2 = .308, R^2_{adj} = .294, F (3, 159) = 23.537, p < .001). This model accounted for 30.8% of variance in intended behavior. These results are sufficient to reject the null hypothesis. Tables 22 and 23 provide analysis statistics.

Table 22

Model Summary[b]

Model	R	R square	Adjusted R square	Std. error of the estimate
1	.555[a]	.308	.294	.77644

a. Predictors: (Constant), Subjective norm, Attitude, Perceived behavioral control
b. Dependent variable: Intended behavior

Table 23

ANOVA[a]

Model		Sum of squares	df	Mean square	F	Sig.
1	Regression	42.568	3	14.189	23.537	.000[b]
	Residual	95.854	159	.603		
	Total	138.423	162			

a. Dependent variable: Intended behavior
b. Predictors: (Constant), Subjective norm, Attitude, Perceived behavioral control

The coefficients (Table 24) shows that IB increased by an average of 0.007 points for each one point increase in ATT, IB increased by an average of 0.380 points for each one point increase in SN, and IB decreased by an average of 0.054 points for each one point increase in PBC across the population. The only variable significant in the model at the $p < .05$ level was SN ($t(159) = 8.192$, $p < .001$). ATT and PBC did not show to be statistically significant. The betas confirm this for each variable as well. The collinearity statistics provided in this same table show the tolerance and variance inflation factor (VIF) for each variable to be in the acceptable range of tolerance above 0.1 and VIF less than 10 demonstrating a lack of multicollinearity.

Table 24

Coefficients[a]

		Unstandardized coefficients		Standardized coefficients	t	Sig.	Collinearity statistics	
Model		B	Std. error	Beta			Tolerance	VIF
1	(Constant)	9.695	.839		11.550	.000		
	Perceived Behavioral control	-.054	.043	-.082	-1.239	.217	.995	1.005
	Attitude	.007	.018	.025	.385	.701	.999	1.001
	Subjective norm	.380	.046	.542	8.192	.000	.995	1.005

a. Dependent variable: Intended behavior

Analysis of residuals. Analyzing residuals is the preferred approach for identifying outliers and assessing normality and linearity when using multiple linear regression (Mertler & Reinhart, 2017). Mahalanobis distance calculation provides chi-square values for identification of possible outliers (Mertler & Reinhart, 2017). I calculated Mahalanobis distance for the residuals using the critical value of 18.467 (at $p <$

.001) with *df* = 4 (number of variables in the model). Case #73 identified as a multivariate outlier (see Table 25). Again, it was determined removal would not occur for any outlier cases at this time due to these outliers providing the primary variability for some of the constructs in the study model. Reconsideration of this point could occur should a corrected model show greater normality.

Table 25

Mahalanobis Distance - Extreme Values

			Case number	Value
MAH_2	Highest	1	73	43.27951
		2	122	14.85641
		3	10	12.78775
		4	155	12.16354
		5	5	11.77792
	Lowest	1	57	.14444
		2	118	.17347
		3	22	.17347
		4	116	.21044
		5	127	.30173

The K-S test results for normality of the residuals (Table 26) show a strong significance level ($p < .001$) and skewness and kurtosis values of -4.088/29.415 (Table 27) are significantly different than 0. Both of these findings indicate a nonnormal distribution. The accompanying histogram (Figure 17) and normal Q-Q plot (Figure 18) reflect this finding.

Table 26

Tests of Normality for Unstandardized Residuals

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Unstandardized residual	.293	163	.000	.588	163	.000

a. Lilliefors significance correction

Table 27

Descriptives for Unstandardized Residuals

			Statistic	Std. error
Unstandardized residual	Mean		.0000000	.06024962
	95% Confidence interval for mean	Lower bound		-.1189759
		Upper bound	.1189759	
	5% Trimmed mean		.0385441	
	Median		-.1032637	
	Variance		.592	
	Std. deviation		.76921567	
	Minimum		-5.62074	
	Maximum		1.69687	
	Range		7.31761	
	Interquartile range		.40724	
	Skewness		-4.088	.190
	Kurtosis		29.415	.378

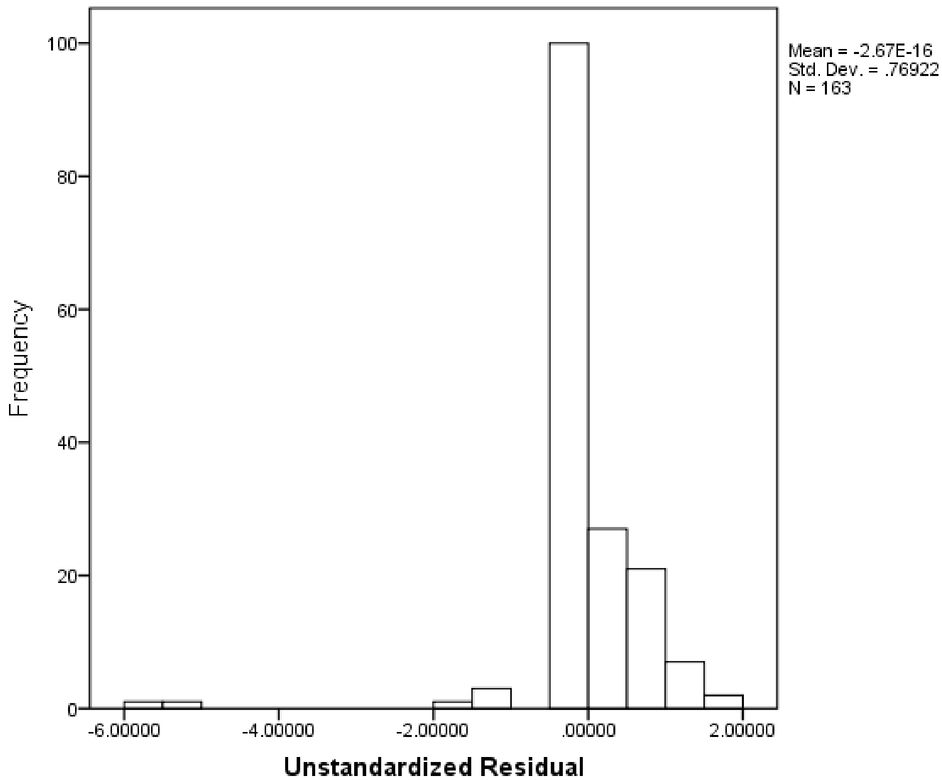

Figure 17. Histogram for unstandardized residuals.

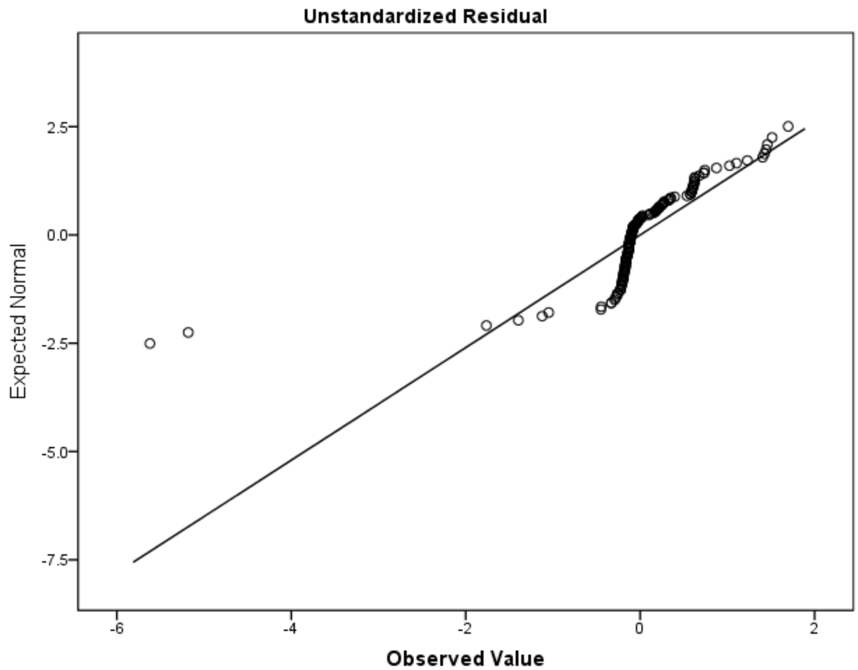

Figure 18. Normal Q-Q plot for unstandardized residuals.

A residual plot provides data to assess linearity. Figure 19 shows a hard diagonal line of values in the upper right corner of the plot. This is opposed to the centered and rectangular clustering that would demonstrate linearity. The primary cause of this result is the issue of many observations having the same value for the dependent variable (IB) as noted earlier.

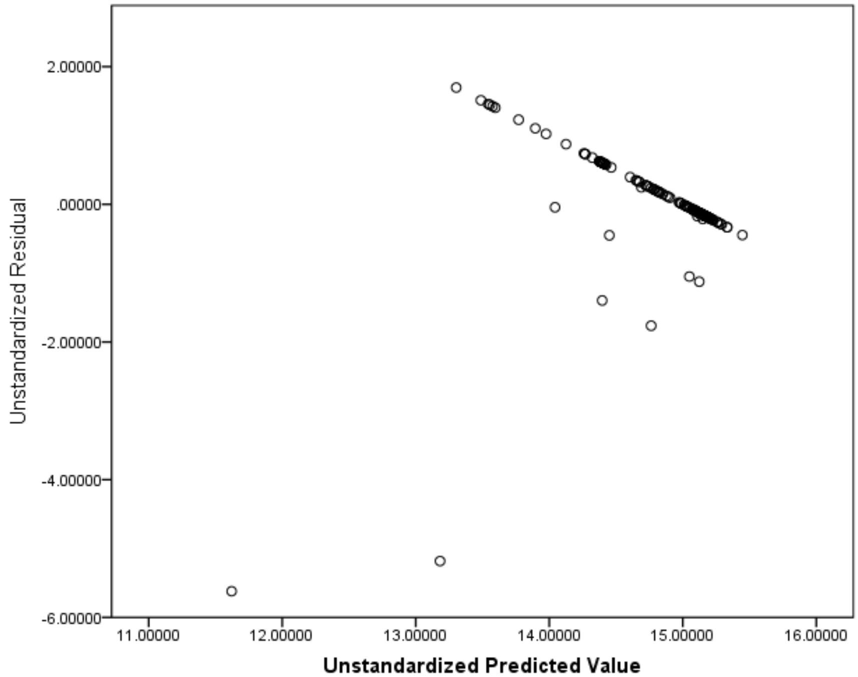

Figure 19. Residual plot for unstandardized residuals.

Summary of initial assessment. The initial multiple linear regression analysis showed that many data assumption violations existed in the data set. Residuals did show normal data distribution and evaluation of linearity and homoscedasticity was not easily possible due to these distribution issues. Although the analysis presented some interesting and significant results, the assumption violations prevented accurate analysis and substantiation of the findings. In an attempt to normalize the study data, the application of several corrective measures occurred and the following sections present the results.

Application of corrective measures. Corrective measures exist that when applied can address data condition issues in a data set. Potential corrective actions listed in Section 2 included applying mathematical corrections in the form of square root, logarithm, and z-score transformations as well as bootstrapping. Application of these corrective measures occurred in order to address the issues of nonnormality of the residuals in the data set. The primary focus in the mathematical transformations is on the dependent variable of the model as it exhibits the greater issues. The following sections present the results of each attempted corrective action.

Square root transformation. Square root transformation takes the value of a variable, calculates the square root of that value, and saves that value as a new variable (Mertler & Reinhart, 2017). Application of this transformation occurred for the dependent variable IB. Figures 20 & 21 show that the residuals were not normalized. Presentation of multiple linear regression data analysis results does not occur here, as correction of the data issue did not materialize.

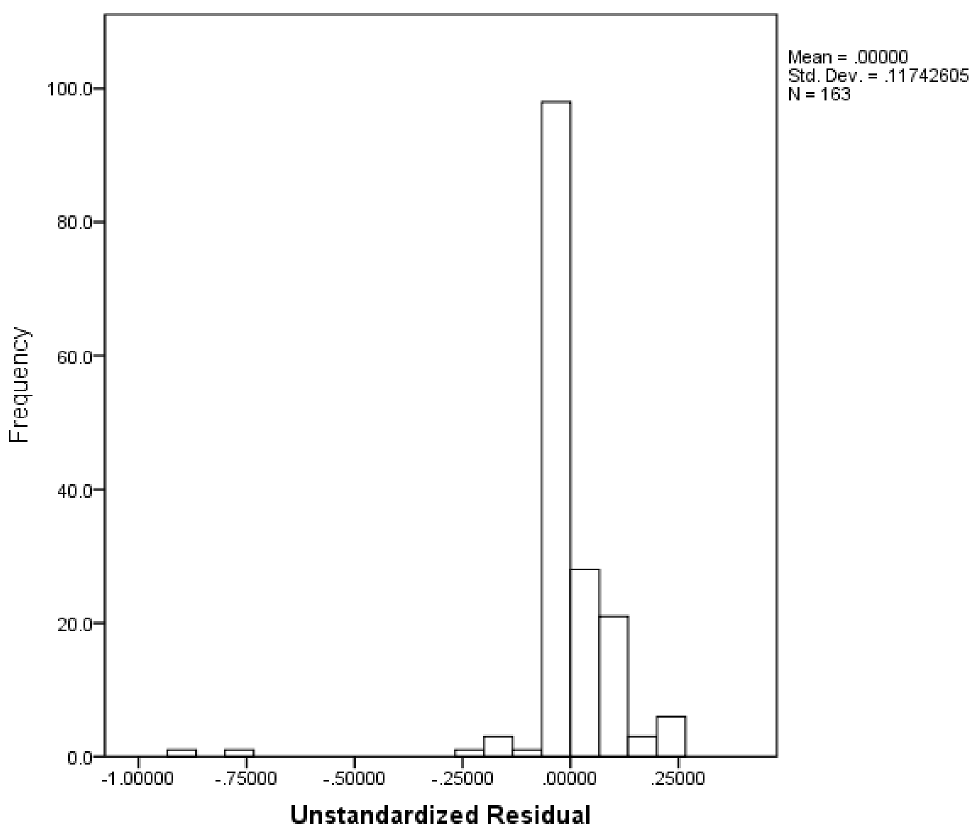

Figure 20. Histogram for unstandardized residuals after square root transformation.

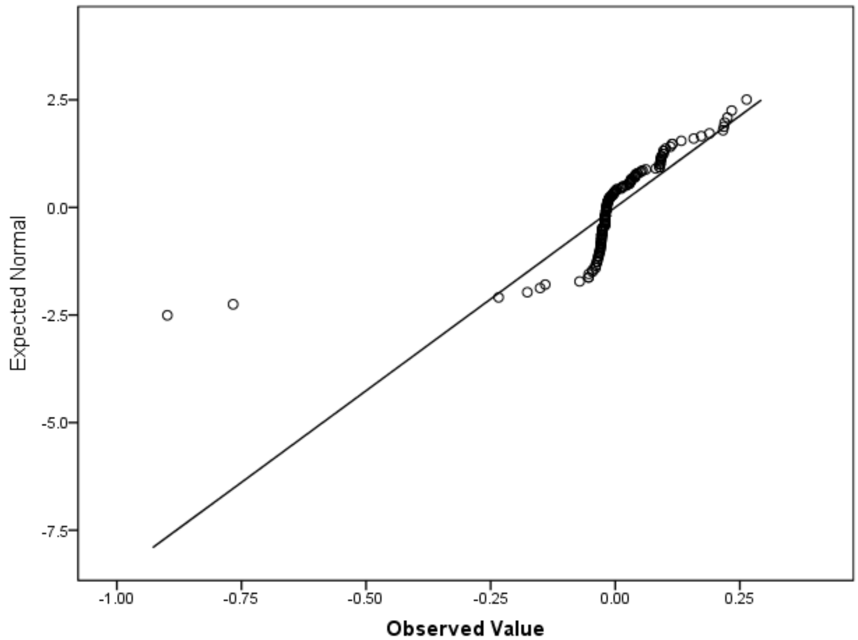

Figure 21. Normal Q-Q plot for unstandardized residuals after square root transformation.

Logarithm transformation. Logarithm transformation takes the value of a variable and calculates the log of that value and saves it as a new variable (Mertler & Reinhart, 2017). Application of the natural log transformation occurred for the dependent variable IB. Figures 22 & 23 show that the residuals were not normalized. Again, presentation of multiple linear regression data analysis results does not occur here, as correction of the data issue did not transpire.

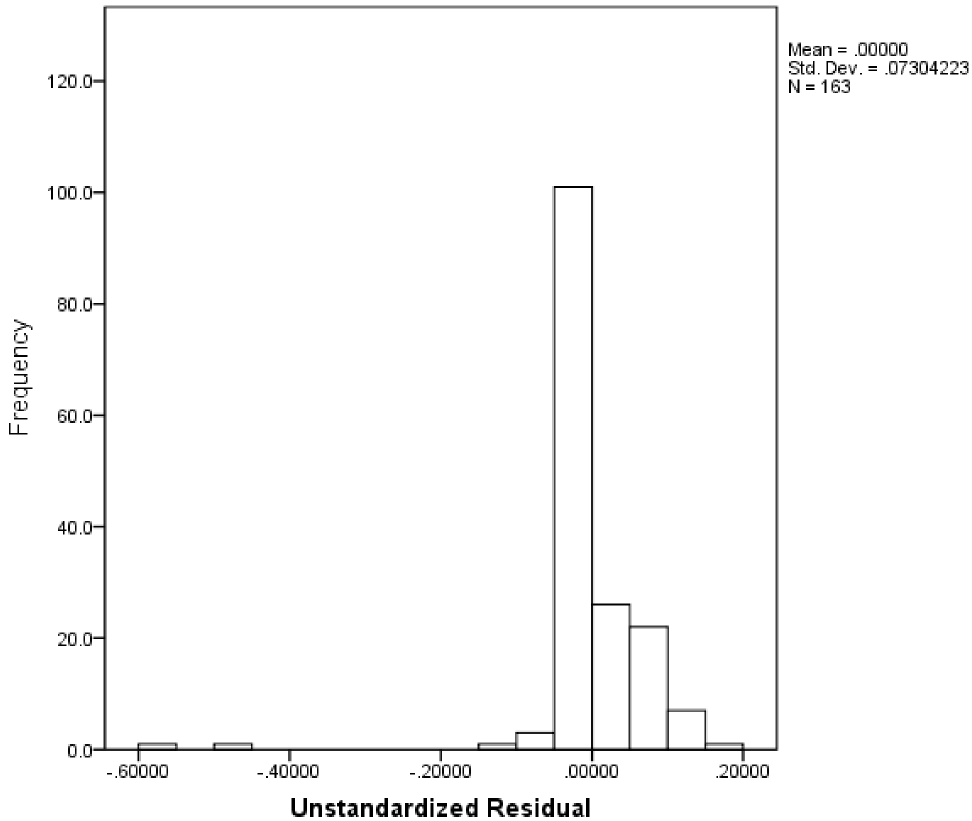

Figure 22. Histogram for unstandardized residuals after natural log transformation.

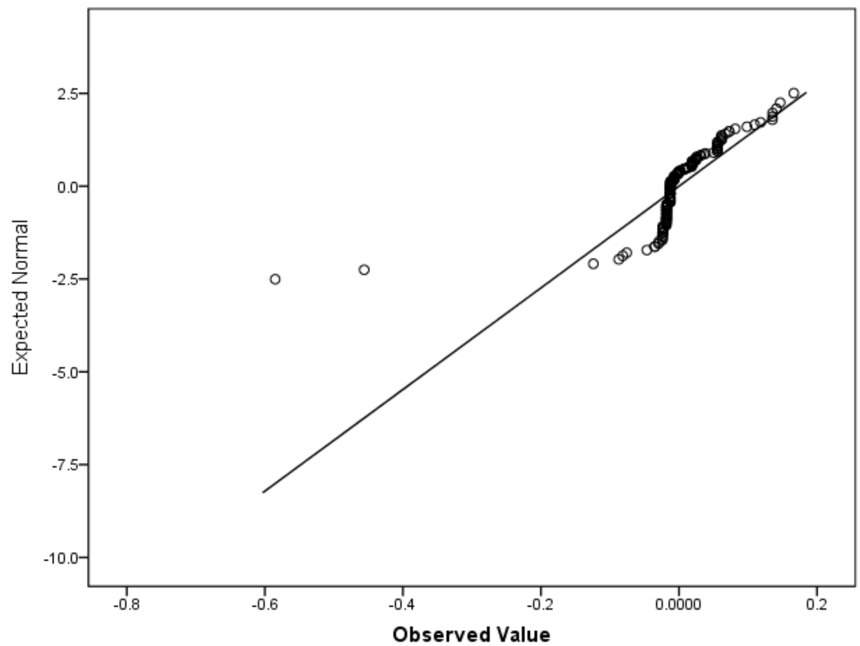

Figure 23. Normal Q-Q plot for unstandardized residuals after natural log transformation.

Z-score transformation. A z-score transformation converts a raw score into a scale value that represents how many standard deviations a particular observation is from the mean for that variable (Mertler & Reinhart, 2017). This transformation does not change the shape of the distribution and thus is not an appropriate method for normalizing data. As such, application of this transformation did not take place.

Bootstrapping. Bootstrapping provides a method of analysis where resampling occurs of empirical observations and data replaced with estimated values for a larger sample size (Mertler & Reinhart, 2017). Bootstrapping is nonparametric and does not require meeting the distributional data assumptions of parametric tests such as multiple linear regression (Nimon & Oswald, 2013; Williams et al., 2013). Since these assumptions no longer apply to the model, normality assumptions validation and reporting does not occur in the following results. The only assumption for bootstrapping is that the sample distribution is a good representation of the study population (Jörg Henseler, Hubona, & Ash, 2016; Rasmussen, 1987). This is a very general assumption. However, the 23.3% response rate for this study (163 valid cases from a population of 699) is well in excess of the originally required 62 responses (to achieve a power of .95, see Figure 2) and is sufficient to meet this assumption.

Bootstrapping was performed at a sample rate of 700 (est. population size), 1,000, and 10,000 with insignificant differences in results. Thus, reporting is only for the 1,000 samples bootstrapping. Model results are the same as those in the initial evaluation (Tables 22 & 23). Below are the coefficients tables for both the bootstrapping (Table 28) and the original multiple linear regression (Table 29) for comparison. Bootstrapping resulted in larger standard errors than the parametrically calculated coefficients. This resulted in larger *p*-values for all independent variables. This is primarily notable for SN, which showed highly significant in the multiple linear regression analysis yet insignificant in the bootstrapped assessment.

Table 28

Bootstrap for Coefficients

			Bootstrap[a]				
						95% Confidence interval	
Model		B	Bias	Std. error	Sig. (2-tailed)	Lower	Upper
1	(Constant)	9.695	.450	2.350	.101	5.848	14.569
	ATT	.007	.003	.021	.813	-.032	.047
	SN	.380	-.040	.185	.134	.010	.660
	PBC	-.054	.007	.044	.314	-.137	.021

a. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples

Table 29

Original Coefficients[a] from Initial Multiple Linear Regression Analysis

Model		Unstandardized coefficients B	Unstandardized coefficients Std. error	Standardized coefficients Beta	t	Sig.	95.0% Confidence interval for B Lower bound	95.0% Confidence interval for B Upper bound
1	(Constant)	9.695	.839		11.550	.000	8.037	11.353
	ATT	.007	.018	.025	.385	.701	-.028	.041
	SN	.380	.046	.542	8.192	.000	.289	.472
	PBC	-.054	.043	-.082	-1.239	.217	-.140	.032

a. Dependent Variable: IB

Summary of corrective measures. The mathematical corrective measures provided no improved results in meeting residual distributional assumptions. This left the multiple linear regression analysis results subject to errors and unsupportable. One could consider the bootstrapping results to be a solution to the nonnormal condition of the residual distribution. However, given the strength and fit of the prediction model, it is surprising that no independent variable showed to be significant after bootstrapping, including SN, which was highly significant in the initial multiple linear regression analysis.

SN does continue to show to be the most significant of the independent variables in the bootstrapping results at $p = .134$, followed by PBC and ATT. The result of having no significant variables in a significant model can occur when there is multicollinearity between the independent variables (Dunlap & Kemery, 1987). However, the analysis shows this is not the case (see Table 24). Some scholars consider bootstrapping to be an underpowered method that does not accurately represent the nature of the variables analyzed (M. Aguirre-Urreta & Ronkko, 2015; Rasmussen, 1987). One could interpret the results of the bootstrapping in this study in this way, particularly for SN, suggesting that the resampled variables and their relation to the dependent variable may not completely represent what empirical findings gathered from a larger population may show. Some argue results from nonnormal multiple linear regression are possibly more relevant than bootstrapping results (Dawes, 1979; Rasmussen, 1987). Due to these findings, it became interesting to perform an alternate analysis in an attempt to identify more clearly the effects of the independent variables. Performing a logistic regression provided additional analysis and discussion of the results occurs in the next section.

Logistic Regression Data Analysis

Logistic regression is similar to multiple linear regression in its ability to assess how multiple independent variables effect a dependent variable. Logistic regression is for use in situations where the dependent variable is not continuous (Lever, Krzywinski, & Altman, 2016) as in the study data set. The difference between multiple linear regression and logistic regression is that in logistic regression the dependent variable is categorical and the results of logistic regression analysis show how likely the independent variables are to influence a respondent's membership in a particular category (Mertler & Reinhart, 2017). Logistic regression has the benefits of no distributional assumptions for the data and is useful when distribution of the dependent variable is nonlinear with one or more independent variables (Mertler & Reinhart, 2017) which is true in this data set.

Even though there are no data distribution assumptions with logistic regression, there are two important test assumptions. The first is that the independent variables are linearly related to the log odds of the probability being analyzed (Arsanjani, Helbich, Kainz, & Boloorani, 2013; Mertler & Reinhart, 2017). A Hosmer-Lemeshow goodness of fit test (Fagerland & Hosmer, 2016) was used to test for this assumption. The other concern is that there is not strong multicollinearity of the predictors (Mertler & Reinhart, 2017). The test for this assumption is in the same manner as in multiple linear regression. The previous testing shows that multicollinearity does not exist (see Table 24).

In the study data, the majority of the dependent variable responses were the same with a value of 15. In order to perform a binary logistic regression, it was necessary to divide the responses into two categories: those who scored a 15, and those who did not. The analysis will then show how the independent variables influence membership in a particular group as an odds ratio. This type of analysis is also able to answer the study hypotheses. The analysis will show to what extent the independent variables of TPB affect intention to follow information security policy by showing how the independent variables effect “full intention” to comply (by being in the group that scores a “perfect” 15), or being in the other group that does not have “full intention” to comply.

First, recoding occurred for the IB variable into a new variable IB_15. Here the value was set to “1” if the respondent scored a 15 for IB or set to “0” if the respondent did not score a 15. IB_15 became the new dependent variable in the model. The goal of the logistic regression model is to determine the probability that a respondent having a value of “1” (full intent to comply) has a relationship to the three independent variables of ATT, SN, and PBC. Data screening for logistic regression is the same for multiple linear regression (Mertler & Reinhart, 2017) and I completed this process in the multiple linear regression analysis. I used the same screened data set for the logistic regression.

Binary logistic regression using the enter method was performed to determine to what extent the independent variables of ATT, SN, and PBC were predictors of having full intention to comply (IB = 15) or not having full intention to comply (IB ≠ 15). Data screening led to the elimination of two cases due to study qualification answers. Regression results indicated that the overall model was statistically significant (*– 2 Log Likelihood* = 69.795, X^2 (3) = 10.754, $p < .05$). Again, as in the multiple linear regression, rejection of the null hypothesis is appropriate. Tables 30 & 31 provide analysis statistics.

Table 30

Model Summary

Step	-2 Log likelihood	Cox & Snell R square	Nagelkerke R square
1	69.795[a]	.064	.164

a. Estimation terminated at iteration number 6 because parameter estimates changed by less than .001.

Table 31

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	10.754	3	.013
	Block	10.754	3	.013
	Model	10.754	3	.013

The model correctly classified 93.9% of the cases (Table 32). Wald statistics indicated that the SN variable was significant (X^2 (1) = 7.794, $p < .01$). The independent variables of ATT and PBC were not significant. The odds ratios (Exp(B)) for SN indicate the odds of an IB equaling 15 multiply by 1.638 for each one point increase of SN across respondents. An alternative interpretation is for each additional one point in SN the odds of showing “full intention” to comply (with information security policy) increases by 63.8%. Presentation of variable statistics is in Table 33.

Table 32

Classification Table[a]

			Predicted		
			IB_15		Percentage
	Observed		.00	1.00	correct
Step 1	IB_15	.00	1	10	9.1
		1.00	0	152	100.0
	Overall percentage				93.9

a. The cut value is .500

Table 33

Statistics for Variables in the Equation

								95% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1[a]	ATT	.154	.090	2.944	1	.086	1.167	.978	1.392
	SN	.494	.177	7.794	1	.005	1.638	1.158	2.317
	PBC	-.131	.252	.271	1	.603	.877	.535	1.438
	Constant	-6.443	3.821	2.843	1	.092	.002		

a. Variable(s) entered on step 1: ATT, SN, PBC.

Test assumptions. A Hosmer-Lemeshow goodness of fit test provided the check for the assumption that a linear relationship exists between the independent variables and the log odds of the probability being analyzed. The null hypothesis of this test is that the fit is appropriate (Fagerland & Hosmer, 2016). The resulting *p*-value of .460 (X^2 (8) = 7.736, $p > .05$) indicates that the null hypothesis is not rejected and the fit of the logistic regression is appropriate (see Table 34). As mentioned earlier, the prior multiple linear regression analysis demonstrated nonmulticollinearity between the independent variables (see Table 24) meeting this test assumption.

Table 34

Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	7.736	8	.460

Summary of Statistical Analyses

Initial multiple linear regression analysis showed the study model based on TPB significantly predicted IB and identified one variable, SN, to be a significant predictor. However, analysis of residuals showed that the data set did not meet several distributional assumptions resulting in the findings being inconclusive and unsupportable. I performed several corrective procedures on the data set to resolve the data condition issues such as square root, log, and z-score transformations. None of these transformations resulted in improved data conditions. Multiple linear regression analysis with bootstrapping returned the same significant model findings, however no variables showed significant. In an attempt to identify significant variables, a second analysis followed using a logistic regression approach. Like the multiple linear regression analysis, the logistic regression also showed the study model to be significant and rejected the null hypothesis. The logistic regression also showed the SN variable as being significant in predicting those respondents who fully intend to comply with information security policy as compared to those who do not.

Discussion of Findings

The empirical results of this study provided good support for the concept that the human behavior factors present in TPB are predictors of human intention in terms of complying with information security policies. The hypotheses for this study were:

$H1_0$: Attitude toward the behavior, subjective norm, and perceived behavioral control does not affect the intention of computer end users in a K-12 environment to follow information security policy.

$H1_a$: Attitude toward the behavior, subjective norm, and perceived behavioral control does affect the intention of computer end users in a K-12 environment to follow information security policy.

A standard multiple linear regression, $\alpha = .05$ (two-tailed), and a logistic regression, $\alpha = .05$ (two-tailed), were performed. Both statistical processes found the theoretical model of the study to be significant and rejected the null hypothesis. Results from these analyses for the multiple linear regression were $R^2 = .308$, $R^2_{adj} = .294$, F (3, 159) = 23.537, $p < .001$ and for the logistic regression – *2 Log Likelihood* = 69.795, X^2 (3) = 10.754, $p < .05$.

Of the three independent variables of TPB, only SN showed to be a significantly strong predictor of IB in the initial multiple linear regression ($t(159) = 8.192$, $p < .001$) and the logistic regression (X^2 (1) = 7.794, $p < .01$). However, SN was not significant in the multiple linear regression bootstrapping results ($t(159) = 8.192$, $p > .05$). Multiple linear regression showed SN to have a positive slope (.380) indicating that for every point increase in SN there is a 38% increase in IB.

Neither ATT nor PBC showed significance in the models and were opposite to each other in terms of level of significance in some of the analyses. In the initial and bootstrapped multiple linear regression analysis PBC was second and ATT third in terms of significance. However, in the logistic regression positions reversed with ATT second and PBC third. Having differing outcomes in this regard is understandable as the two analysis methods present similar results from a different approach. Multiple linear regression is measuring direct effect of the predictors on the response variable, where the logistic regression is predicting odds of predictors resulting in membership to a group.

ATT showed to be an insignificant predictor of IB in the initial multiple linear regression ($t(159) = .385$, $p > .05$), multiple linear regression bootstrapping ($t(159) =$ $.385$, $p > .05$), and logistic regression (X^2 (1) = 2.944, $p > .05$). Multiple linear regression showed ATT to have a positive slope (.007) indicating that for every point increase in ATT there is a 0.7% increase in IB. This slope is negligible, and with $p > .05$ ATT cannot be considered a predictor of IB in this study.

PBC also showed to be an insignificant predictor in the initial multiple linear regression ($t(159) = -1.239$, $p > .05$), multiple linear regression bootstrapping ($t(159) = -$

1.239, $p > .05$), and logistic regression (X^2 (1) = .271, $p > .05$). Multiple linear regression showed PBC to have a negative slope (-.054) indicating that for every point increase in PBC there is a 5.4% decrease in IB. This would be an interesting point if PBC were a significant predictor of IB, however with $p > .05$ this was not the case in this study.

Theoretical discussion. When comparing to existing literature, I confirmed in this study the effectiveness of TPB as a predictive model for intention the same as it has been in all previous applications both in information security related studies and studies not related to information security cited in the preceding literature review. Armitage & Conner (2001) and Sommestad et al. (2015) extensively reviewed and tested this theory and its effectiveness, and in this study, I confirmed their findings that TPB is a valid model for predicting intention. The literature review contains many studies that apply TPB in this manner and all have shown the model significant. With no contrasting findings for the model in the literature review, simply listing all the cited studies that have the same findings as this one would be redundant. The greater discussion for this study existed in the findings related to the significance of the predictors themselves.

As documented in the literature review, the significance level of the TPB predictors differs widely across information security studies and studies not related to information security. Likewise, several studies show one or more of the predictors insignificant at some point in time. This is in line with Ajzen’s (1991) suggestion that the significance of each independent construct in the TPB framework will depend on the subject matter and sample population. However, generally speaking, the ATT construct tends to be more predominant, and the SN construct lesser so, with PBC falling somewhere in the middle.

Lebek (2014), in a review of IT studies applying TPB, showed that eight of ten studies demonstrated significant correlations between ATT and IB with six of those studies showing strong relationships at the $p < 0.01$ level. Researchers equally confirm the significance of ATT in many other TPB related IT studies (Arpaci & Baloglu, 2016; Dang-Pham et al., 2017; Flores & Ekstedt, 2016; Gurung & Raja, 2016; Herath et al., 2014; Jafarkarimi et al., 2016; Moody & Siponen, 2013; Safa et al., 2016) as well as non-IT studies (Ajzen & Klobas, 2013; Ajzen & Sheikh, 2013; Castanier et al., 2013; Dawson et al., 2014; Efrat & Shoham, 2013; Greaves et al., 2013; Tipton, 2014; Zemore & Ajzen, 2014). The findings in this literature contrast with the findings of this study and make it notable that ATT was not significant. However, these findings coincide with two of the studies reviewed by Lebek that did not show ATT as being significant in predicting IB.

The findings of this study showed SN being the most significant predictor and indicate that the drivers in the study environment differed from those of other studies performed in other environments. Other related IT studies, typically performed in corporations or surveying college students, find SN to be a weak (Dinev & Hu, 2007; Jafarkarimi et al., 2016) or insignificant (Yoon & Kim, 2013) predictor of IB. In a review of 161 studies applying TPB, Armitage & Conner (2001) found subjective norm to be the weakest of predictors overall. However, in the K-12 school system environment of this study, the perceptions of others and their thoughts towards information security were a substantial driver toward the information security intentions of the population.

Other TPB based information security studies support the findings of this study regarding the significance of SN. One study showed SN to be at minimum a strong predictor (Yazdanmehr & Wang, 2015) and some such as Cox (2012), Safa (2015), and Hu et al. (2012) showed SN to be the most significant predictor of IB in the model. Other studies not related to information security such as Greaves et al. (2013) and Prapavessis et al. (2015) also support the results of this study through finding SN the strongest predictor of IB.

The findings of this study showed PBC to be insignificant. This contrasts with Lebek (2014) who determined that 92% of the correlations in existing information security literature between PBC and IB to be significant at $p < 0.05$ levels. However, the findings of this study are supported by several studies that find this construct to be the weakest predictor of intention (Ajzen & Klobas, 2013; Ajzen & Sheikh, 2013; Castanier et al., 2013; Greaves et al., 2013; Prapavessis et al., 2015) or insignificant (Greaves et al., 2013; Tipton, 2014).

The insignificance of ATT and PBC in the study environment may be the result of the organization having already well addressed the motivational factors that define these variables via their current SETA efforts. It is possible that the organization has set the correct mindset regarding the potential vulnerability and severity of negative information security events and enabled the respondents to take appropriate action in these cases. This would result in individual views in these areas being largely the same. This would be an area for further research and such discussion occurs in a following section. However, it is evident by the strength of SN, which represents the social pressure perceived by the individual to perform or not perform a particular behavior (Ajzen, 1991; Yazdanmehr & Wang, 2015), was a strong driver for respondents information security compliance intentions in the study environment.

Current literature. This section provides theoretical discussion of relevant literature published since the writing of the literature review in Section 2 in comparison to the findings of this study. The review included seven information security studies and five non-IT studies utilizing TPB. All of the participants for the studies reviewed were college students or employees of commercial businesses. None of the studies addressed the educational sector. The studies remained consistent with past literature in the fact that the three variables of TPB showed differing levels of significance depending on various factors of the study.

Three information security studies based on TPB found all the variables in the theoretical model to be significant. One study addressing medical records privacy with hospital employees found SN to be the most significant predictor (Sher, Talley, Yang, & Kuo, 2017) providing support for the findings of this study. The second utilized three PMT/TPB hybrid models to assess intentions to use online banking (Jansen & van Schaik, 2017). Here separation occurred for SN into injunctive and descriptive norms, with descriptive norms having a similar definition as normative beliefs in this study report and was found significant where the injunctive norms were not. Separation also occurred for PBC in the second reviewed study into self-efficacy and locus of control, supporting the indicators used for this study. The third was a German study regarding productivity and security with the order of variable significance being ATT, SN, and

PBC (Mayer, Gerber, McDermott, Volkamer, & Vogt, 2017). The third study was of particular interest as it specifically addresses the measurement factor of reward that was included in this study and found the indicator associated with a decrease in security compliance.

Four of the five non-IT studies reviewed found all the variables of TPB significant as well. Three of these studies found ATT the most significant, followed by SN and then PBC (Park, Hsieh, & Lee, 2017; Record, 2017; Heetae Yang, Lee, & Zo, 2017). The fourth ordered the significance of variables as PBC, ATT, then SN (Jiang, Ling, Feng, Wang, & Guo, 2017). These findings differed from the study in this report in the fact that only one variable was significant (SN) in this study and that SN was not the most significant in any of the other studies.

The remaining studies reviewed had differing and mixed results. A study on information disclosure among social network users found ATT the most significant factor and SN insignificant (Koohikamali, Peak, & Prybutok, 2017). The same findings existed in a non-IT study very similar to the study in this report addressing policy compliance at an overall HR level (instead of only the IT level) (Hofeditz, Nienaber, Dysvik, & Schewe, 2017). These findings were in direct contrast to those in this study report. A study addressing information security awareness (a key component of SETA) found ATT and SN both significant, but not PBC (Bauer & Bernroider, 2017). Other study examples were of interest as they contained good support for the measurement indicators used in the reported study (Anwar et al., 2017; Snyman & Kruger, 2017), however they were too conceptually different for direct comparison.

The study reviewed that provided the most support for this study was one with participants in the Department of Defense where the researchers utilized eight different TPB models in analyzing employee status as a driver for information security compliance (Aurigemma & Mattson, 2017). Here, in all eight models, SN was the most significant variable with ATT insignificant and PBC only weakly so. All of the research findings reviewed in these recent studies go back to supporting Ajzen's (2002) assertion that the significance of TPB variables will vary greatly depending on study conditions.

Applications to Professional Practice

End users often engage in risky behavior and represent the weakest link in the information security chain (Cox, 2012; Ifinedo, 2012). Technical solutions alone are not sufficient to protect against human behavior vulnerabilities (Ahmad et al., 2014; Da Veiga & Martins, 2015a; Flores et al., 2014; Safa et al., 2016). Implementation of SETA is a nontechnical information security control to aid in protecting a computer environment from human behaviors (Posey et al., 2014). NIST 800-53 (NIST, 2015) places SETA development responsibility specifically with the IT security program manager. Use of sociobehavioral theories has been effective in predicting information security compliant behavior (Lebek et al., 2014; Sommestad et al., 2015) and providing data to improve SETA campaigns (Posey et al., 2014). The findings from this study may aid IT security program managers in K-12 organizations in implementing multilayered solutions that include addressing human reactions, behaviors, and motivators (Ahmad et al., 2014) that, when combined with technical protections, could make for a more effective data protection model.

The population for this study was the 699 K-12 school administrators of the Bigg County Public School System located in Northeast Georgia. The literature showed there is a need to look at motivators of organizational managers, such as school administrators, that change organization operations and results in potential major data exposure (Hu et al., 2012). K-12 information security program managers have an interest in K-12 administrators as they represent the leaders and decision makers for technology implementation and information security at the individual school level (Blau & Presser, 2013; Metcalf, 2012; Raman et al., 2014; Weng & Tang, 2014) much as senior management in corporations (Barton et al., 2016). This means that exposure and guidance for technology and policy for K-12 faculty, staff, and students largely disseminates through the K-12 administration (Metcalf, 2012). K-12 information security program managers, by gaining an understanding of K-12 administrators information security motivators and developing SETA programs that address these motivators, are able to implement SETA campaigns as a security control for human information security behaviors in the K-12 environment.

The drivers and beliefs of those receiving information security messages must be considered when developing effective SETA programs (Allam et al., 2014; Furman et al., 2012; Tsohou, Karyda, & Kokolakis, 2015). The findings of this study present IT security program managers in K-12 organizations additional insight into aspects of human behavior to consider. These findings indicate that the technocratic SETA approach (Ashenden & Sasse, 2013; Reece & Stahl, 2015) needs to be modified to include considerations for human drivers such as ATT, SN, and PBC. The discussion below begins with SN, as it was the significant predictor of IB in the study environment. Argument for ATT and PBC will conclude this section.

Salient normative beliefs of the individual influence SN (Armitage & Conner, 2001). Here the individual is concerned with whether or not those individuals or groups important to them approve or disapprove of performing a particular behavior (Yoon & Kim, 2013). To address this motivational factor, IT security program managers may develop SETA programs that involve the exposure of individuals' information security related thoughts and expectations to others in the population through social interaction groups. This approach places more emphasis on the awareness component of SETA (Dinev & Hu, 2007; Flores & Ekstedt, 2016; Hanus & Wu, 2016; Kearney & Kruger, 2016; Montesdioca & Maçada, 2015) as opposed to just providing technical vulnerability education and security training. Exposing the true thoughts and drivers of others may help prevent misconceptions regarding social norms in the form of pluralistic ignorance and false consensus (H. Chen & Li, 2014).

SN may also be addressed through other SETA methods such as the development of clear information security policies, communication of policies, and confirmation of awareness and knowledge (Allam et al., 2014; Soomro et al., 2016). These approaches set all perceptions the same instead of individual thoughts being open to interpretation through normative beliefs. This information can be conveyed via formal or informal knowledge sharing processes in the organization (Dang-Pham et al., 2017; Flores et al., 2014).

Due to the importance of SN in determining IB shown in this study, IT security program managers are encouraged to investigate the information security culture of the organization. This investigation is to discover what are the current information security mindsets and perceptions in the environment, where they come from, and how they are developed and communicated (Ashenden & Sasse, 2013; Tsohou, Karyda, Kokolakis, et al., 2015; Wilson & Hash, 2003). In other words, find out why some computer users make the decisions they do and how others learn about and ultimately follow these decisions and actions. If these thoughts and actions are determined to be information security negative, IT security program managers should attempt to correct them. They can achieve this by developing policies that enable the workforce to do their job effectively and securely, and then interrupt and intervene in the communication process to inject this information to correct information security related perceptions (Allam et al., 2014; Furman et al., 2012; Rashid et al., 2013; Soomro et al., 2016). IT security program managers should not let information security policy be a block to productivity and improvement but instead educate the end user on how to achieve organization goals safely (Thapa & Harnesk, 2014).

Although ATT and PBC did not show significance on their own in this study, they are still validated parts of the theoretical model that IT security program managers should address. ATT is defined here as the favorable or unfavorable appraisal an individual holds regarding a particular behavior (Ajzen, 1991) and can be influenced by training that modifies this trait (Parsons, McCormac, Butavicius, et al., 2014). This training should include exposing and explaining information security vulnerabilities (Dinev & Hu, 2007;

Flores & Ekstedt, 2016; Hanus & Wu, 2016; Kearney & Kruger, 2016; Montesdioca & Maçada, 2015), aiding end users in understanding the severity of these vulnerabilities (Arachchilage & Love, 2014; Komatsu et al., 2013; Öğütçü et al., 2016), and developing programs that reward positive information security behaviors directly or indirectly. Direct reward can be in the form of performance reviews (Cheng et al., 2013; Farahmand et al., 2013). Indirect reward may simply be in the form of providing a positive information security culture where an end user is encouraged and acknowledged for bringing forth information security concerns when attempting to meet organizational goals (Posey et al., 2015; Siponen et al., 2014).

Salient control beliefs held by the individual influence PBC (Ajzen, 2002) such as locus of control and self-efficacy (Ajzen, 1991). Locus of control is how much an individual believes performing an act is in their control, and self-efficacy is their ability to perform an act effectively (Ajzen, 2002). IT security program managers should address each of these elements through SETA. SETA programs should not be limited to only informing individuals of risks, but advising them what actions they can take in response to risks and what the outcome and effect of their actions will have to negate this risk. IT security program managers should follow with technical training that provides the individual with the tools and the confidence to effectively perform risk aversion actions when required. The focus of these trainings should be to enable and empower the individual in regards to taking corrective information security actions.

Implications for Social Change

The intention of this study was to identify drivers of information security related human behavior in order for IT security program managers in K-12 environments to develop improved SETA programs. The education sector is at high risk for information security breaches (Okpamen, 2013; Pardo & Siemens, 2014) and improved security has implications for social change. SETA programs are effective in increasing the security posture of an organization (NIST, 2015). IT security program managers accomplish this through changes in moral beliefs (Pfleeger et al., 2014), effecting intentions to comply with policies (Choi et al., 2013), and transforming organizational culture (Ashenden & Sasse, 2013; D'Arcy & Greene, 2014; Karlsson et al., 2015) in regards to information security. The study findings have identified TPB as a sufficient predictive model of information security drivers, and SN showed to be a significant motivational factor that when addressed in the K-12 environment could improve the information security posture of the organization.

When a K-12 organization is at risk for security breaches, many groups and individuals are subject to harm. This includes the employees of the organization, the vulnerable student population, as well as the school system itself. School systems are viewed by many as a core organization in a community (Sanders, 2015) and as a result have direct implications on the safety and reputation of a community overall. Harm may occur through exposure of private information that may be used to directly or indirectly damage individuals, their families, or the organization. Examples of potential harms at the individual level are exposure of location, abduction, and identify theft. Harms at the organizational level include exposure of internal operations, physical security, and damage to reputation. Through the development of improved SETA programs that address the findings of this study, K-12 IT security program managers may make the organization and community safer and less vulnerable to information security threats. This in turn effects social change through more secure communities and increased freedoms and privacy for individuals (DHS Privacy Office and the Office for Civil Rights and Civil Liberties, 2015).

Recommendations for Action

The education sector has been shown to be at high levels of information security risk due to poor habits, practices, and motivation (Chou & Chou, 2016). This study applied TPB in order to identify human behavior factors in K-12 organizations that drive intentions for information security compliance. Study findings show SN as a significant factor. Consideration of this factor in improved SETA programs by IT security program managers may result in a more secure organization, improved privacy for employees and students, and increased community protections. Providing this report and results from this study to the IT department of Bigg County Public Schools with the following recommendations will occur with these goals in mind.

The first recommendation is that the IT department of Bigg County Public Schools provides the findings of this study to their IT security program manager(s). The purpose of sharing this information with these individuals is to inform them of discovered human factors that drive intentions to comply with information security policies in that organization. The dissemination of these findings may occur through providing this report directly, a revised summary document developed by the organization that includes these findings with other organizational security goals, or through visual and oral presentation in live meeting scenarios in line with the normal operations of the organization.

The study findings show that SN is significant in determining individuals' intention to follow information security policy. The second recommendation is that the IT security program manager(s) consider this finding when developing improved SETA programs. These improvements should include discovering formal and informal communications paths in the organization that shape the normative beliefs of the individuals and result in the forming of SN. SETA programs should then be created that properly expose the true thoughts of individuals regarding information security compliance to the broader target audience in a manner than properly sets intention and expectation for information security policy compliance.

The third recommendation is to improve SETA campaigns to convey the desired understanding of information security vulnerabilities and protective actions into the organizational communications processes. This may be through formal training as well as awareness programs communicated via electronic and print media. Reinforcement of such programs should include technical training that enables and empowers individuals to take corrective and protective information security actions. This recommendation addresses the ATT and PBC aspects of the TPB model, which although not identified as individually significant in the study, are still relevant and important in the TPB model and driving information security compliance intention.

Recommendations for Further Study

The limitations of this study provide a basis for recommendations for further study. The first limitation identified was the potential for differentiation in the level of SETA exposure for the study participants possibly skewing understanding of information security related questions or holding a better understanding of information security issues. Future study could investigate the level of SETA exposure of the end user and/or assess information security compliance intention based on categorical SETA-exposed group membership.

This study applied the single theoretical model of TPB. The limitation is that other factors not part of the TPB model could be affecting information security compliance intention. Identification of these factors may not occur in a study under the confines of a single theory. Two separate approaches are available for future study to address this limitation. One approach would be to apply a differing theory with differing independent variables/factors. Another approach would be to apply a qualitative methodology, as opposed to the quantitative methodology of this study, in order to explore the environment in a manner as to expose and identify motivational factors for information security compliance intention.

Other methodological limitations are present in this study in terms of time line and data collection. The cross-sectional nature of this study gives a limited snapshot of conditions at a single point in time. Thoughts and opinions regarding information security can change over time (Crossler et al., 2013), and a longitudinal study may more accurately identify information security compliance motivational factors. When considering data collection, self-reported data has the potential to provide socially desirable answers. A more accurate method of data collection may be observation of actual behavior as opposed to measuring intention. An alternative method of data gathering such as live interviews may also provide differing insight if performed in line with the methodological approach of an overall exploratory study.

Limitations existed in this study in terms of population in that it was limited to K-12 school administrators. The findings of this study may not be generalizable to other populations in other school systems, corporations, or organizations. The stated expectation in the study proposal was that this study would provide statistical generalizability to the K-12 administration population. Groups other than those studied may hold differing information security thoughts, beliefs, and motivations.

Differing types of computer end users exist in the K-12 environment including other faculty, staff, and students. I acknowledged in the study that results may not be generalizable to the entire population of K-12 computer end users. K-12 administrators, faculty, and staff do have similar computer use cases as they have largely independent and unencumbered usage of technology, have exposure to the same or similar information security policies, are under indirect supervision, and are largely the target of SETA programs developed by information security program managers. Based on this, some generalization is possible.

Generalizability of information systems research can happen at four different levels: Generalizing from data to description, generalizing from description to theory, generalizing theory to description, and generalizing from concepts to theory (Lee &

Baskerville, 2003). In this study, generalization from data to description is possible as the findings from the study sample could generalize to the unstudied population of K-12 faculty and staff due to the similarity in computer use case.

The computer use case for K-12 students is different as they use computers under limited access, strict direction, and direct supervision. There is also an expectation that the measures for the independent variables of TPB may be different for an adolescent student population. This is in line with Ajzen's (2002) expectation of measures to differ between populations when applying TPB. This group may be the target of some SETA programs, but exposure is not directly from the information security program managers but passed down through K-12 administrators and faculty. It is possible for the results of this study to generalize from description to theory for the student group (Lee & Baskerville, 2003). This suggests that the study findings support the application of the chosen theory (TPB) to this population. However, this would require empirical validation. Further detailed discussion of these points occurs in the "Participants," "Population and Sampling," and "Study Validity" sections of this paper. Future study could focus on another population in a K-12 school system or another organization entirely. The size of the school system studied is also atypical, and a study of more commonly sized systems could be beneficial.

A different approach to data analysis could also be beneficial. This study applied multiple linear regression and logistic regression to the variables of TPB. Other analysis approaches such as structural equation modeling (SEM) may provide greater insight to which measurement indicators are more significant in describing the independent variables providing a more granular view into the theoretical model.

Lastly, the information security literature provides a wide range of information security compliance research suggestions loosely related to this study. Suggestions exist such as investigating information security culture in the organization, personality traits that drive compliance, and organizational factors that may influence information security. The "Aspects for Further Research Cited in Extant Literature" section of the literature review provides additional details on these topics.

Reflections

This study provided some interesting results and insights for myself as the researcher. Having worked in the research environment, I had observed various attitudes and actions of end users in relation to information security. This bias is one of the major factors that drove toward a quantitative study approach as to discover accurate results not influenced by my own preconceptions. Regarding the study results, there was a greater expectation that ATT would have a significantly high influence on information security compliance based on my observations and the existing literature. The results of the study showing this variable to be insignificant was an intriguing finding and changed my thoughts on the strength of this driver in the environment.

There was an expectation of finding SN significant based on direct observations in the environment. Individuals often cited following the actions and opinions of others in the organization as justification for their own individual actions. Finding PBC insignificant was also not surprising as I had a perception that the organization had already done well at technical training and empowering the end users to make information security related decisions and take appropriate actions. As a result, this variable is not an intention driver in the environment. Neither the findings for SN or PCB changed my perceptions for these motivators.

The response to the study by the organization and participants was positive and greater than expected. Information security can be a sensitive subject area and often such studies experience a low response rate. This was not the case in this study. The participants were eager and active, providing for a 23.3% response rate. The high level of support for doctoral studies (as many of those surveyed have or are pursing such degrees), holding such degrees in high regard, and support for the pursuit of education in general in the environment may attribute to the positive response.

I do not think my involvement or the act of performing the study had any direct effect on the study population or organization. However, I do believe the results of the study will have an effect for both. If the organization gives consideration for the results and recommendations, I do believe the study organization can become a more secure environment and the study population will gain from policies that both protect individuals and the organization as well as support accomplishing the goals and objectives of the organization. I also believe this could result in social change through the improvement of privacy and freedom for individuals and a safer, more secure community.

Summary and Study Conclusions

The education sector is at high risk for information security breaches (Misenheimer, 2014; Okpamen, 2013; Pardo & Siemens, 2014; Romanosky et al., 2014) and in need of improved security practices (Chou & Chou, 2016). Achieving information security cannot be through technical means alone (Ahmad et al., 2014; Da Veiga & Martins, 2015a; Flores et al., 2014; Safa et al., 2016). Addressing the human factor is required as it is the weakest link in the information security chain (Cox, 2012; Ifinedo, 2012). SETA is an effect method of addressing human information security behavior (Ahlan et al., 2015; Safa et al., 2015). Applying sociobehavioral theories to information security research provides information to aid IT security program managers in developing improved SETA programs (Lebek et al., 2014).

This study showed TPB to be an effective model for predicting intention to comply with information security policies. SN was a significant predictor of intention in the TPB model and addressing this factor may improve SETA programs. The TPB constructs of ATT and PBC did not show significant in this study. However, they are still part of the predictive model and including them should occur during SETA development and improvement. The application of improved SETA programs that incorporate the findings and recommendations of this study could lead to a more secure school system. A more secure school system may contribute to greater information and security protection for employees, students, and the community.

References

Acharya, A. S., Prakash, A., Saxena, P., & Nigam, A. (2013). Sampling: why and how of it? *Indian Journal of Medical Specialities*, *4*(2). http://doi.org/10.7713/ijms.2013.0032

Aguinis, H., & Edwards, J. R. (2014). Methodological wishes for the next decade and how to make wishes come true. *Journal of Management Studies*, *51*(1), 143–174. http://doi.org/10.1111/joms.12058

Aguirre-Urreta, M. I., Marakas, G. M., & Ellis, M. E. (2013). Measurement of composite reliability in research using partial least squares : Some issues and an alternative approach. *Data Base for Advances in Information Systems*, *44*(4), 11–43. http://doi.org/10.1145/2544415.2544417

Aguirre-Urreta, M., & Ronkko, M. (2015). Sample size determination and statistical power analysis in PLS using R : An annotated tutorial. *Communications of the Association for Information Systems*, *36*(1), 33–51. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3830&context=cais

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: Its antecedents and measures. *Procedia Computer Science*, *72*, 361–373. http://doi.org/10.1016/j.procs.2015.12.151

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. http://doi.org/10.1007/s10845-012-0683-0

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl &

J. Beckmann (Eds.), *Action Control* (pp. 11–39). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. http://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683. http://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I. (2014). The theory of planned behaviour is alive and well, and not ready to retire: A commentary on Sniehotta, Presseau, and Araújo-Soares. *Health Psychology Review*, *7199*(May), 1–7. http://doi.org/10.1080/17437199.2014.883474

Ajzen, I., & Klobas, J. (2013). Fertility intentions: An approach based on the theory of planned behaviour. *Demographic Research*, *29*(8), 203–232. http://doi.org/10.4054/DemRes.2013.29.8

Ajzen, I., & Sheikh, S. (2013). Action versus inaction: Anticipated affect in the theory of planned behavior. *Journal of Applied Social Psychology*, *43*(1), 155–162. http://doi.org/10.1111/j.1559-1816.2012.00989.x

Al-Alawi, A. I., Al-Kandari, S. M. H., & Abdel-Razek, R. H. (2016). Evaluation of information systems security awareness in higher education : An empirical study of Kuwait University. *Journal of Innovation and Business Best Practice*, *2016*. http://doi.org/10.5171/2016.329374

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations.

Information and Computer Security, *23*(1), 102–118. http://doi.org/10.1108/ICS-03-2014-0018

Alaskar, M., Vodanovich, S., & Shen, K. N. (2015). Evolvement of information security research on employees' behavior: A systematic review and future direction. In *2015 48th Hawaii International Conference on System Sciences* (pp. 4241–4250). http://doi.org/10.1109/HICSS.2015.508

Albaum, G., Roster, C. A., Smith, S. M., Albaum, G., & Smith, S. M. (2014). Topic sensitivity and research design: effects on internet survey respondents' motives. *Asia Pacific Journal of Marketing and Logistics*, *26*(1), 147–161. http://doi.org/10.1108/APJML-12-2012-0127

Aldridge, J. (2014). Working with vulnerable groups in social research: dilemmas by default and design. *Qualitative Research*, *14*(1), 112–130. http://doi.org/10.1177/1468794112455041

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

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*, 55–65. http://doi.org/10.1016/j.cose.2014.01.005

Ames, D. R., Rose, P., & Anderson, C. P. (2006). The NPI-16 as a short measure of narcissism. *Journal of Research in Personality*, *40*(4), 440–450. http://doi.org/10.1016/j.jrp.2005.03.002

Ansolabehere, S., & Schaffner, B. F. (2014). Does survey mode still matter? Findings from a 2010 multi-mode comparison. *Political Analysis*, *22*(3), 285–303. http://doi.org/10.1093/pan/mpt025

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. http://doi.org/10.1016/j.chb.2016.12.040

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. http://doi.org/10.1016/j.chb.2014.05.046

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185–197. http://doi.org/10.1016/j.chb.2016.02.065

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology*, *40*(4), 471–499. http://doi.org/10.1348/014466601164939

Arpaci, I., & Baloglu, M. (2016). The impact of cultural collectivism on knowledge sharing among information technology majoring undergraduates. *Computers in Human Behavior*, *56*, 65–71. http://doi.org/10.1016/j.chb.2015.11.031

Arsanjani, J. J., Helbich, M., Kainz, W., & Boloorani, A. D. (2013). Integration of logistic regression, Markov chain and cellular automata models to simulate urban expansion. *International Journal of Applied Earth Observation and Geoinformation*, *21*(1), 265–275. http://doi.org/10.1016/j.jag.2011.12.014

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers and Security*, *39*(PART B), 396–405. http://doi.org/10.1016/j.cose.2013.09.004

Astrachan, C. B., Patel, V. K., & Wanzenried, G. (2014). A comparative study of CB-SEM and PLS-SEM for theory development in family firm research. *Journal of Family Business Strategy*, *5*(1), 116–128. http://doi.org/10.1016/j.jfbs.2013.12.002

Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers and Security*, *66*, 218–234. http://doi.org/10.1016/j.cose.2017.02.006

Austin, E. J., Saklofske, D. H., Smith, M., & Tohver, G. (2014). Associations of the managing the emotions of others (MEOS) scale with personality, the Dark Triad and trait EI. *Personality and Individual Differences*, *65*, 8–13. http://doi.org/10.1016/j.paid.2014.01.060

Ayatollahi, H., Bath, P. A., Goodacre, S., Lo, S. Y., Draegebo, M., & Khan, F. A. (2013). What factors influence emergency department staff attitudes towards using information technology? *Emergency Medicine Journal*, *30*(4), 303–307 5p. http://doi.org/10.1136/emermed-2011-200446

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

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don’t make excuses!

Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*(Part B), 145–159. http://doi.org/10.1016/j.cose.2013.05.006

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*(217528), 32–45. http://doi.org/10.1016/j.cose.2016.05.004

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, *59*, 9–25. http://doi.org/10.1016/j.cose.2016.02.007

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *Data Base for Advances in Information Systems*, 48(3), 44-68. http://doi.org/10.1145/3130515.3130519

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61. http://doi.org/10.1016/j.chb.2015.01.039

Bennett, N. D., Croke, B. F. W., Guariso, G., Guillaume, J. H. A., Hamilton, S. H., Jakeman, A. J., . . . Andreassian, V. (2013). Characterising performance of environmental models. *Environmental Modelling and Software*, *40*, 1–20. http://doi.org/10.1016/j.envsoft.2012.09.011

Berenson, M. L. (2013). Using excel for White’s test-an important technique for evaluating the equality of variance assumption and model specification in a regression analysis. *Decision Sciences Journal of Innovative Education*, *11*(3), 243–262. http://doi.org/10.1111/dsji.12008

Bettany-Saltikov, J., & Whittaker, V. J. (2014). Selecting the most appropriate inferential statistical test for your quantitative research study. *Journal of Clinical Nursing*, *23*(11–12), 1520–1531. http://doi.org/10.1111/jocn.12343

Beville, J. M., Umstattd Meyer, M. R., Usdan, S. L., Turner, L. W., Jackson, J. C., & Lian, B. E. (2014). Gender differences in college leisure time physical activity: Application of the theory of planned behavior and integrated behavioral model. *Journal of American College Health*, *62*(3), 173–184. http://doi.org/10.1080/07448481.2013.872648

Bishop, A. C., Baker, G. R., Boyle, T. A., & MacKinnon, N. J. (2015). Using the health belief model to explain patient involvement in patient safety. *Health Expectations*, *18*(6), 3019–3033. http://doi.org/10.1111/hex.12286

Blau, I., & Presser, O. (2013). E-Leadership of school principals: Increasing school effectiveness by a school data management system. *British Journal of Educational Technology*, *44*(6), 1000–1011. http://doi.org/10.1111/bjet.12088

Bornstein, M. H., Jager, J., & Putnick, D. L. (2013). Sampling in developmental science: Situations, shortcomings, solutions, and standards. *Developmental Review*, *33*(4), 357–370. http://doi.org/10.1016/j.dr.2013.08.003

Boss, S. R., Galletta, D. F., Lowry, P. B., 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 behaviours. *MIS Quarterly*, *39*(4), 837–864.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy*, *12*(1), 28–38. http://doi.org/10.1109/MSP.2013.106

Casson, R. J., & Farmer, L. D. M. (2014). Understanding and checking the assumptions of linear regression: A primer for medical researchers. *Clinical and Experimental Ophthalmology*, *42*(6), 590–596. http://doi.org/10.1111/ceo.12358

Castanier, C., Deroche, T., & Woodman, T. (2013). Theory of planned behaviour and road violations: The moderating influence of perceived behavioural control. *Transportation Research Part F: Traffic Psychology and Behaviour*, *18*, 148–158. http://doi.org/10.1016/j.trf.2012.12.014

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2013). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information and Management*, *52*(4), 385–400. http://doi.org/10.1016/j.im.2014.12.004

Chan, L., & Bishop, B. (2013). A moral basis for recycling: Extending the theory of planned behaviour. *Journal of Environmental Psychology*, *36*, 96–102. http://doi.org/10.1016/j.jenvp.2013.07.010

Charlwood, A., Forde, C., Grugulis, I., Hardy, K., Kirkpatrick, I., MacKenzie, R., & Stuart, M. (2014). Clear, rigorous and relevant: publishing quantitative research articles. *Work, Employment & Society*, *28*(2), 155–167. http://doi.org/10.1177/0950017014526448

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. http://doi.org/10.1080/07421222.2014.1001257

Chen, H., & Li, W. (2014). Understanding organization employee`s information security omission behavior: An integrated model of social norm and deterrence. In *Pacific Asia Conference on Information Systems 2014 Proceedings*. Chengdu, China. Retrieved from http://aisel.aisnet.org/pacis2014/280

Chen, M. F., & Tung, P. J. (2014). Developing an extended Theory of Planned Behavior model to predict consumers' intention to visit green hotels. *International Journal of Hospitality Management*, *36*, 221–230. http://doi.org/10.1016/j.ijhm.2013.09.006

Chen, Y., Li, Y., Wu, H., & Liang, L. (2014). Data envelopment analysis with missing data: A multiple linear regression analysis approach. *International Journal of Information Technology & Decision Making*, *13*(1), 137–153. http://doi.org/10.1142/S0219622014500060

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*(PART B), 447–459. http://doi.org/10.1016/j.cose.2013.09.009

Choi, M., Levy, Y., & Hovav, A. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In *pre-ICIS workshop on Information Security and Privacy (SIGSEC)*. Retrieved from http://aisel.aisnet.org/wisp2012/29

Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, *65*, 334–345. http://doi.org/10.1016/j.chb.2016.08.034

Cook, D. A., Zendejas, B., Hamstra, S. J., Hatala, R., & Brydges, R. (2014). What counts as validity evidence? Examples and prevalence in a systematic review of simulation-based assessment. *Advances in Health Sciences Education*, *19*(2), 233–250. http://doi.org/10.1007/s10459-013-9458-4

Cox, J. A. (2012). *Organizational narcissism as a factor in information security: A structured model of the user knowing-doing gap*. Capella University (Dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI No. 3499909)

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. http://doi.org/10.1016/j.cose.2012.09.010

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. http://doi.org/10.2308/isys-50704

Crysel, L. C., Crosier, B. S., & Webster, G. D. (2013). The Dark Triad and risk behavior. *Personality and Individual Differences*, *54*(1), 35–40. http://doi.org/10.1016/j.paid.2012.07.029

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474–489. http://doi.org/10.1108/IMCS-08-2013-0057

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. http://doi.org/10.2753/MIS0742-1222310210

Da Veiga, A., & Martins, N. (2015a). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162–176. http://doi.org/10.1016/j.cose.2014.12.006

Da Veiga, A., & Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review*, *31*(2), 243–256. http://doi.org/10.1016/j.clsr.2015.01.005

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, *48*, 281–297. http://doi.org/10.1016/j.cose.2014.11.002

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, *67*, 196–206. http://doi.org/10.1016/j.chb.2016.10.025

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. *International Journal of Human Computer Studies*, *72*(2), 154–168. http://doi.org/10.1016/j.ijhcs.2013.10.003

Dawes, R. M. (1979). The robust beauty of improper linear models in decision making. *American Psychologist*, *34*(7), 571–582. http://doi.org/10.1037//0003-066X.34.7.571

Dawson, L., Mullan, B., & Sainsbury, K. (2014). Using the theory of planned behaviour to measure motivation for recovery in anorexia nervosa. *Appetite*, *84*, 309–315. http://doi.org/10.1016/j.appet.2014.10.028

de Leeuw, A., Valois, P., Ajzen, I., & Schmidt, P. (2015). Using the theory of planned behavior to identify key beliefs underlying pro-environmental behavior in high-school students: Implications for educational interventions. *Journal of Environmental Psychology*, *42*, 128–138. http://doi.org/10.1016/j.jenvp.2015.03.005

DeLyser, D., & Sui, D. (2013). Crossing the qualitative- quantitative divide II: Inventive approaches to big data, mobile methods, and rhythmanalysis. *Progress in Human Geography*, *37*(2), 293–305. http://doi.org/10.1177/0309132512444063

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153. http://doi.org/10.1046/j.1365-2575.2001.00099.x

DHS Privacy Office and the Office for Civil Rights and Civil Liberties. (2015). *Executive order 13636 privacy and civil liberties assessment report*. Washington, DC: Author. Retrieved from https://www.dhs.gov/publication/2015-executive-order-13636-privacy-and-civil-liberties-assessment-report

Dietrich, F., & List, C. (2013). A reason-based theory of rational choice. *Nous*, *47*(1), 104–134. http://doi.org/10.1111/j.1468-0068.2011.00840.x

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1325&context=jais

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(April), 92–100. http://doi.org/10.4236/jis.2013.42011

Djajadikerta, H. G., Roni, S. M., & Trireksani, T. (2015). Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research. *Information and Management*, *52*(8), 1012–1024. http://doi.org/10.1016/j.im.2015.07.008

Donald, I. J., Cooper, S. R., & Conchie, S. M. (2014). An extended theory of planned behaviour model of the psychological factors affecting commuters' transport mode use. *Journal of Environmental Psychology*, *40*, 39–48. http://doi.org/10.1016/j.jenvp.2014.03.003

Doyle, G. J., Garrett, B., & Currie, L. M. (2014). Integrating mobile devices into nursing curricula: Opportunities for implementation using Rogers' diffusion of innovation model. *Nurse Education Today*, *34*(5), 775–782. http://doi.org/10.1016/j.nedt.2013.10.021

Drouin, N., & Jugdev, K. (2014). Standing on the shoulders of strategic management giants to advance organizational project management. *International Journal of Managing Projects in Business*, *7*(1), 61–77. http://doi.org/10.1108/IJMPB-04-2013-0021

Dunlap, W. P., & Kemery, E. R. (1987). Failure to detect moderating effects: Is multicollinearity the problem? *Psychological Bulletin*, *102*(3), 418–420. http://doi.org/10.1037/0033-2909.102.3.418

Efrat, K., & Shoham, A. (2013). The theory of planned behavior, materialism, and aggressive driving. *Accident Analysis and Prevention*, *59*, 459–465. http://doi.org/10.1016/j.aap.2013.06.023

Experian. (2015). *Data breach industry forecast*. Schaumburg, IL: Author. Retrieved from http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182

Fagerland, M. W., & Hosmer, D. W. (2016). Tests for goodness of fit in ordinal logistic regression models. *Journal of Statistical Computation and Simulation*, *86*(17), 3398–3418. http://doi.org/10.1080/00949655.2016.1156682

Farahmand, F., Atallah, M. M. J., & Spafford, E. H. (2013). Incentive alignment and risk perception: An information security application. *IEEE Transactions on Engineering Management*, *60*(2), 238–246. http://doi.org/10.1109/TEM.2012.2185801

Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. *Information Systems Frontiers*, *15*(1), 5–15. http://doi.org/10.1007/s10796-010-9265-x

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–60. http://doi.org/10.3758/BRM.41.4.1149

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs - Principles and practices. *Health Services Research*, *48*(6 PART2), 2134–2156. http://doi.org/10.1111/1475-6773.12117

Finn, A., & Wang, L. (2014). Formative vs. reflective measures: Facets of variation. *Journal of Business Research*, *67*(1), 2821–2826. http://doi.org/10.1016/j.jbusres.2012.08.001

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley. Retrieved from http://people.umass.edu/aizen/f&a1975.html

Flick, U. (2015). Qualitative inquiry--2.0 at 20? Developments, trends, and challenges for the politics of research. *Qualitative Inquiry*, *21*(7), 599–608. http://doi.org/10.1177/1077800415583296

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. http://doi.org/10.1016/j.cose.2014.03.004

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26–44. http://doi.org/10.1016/j.cose.2016.01.004

Font, X., Garay, L., & Jones, S. (2016). A social cognitive theory of sustainability empathy. *Annals of Tourism Research*, *58*, 65–80. http://doi.org/10.1016/j.annals.2016.02.004

Furman, S., Theofanos, M. F., Choong, Y. Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions. *IEEE Security and Privacy*, *10*(2), 40–49. http://doi.org/10.1109/MSP.2011.180

Galvez, S. M., Shackman, J. D., Guzman, I. R., & Ho, S. M. (2015). Factors affecting individual information security practices. In *Proceedings of the 2015 ACM Special Interest Group on Management Information Systems Conference on Computers and People Research '15* (pp. 135–144). New York, NY: ACM Press. http://doi.org/10.1145/2751957.2751966

Galvin, B. M., Lange, D., & Ashforth, B. E. (2015). Narcissistic organizational identification: Seeing oneself as central to the organization's identity. *Academy of Management Review*, *40*(2), 163–181. http://doi.org/10.5465/amr.2013.0103

Gnambs, T., & Kaspar, K. (2014). Disclosure of sensitive behaviors across self-administered survey modes: a meta-analysis. *Behavior Research Methods*, 1–23. http://doi.org/10.3758/s13428-014-0533-4

Goertz, G., & Mahoney, J. (2013). Methodological rorschach tests: Contrasting interpretations in qualitative and quantitative research. *Comparative Political Studies*, *46*(2), 236–251. http://doi.org/10.1177/0010414012466376

Grabemann, M., Mette, C., Zimmermann, M., Wiltfang, J., & Kis, B. (2014). Serum albumin correlates with affective prosody in adult males with attention-deficit hyperactivity disorder. *Psychiatry Research*, *217*(3), 198–201.

http://doi.org/10.1016/j.psychres.2014.03.030

Granato, D., de Araújo Calado, V. M., & Jarvis, B. (2014). Observations on the use of statistical methods in food science and technology. *Food Research International*, *55*(October), 137–149. http://doi.org/10.1016/j.foodres.2013.10.024

Greaves, M., Zibarras, L. D., & Stride, C. (2013). Using the theory of planned behavior to explore environmental behavioral intentions in the workplace. *Journal of Environmental Psychology*, *34*, 109–120. http://doi.org/10.1016/j.jenvp.2013.02.003

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *Africa Research Journal*, *104*(2), 69–79. Retrieved from http://cdn.entelectonline.co.za/wm-418498-cmsimages/ARJv102.v2.pdf#page=33

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*(1), 242–251. http://doi.org/10.1016/j.cose.2012.10.003

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security*, *24*(4), 348–371. http://doi.org/10.1108/ICS-05-2015-0020

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. http://doi.org/10.2753/MTP1069-6679190202

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long Range Planning*, *46*(1–2), 1–12. http://doi.org/10.1016/j.lrp.2013.01.001

Hales, S., Lesher-Trevino, A., Ford, N., Maher, D., & Tran, N. (2016). Reporting guidelines for implementation and operational research. *Bulletin of the World Health Organization*, *94*(January 2016), 58–64. http://doi.org/10.2471/BLT.15.167585

Halfens, R. J. G., & Meijers, J. M. M. (2013). Back to basics: An introduction to statistics. *Journal of Wound Care*, *22*(5), 248–51. http://doi.org/10.12968/jowc.2013.22.5.248

Hankins, M., French, D., & Horne, R. (2000). Statistical guidelines for studies of the theory of reasoned action and the theory of planned behaviour. *Psychology & Health*, *15*(2), 151–161. http://doi.org/10.1080/08870440008400297

Hannigan, A., & Lynch, C. D. (2013). Statistical methodology in oral and dental research: Pitfalls and recommendations. *Journal of Dentistry*, *41*(5), 385–392. http://doi.org/10.1016/j.jdent.2013.02.013

Hanus, B., & Wu, Y. "Andy." (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16. http://doi.org/10.1080/10580530.2015.1117842

Hazen, B. T., Overstreet, R. E., & Boone, C. A. (2015). Suggested reporting guidelines for structural equation modeling in supply chain management research. *International Journal of Logistics Management*, *26*(3), 627–641. http://doi.org/10.1108/JFM-03-2013-0017

Henry, G. T., Smith, A. A., Kershaw, D. C., & Zulli, R. A. (2013). Formative evaluation: Estimating preliminary outcomes and testing rival explanations. *American Journal of Evaluation*, *34*(4), 465–485. http://doi.org/10.1177/1098214013502577

Henseler, J., Hubona, R., & Ash, P. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, *116*(1), 2–20. http://doi.org/10.1108/02635570710734262

Henseler, J., Ringle, C. M., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. http://doi.org/10.1007/s11747-014-0403-8

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61–84. http://doi.org/10.1111/j.1365-2575.2012.00420.x

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. http://doi.org/10.1016/j.dss.2009.02.005

Heyvaert, M., Maes, B., & Onghena, P. (2013). Mixed methods research synthesis: Definition, framework, and potential. *Quality & Quantity*, *47*(2), 659–676. http://doi.org/10.1007/s11135-011-9538-6

Hofeditz, M., Nienaber, A. M., Dysvik, A., & Schewe, G. (2017). “Want to” versus “have to”: Intrinsic and extrinsic motivators as predictors of compliance behavior intention. *Human Resource Management*, *56*(1), 25–49. http://doi.org/10.1002/hrm.21774

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. http://doi.org/10.1111/j.1540-5915.2012.00361.x

IBM Corp. (2015). IBM SPSS Statistics for Windows, Version 23.0. Armonk, NY: IBM Corp.

Identity Theft Resource Center. (2014). *Data breach reports*. San Diego, CA: Author. Retrieved from http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. http://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. http://doi.org/10.1016/j.im.2013.10.001

Ingenhoff, D., & Buhmann, A. (2016). Advancing PR measurement and evaluation: Demonstrating the properties and assessment of variance-based structural equation models using an example study on corporate reputation. *Public Relations Review*, *42*(3), 418–431. http://doi.org/10.1016/j.pubrev.2015.11.010

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H., & Hee, J. M. (2016). Behavioral intention in social networking sites ethical dilemmas: An extended model based on theory of planned behavior. *Computers in Human Behavior*, *62*, 545–561. http://doi.org/10.1016/j.chb.2016.04.024

Jakobsen, M., & Jensen, R. (2015). Common method bias in public management studies. *International Public Management Journal*, *18*(1), 3–30. http://doi.org/10.1080/10967494.2014.997906

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, *25*(2), 165–180. http://doi.org/10.1108/ICS-03-2017-0018

Jiang, K., Ling, F., Feng, Z., Wang, K., & Guo, L. (2017). Psychological predictors of mobile phone use while crossing the street among college students: An application of the theory of planned behavior. *Traffic Injury Prevention*, *18*(2), 118–123. http://doi.org/10.1080/15389588.2016.1236195

John Opala, O., Rahman, S., & Alelaiwi, A. (2015). The influence of information security on the adoption of cloud computing: An exploratory analysis. *International Journal of Computer Networks & Communications*, *7*(4), 57–74. http://doi.org/10.5121/ijcnc.2015.7404

Johnson, M. E., Brems, C., Hanson, B. L., Corey, S. L., Eldridge, G. D., & Mitchell, K. (2013). Conducting ethical research with correctional populations: Do researchers and IRB members know the federal regulations? *Research Ethics*, *10*(1), 6–16. http://doi.org/10.1177/1747016113494652

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), 113–134.

Jung, B., & Kim, S. (2014). A festival satisfaction evaluation method using multiple regression analysis. *International Journal of Software Engineering and Its Applications*, *8*(4), 187–196. http://doi.org/10.14257/ijseia.2014.8.4.20

Kajzer, M., Darcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security*, *43*, 64–76. http://doi.org/10.1016/j.cose.2014.03.003

Karlsson, F., Astrom, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information and Computer Security*, *23*(3), 246–278. http://doi.org/http://dx.doi.org/10.1108/ICS-05-2014-0033

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, *61*, 46–58. http://doi.org/10.1016/j.cose.2016.05.006

Kim, C., Kim, M. K., Lee, C., Spector, J. M., & DeMeester, K. (2013). Teacher beliefs and technology integration. *Teaching and Teacher Education*, *29*(1), 76–85. http://doi.org/10.1016/j.tate.2012.08.005

Kim, D., & Ammeter, T. (2014). Predicting personal information system adoption using an integrated diffusion model. *Information and Management*, *51*(4), 451–464. http://doi.org/10.1016/j.im.2014.02.011

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

Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security and Privacy*, *10*(2), 24–32. http://doi.org/10.1109/MSP.2011.179

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with brazilian users. *Journal of Information Systems and Technology Management*, *13*(3), 479–496. http://doi.org/10.4301/S1807-17752016000300007

Kohlborn, T. (2014). Quality assessment of service bundles for governmental one-stop portals: A literature review. *Government Information Quarterly*, *31*(2), 221–228. http://doi.org/10.1016/j.giq.2013.10.006

Kokkinos, C. M., Baltzidis, E., & Xynogala, D. (2016). Prevalence and personality correlates of Facebook bullying among university undergraduates. *Computers in Human Behavior*, *55*, 840–850. http://doi.org/10.1016/j.chb.2015.10.017

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, *33*, 3–11. http://doi.org/10.1016/j.cose.2012.07.001

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security. *Information Management & Computer Security*, *21*, 5–15. http://doi.org/doi:10.1108/09685221311314383

Koohikamali, M., Peak, D. A., & Prybutok, V. R. (2017). Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human*

Behavior, *69*, 29–42. http://doi.org/10.1016/j.chb.2016.12.012

Krumpal, I. (2013). Determinants of social desirability bias in sensitive surveys: A literature review. *Quality & Quantity*, *47*(4), 2025–2047. http://doi.org/10.1007/s11135-011-9640-9

Kumar, G., & Kumar, K. (2014). Network security – an updated perspective. *Systems Science & Control Engineering*, *2*(1), 325–334. http://doi.org/10.1080/21642583.2014.895969

Lakens, D. (2013). Calculating and reporting effect sizes to facilitate cumulative science: A practical primer for t-tests and ANOVAs. *Frontiers in Psychology*, *4*(NOV), 1–12. http://doi.org/10.3389/fpsyg.2013.00863

Lancsar, E., & Swait, J. (2014). Reconceptualising the external validity of discrete choice experiments. *PharmacoEconomics*, *32*(10), 951–965. http://doi.org/10.1007/s40273-014-0181-7

Landers, R. N., & Behrend, T. S. (2015). An inconvenient truth: Arbitrary distinctions between organizational, Mechanical Turk, and other convenience samples. *Industrial and Organizational Psychology*, *8*(March), 1–23. http://doi.org/10.1017/iop.2015.13

Lange, M. M., Rogers, W., & Dodds, S. (2013). Vulnerability in research ethics: A way forward. *Bioethics*, *27*(6), 333–340. http://doi.org/10.1111/bioe.12032

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. http://doi.org/10.1108/MRR-04-2013-0085

Lebo, M., & Weber, C. (2015). An effective approach to the repeated cross sectional design. *American Journal of Political Science*, *59*(1), 242–258. http://doi.org/10.7910/DVN1/22651

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research*, *14*(3), 221–243. http://doi.org/10.1287/isre.14.3.221.16560

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60–70. http://doi.org/10.1016/j.cose.2016.02.004

Lee, M. Y. (2014). The effect of nonzero autocorrelation coefficients on the distributions of Durbin-Watson test estimator: Three autoregressive models. *Expert Journal of Economics*, *2*(3), 85–99. Retrieved from http://economics.expertjournals.com/23597704-211/

Lever, J., Krzywinski, M., & Altman, N. (2016). Points of significance: Logistic regression. *Nature Methods*, *13*(7), 541–542. http://doi.org/10.1038/nmeth.3904

Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, *78*(1), 13–21. http://doi.org/10.1016/j.knosys.2015.01.009

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, *57*(2), 123–146. http://doi.org/10.1109/TPC.2014.2312452

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193–273. http://doi.org/10.1111/isj.12063

MacFarlane, K., & Woolfson, L. M. (2013). Teacher attitudes and behavior toward the inclusion of children with social, emotional and behavioral difficulties in mainstream schools: An application of the theory of planned behavior. *Teaching and Teacher Education*, *29*(1), 46–52. http://doi.org/10.1016/j.tate.2012.08.006

Mahmood, J., Dahlan, H. M., Hussin, A. R. C., & Ahmad, M. A. (2016). Review on knowledge sharing behavior studies: Theories and research approaches. *Indian Journal of Science and Technology*, *9*(34). http://doi.org/10.17485/ijst/2016/v9i34/100834

Mahon, P. Y. (2014). Internet research and ethics: Transformative issues in nursing education research. *Journal of Professional Nursing*, *30*(2), 124–129. http://doi.org/10.1016/j.profnurs.2013.06.007

Marcellesi, A. (2015). External validity: Is there still a problem? *Philosophy of Science*, *82*(5), 1308–1317. http://doi.org/10.1086/684084

Mathieu, C. (2013). Personality and job satisfaction: The role of narcissism. *Personality and Individual Differences*, *55*(6), 650–654. http://doi.org/10.1016/j.paid.2013.05.012

McCormack, L. A., Friedrich, C., Fahrenwald, N., & Specker, B. (2014). Feasibility and acceptability of alternate methods of postnatal data collection. *Maternal and Child Health Journal*, *18*(4), 852–857. http://doi.org/10.1007/s10995-013-1310-1

Mertler, C. A., & Reinhart, R. V. (2017). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). New York, NY: Routledge.

Metcalf, W. B. (2012). *K-12 principals' perceptions of their technology leadership preparedness*. Georgia Sothern University (Dissertation). Retrieved from Electronic Theses & Dissertations. Paper 400

Michie, S., & West, R. (2013). Behaviour change theory and evidence: A presentation to Government. *Health Psychology Review*, *7*(1), 1–22. http://doi.org/10.1080/17437199.2011.649445

Misenheimer, K. J. (2014). *Exploring information technology security requirements for academic institutions to reduce information security attacks, breaches, and threats*. Northcentral University (Dissertation).

Mlikotic, R., Parker, B., & Rajapakshe, R. (2016). Assessing the effects of participant preference and demographics in the usage of web-based survey questionnaires by women attending screening mammography in British Columbia. *Journal of Medical Internet Research*, *18*(3), e70. http://doi.org/10.2196/jmir.5068

Montanaro, E. a, & Bryan, A. D. (2014). Comparing theory-based condom interventions: Health belief model versus theory of planned behavior. *Health Psychology*, *33*(10), 1251–1260. http://doi.org/10.1037/a0033969

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48*, 267–280.

http://doi.org/10.1016/j.cose.2014.10.015

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

Mortenson, M. J., & Vidgen, R. (2016). A computational literature review of the technology acceptance model. *International Journal of Information Management*, *36*(6), 1248–1259. http://doi.org/10.1016/j.ijinfomgt.2016.07.007

Moyo, M. (2013). Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems. In *2013 Information Security for South Africa* (pp. 1–6). Johannesburg: IEEE. http://doi.org/10.1109/ISSA.2013.6641062

Mullan, B., Allom, V., Sainsbury, K., & Monds, L. A. (2015). Examining the predictive utility of an extended theory of planned behaviour model in the context of specific individual safe food-handling. *Appetite*, *90*, 91–98. http://doi.org/10.1016/j.appet.2015.02.033

Nathans, L., Oswald, F., & Nimon, K. (2012). Interpreting multiple linear regression: A guidebook of variable importance. *Practical Assesment Research & Evaluation*, *17*(9), 19. http://doi.org/10.3102/00346543074004525

National Institute of Standards and Technology. (2015). *Security and privacy controls for federal information systems and organizations*. *Special Publication 800-53 Revision 4*. Gaithersburg, MD: Author. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

National Institute of Standards and Technology Joint Task Force. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. *NIST Special Publication 800-53* (Vol. 4). Gaithersburg, MD: Author. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Navarro-Gonzalez, D., Lorenzo-seva, U., & Vigil-colet, A. (2016). How response bias affects the factorial structure of personality self-reports. *Psicothema: Revista de Psicologia*, *28*(4), 465–470. http://doi.org/10.7334/psicothema2016.113

Newman, I., Hitchcock, J. H., & Newman, D. (2015). The use of research syntheses and nomological networks to develop HRD theory. *Advances in Developing Human Resources*, *17*(1), 117–134. http://doi.org/10.1177/1523422314559810

Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security*, *53*, 132–142. http://doi.org/10.1016/j.cose.2015.05.011

Nimon, K. F., & Oswald, F. L. (2013). Understanding the results of multiple linear regression: Beyond standardized regression coefficients. *Organizational Research Methods, 16*(4), 650–674. http://doi.org/10.1177/1094428113493929

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93. http://doi.org/10.1016/j.cose.2015.10.002

Okpamen, P. (2013). Security requirements, analysis and policy formulation for educational institutions. *Journal of Educational and Social Research, 3*(5), 93–102. http://doi.org/10.5901/jesr.2013.v3n5p93

Ord, A. S., Ripley, J. S., Hook, J., & Erspamer, T. (2016). Teaching statistics in APA-accredited doctoral programs in clinical and counseling psychology: A syllabi review. *Teaching of Psychology*, *43*(3), 221–226. http://doi.org/10.1177/0098628316649478

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533–544. http://doi.org/DOI 10.1007/s10488-013-0528-y

Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology*, *45*(3), 438–450. http://doi.org/10.1111/bjet.12152

Park, S. H., Hsieh, C. M., & Lee, C. K. (2017). Examining chinese college students' intention to travel to Japan using the extended theory of planned behavior: Testing destination image and the mediating role of travel constraints. *Journal of Travel & Tourism Marketing*, *34*(1), 113–131. http://doi.org/10.1080/10548408.2016.1141154

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. http://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations.

Information Management & Computer Security, *22*(4), 334–345. http://doi.org/10.1108/IMCS-10-2013-0078

Paternoster, R., Bachman, R., Bushway, S., Kerrison, E., & O'Connell, D. (2015). Human agency and explanations of criminal desistance: Arguments for a rational choice theory. *Journal of Developmental and Life-Course Criminology*, 209–235. http://doi.org/10.1007/s40865-015-0013-2

Pearl, J. (2015). Generalizing experimental findings. *Journal of Causal Inference*, *3*(2), 259–266. http://doi.org/10.1515/jci-2015-0025

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

Pham, H.-C., El-Den, J., & Richardson, J. (2016). Stress-based security compliance model – an exploratory study. *Information and Computer Security*, *24*(4), 326–347. http://doi.org/10.1108/ICS-10-2014-0067

Ponemon Institute. (2015). *2015 cost of data breach study: Global analysis*. Traverse City, Michigan: Author. Retrieved from http://www-03.ibm.com/security/data-breach/

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *57*(November), 338–349. http://doi.org/10.1080/07421222.2015.1138374

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R, J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, *37*(4), 1189–1210.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information and Management*, *51*(5), 551–567. http://doi.org/10.1016/j.im.2014.03.009

Prapavessis, H., Gaston, A., & DeJesus, S. (2015). The Theory of Planned Behavior as a model for understanding sedentary behavior. *Psychology of Sport and Exercise*, *19*, 23–32. http://doi.org/10.1016/j.psychsport.2015.02.001

PricewaterhouseCoopers (PwC). (2013). *The global state of information security survey 2014*. New York, NY: Author. Retrieved from http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

Privacy Rights Clearinghouse. (2016). Data Breaches. San Diego, CA: Author. Retrieved June 22, 2016, from https://www.privacyrights.org/data-breach

Raman, A., Don, Y., & Kasim, A. L. (2014). The relationship between principals' technology leadership and teachers' technology use in Malaysian secondary schools. *Asian Social Science*, *10*(18), 30–36. http://doi.org/10.5539/ass.v10n18p30

Randall, D. M., & Gibson, A. M. (1991). Ethical decision making in the medical profession: An application of the theory of planned behavior. *Journal of Business Ethics*, *10*(2), 111–122. http://doi.org/10.1007/BF00383614

Rashid, R. M., Zakaria, O., & Zulhemay, M. N. (2013). The relationship of information security knowledge (ISK) and human factors: Challenges and solution. *Journal of Theoretical and Applied Information Technology*, *57*(1), 67–75.

Rasmussen, J. L. (1987). Estimating correlation coefficients: Bootstrap and parametric approaches. *Psychological Bulletin*, *101*(1), 136–139. http://doi.org/10.1037/0033-2909.101.1.136

Record, R. A. (2017). Tobacco-free policy compliance behaviors among college students: A theory of planned behavior perspective. *Journal of Health Communication*, *22*(7), 562–567. http://doi.org/10.1080/10810730.2017.1318984

Reece, R. P., & Stahl, B. C. (2015). The professionalisation of information security: Perspectives of UK practitioners. *Computers & Security*, *48*, 182–195. http://doi.org/10.1016/j.cose.2014.10.007

Rhodes, R. (2014). Good and not so good medical ethics. *Journal of Medical Ethics*, *41*(1), 71–74. http://doi.org/10.1136/medethics-2014-102312

Ringle, C. M., & Sarstedt, M. (2016). Gain more insight from your PLS-SEM results. *Industrial Management & Data Systems*, *116*(9), 1865–1886. http://doi.org/10.1108/IMDS-10-2015-0449

Romanosky, S., Hoffman, D. a., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*(1), 74–104. http://doi.org/10.2139/ssrn.1986461

Rutkowski, L., & Zhou, Y. (2015). Correcting measurement error in latent regression covariates via the MC-SIMEX method. *Journal of Educational Measurement*, *52*(4), 359–375. http://doi.org/10.1111/jedm.12090

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. http://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 1–13. http://doi.org/10.1016/j.cose.2015.10.006

Said, A. R., Abdullah, H., Uli, J., & Mohamed, Z. A. (2014). Relationship between organizational characteristics and information security knowledge management implementation. *Procedia - Social and Behavioral Sciences*, *123*, 433–443. http://doi.org/10.1016/j.sbspro.2014.01.1442

Sandelowski, M. (2014). Unmixing mixed-methods research. *Research in Nursing and Health*, *37*(1), 3–8. http://doi.org/10.1002/nur.21570

Sanders, M. (2015). Leadership, partnerships, and organizational development: Exploring components of effectiveness in three full-service community schools. *School Effectiveness and School Improvement*, *2*(27), 157–177. http://doi.org/10.1080/09243453.2015.1030432

Sarstedt, M., Ringle, C. M., Smith, D., Reams, R., & Hair, J. F. (2014). Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. *Journal of Family Business Strategy*, *5*(1), 105–115. http://doi.org/10.1016/j.jfbs.2014.01.002

Schubring, S., Lorscheid, I., Meyer, M., & Ringle, C. M. (2016). The PLS agent:

Predictive modeling with PLS-SEM and agent-based simulation. *Journal of Business Research*, *69*(10), 4604–4612. http://doi.org/10.1016/j.jbusres.2016.03.052

Shepherd, M. M., & Mejias, R. J. (2016). Nontechnical deterrence effects of mild and severe internet use policy reminders in reducing employee internet abuse. *International Journal of Human-Computer Interaction*, *32*(7), 557–567. http://doi.org/10.1080/10447318.2016.1183862

Sher, M.-L., Talley, P. C., Yang, C.-W., & Kuo, K.-M. (2017). Compliance with electronic medical records privacy policy: An empirical investigation of hospital information technology staff. *INQUIRY: Journal of Health Care Organization, Provision, and Financing*, *54*(8), 1–12. http://doi.org/10.1177/0046958017711759

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207. http://doi.org/10.1016/j.chb.2015.01.046

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. http://doi.org/10.1016/j.cose.2015.01.002

Silic, M., & Back, A. (2014). Information management & computer security information security: Critical review and future directions for research. *Information Management & Computer Security*, *22*(3), 279–308. http://doi.org/10.1108/IMCS-05-2013-0041

Şimşek, M. (2015). A new metric for flow-level filtering of low-rate DDoS attacks. *Security and Communication Networks*, *8*(18), 3815–3825.

http://doi.org/10.1002/sec.1302

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees’ adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. http://doi.org/10.1016/j.im.2013.08.006

Skorek, M., Song, A. V., & Dunham, Y. (2014). Self-esteem as a mediator between personality traits and body esteem: Path analyses across gender and race/ethnicity. *PLOS ONE*, *9*(11), 1–9. http://doi.org/10.1371/journal.pone.0112086

Skorodumov, B. I., Skorodumova, O. B., & Matronina, L. F. (2015). Research of human factors in information security. *Modern Applied Science*, *9*(5), 287–294. http://doi.org/10.5539/mas.v9n5p287

Sniehotta, F. F., Presseau, J., & Araújo-Soares, V. (2014). Time to retire the theory of planned behaviour. *Health Psychology Review*, *8*(1), 1–7. http://doi.org/10.1080/17437199.2013.869710

Snyman, D. P., & Kruger, H. (2017). The application of behavioural thresholds to analyse collective behaviour in information security. *Information and Computer Security*, *25*(2), 152–164. http://doi.org/10.1108/ICS-03-2017-0015

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

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, *23*(2), 200–217. http://doi.org/10.1108/ICS-04-

2014-0025

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. http://doi.org/10.1016/j.ijinfomgt.2015.11.009

Sparkes, A. C. (2015). Developing mixed methods research in sport and exercise psychology: Critical reflections on five points of controversy. *Psychology of Sport and Exercise*, *16*(P3), 49–59. http://doi.org/10.1016/j.psychsport.2014.08.014

Spurlin, D. F., & Garven, S. (2016). Unique requirements for social science human subjects research within the United States Department of Defense. *Research Ethics, 12*(3), 158-166. http://doi.org/10.1177/1747016115626198

Such, J. M., Gouglidis, A., Knowles, W., Misra, G., & Rashid, A. (2016). Information assurance techniques: Perceived cost effectiveness. *Computers & Security*, *60*, 117–133. http://doi.org/10.1016/j.cose.2016.03.009

Tavakol, M., & Sandars, J. (2014a). Quantitative and qualitative methods in medical education research: AMEE Guide No 90: Part I. *Medical Teacher*, *36*(90), 746–756. http://doi.org/10.3109/0142159X.2014.915298

Tavakol, M., & Sandars, J. (2014b). Quantitative and qualitative methods in medical education research: AMEE Guide No 90: Part II. *Medical Teacher*, *36*(90), 838–848. http://doi.org/10.3109/0142159X.2014.915297

Thapa, D., & Harnesk, D. (2014). Rethinking the information security risk practices: A critical social theory perspective. In *2014 47th Hawaii International Conference on*

System Sciences (pp. 3207–3214). IEEE. http://doi.org/10.1109/HICSS.2014.397

Tipton, J. A. (2014). Using the theory of planned behavior to understand caregivers' intention to serve sugar-sweetened beverages to non-hispanic black preschoolers. *Journal of Pediatric Nursing*, *29*(6), 564–575. http://doi.org/10.1016/j.pedn.2014.07.006

Tonidandel, S., & LeBreton, J. M. (2013). Beyond step-down analysis: A new test for decomposing the importance of dependent variables in MANOVA. *Journal of Applied Psychology*, *98*(3), 469–477. http://doi.org/10.1037/a0032001

Tricco, A. C., Antony, J., Soobiah, C., Kastner, M., MacDonald, H., Cogo, E., . . . Straus, S. E. (2016). Knowledge synthesis methods for integrating qualitative and quantitative data: A scoping review reveals poor operationalization of the methodological steps. *Journal of Clinical Epidemiology*, 1–7. http://doi.org/10.1016/j.jclinepi.2015.12.011

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., J.Rifon, N., & R.Cotten, S. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*(1318885), 138–150. http://doi.org/10.1016/j.cose.2016.02.009

Tsang, E. W. K. (2014). Generalizing from research findings: The merits of case studies. *International Journal of Management Reviews*, *16*(4), 369–383. http://doi.org/10.1111/ijmr.12024

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies:

Recommendations for information security awareness programs. *Computers & Security*, *52*(March 2016), 128–141. http://doi.org/10.1016/j.cose.2015.04.006

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38–58. http://doi.org/10.1057/ejis.2013.27

Turner, T. L., Balmer, D. F., & Coverdale, J. H. (2013). Methodologies and study designs relevant to medical education research. *International Review of Psychiatry*, *25*(3), 301–10. http://doi.org/10.3109/09540261.2013.790310

Vaidyanathan, B., Strand, M., Choi-Fitzpatrick, A., Buschman, T., Davis, M., & Varela, A. (2016). Causality in contemporary American sociology: An empirical assessment and critique. *Journal for the Theory of Social Behaviour*, *46*(1), 3–26. http://doi.org/10.1111/jtsb.12081

van Deursen, A. J., & van Dijk, J. A. (2013). The digital divide shifts to differences in usage. *New Media & Society*, *16*(3), 507–526. http://doi.org/10.1177/1461444813487959

Vater, A., Schröder-Abé, M., Ritter, K., Renneberg, B., Schulze, L., Bosson, J. K., & Roepke, S. (2013). The narcissistic personality inventory: A useful tool for assessing pathological narcissism? Evidence from patients with narcissistic personality disorder. *Journal of Personality Assessment*, *95*(3), 301–308. http://doi.org/10.1080/00223891.2012.732636

Venkatesh, V., Brown, S. a, & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*(1), 21–54.

Verizon. (2015). *2015 data breach investigations report*. Basking Ridge, NJ: Author. Retrieved from http://www.verizonenterprise.com/DBIR/

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy & Security*, *9*(4), 52–79. http://doi.org/10.1080/15536548.2013.10845690

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*. http://doi.org/http://dx.doi.org/10.1016/j.dss.2016.09.013

Weigold, A., Weigold, I. K., & Russell, E. J. (2013). Examination of the equivalence of self-report survey-based paper-and-pencil and internet data collection methods. *Psychological Methods*, *18*(1), 53–70. http://doi.org/10.1037/a0031607

Weinberg, J., Freese, J., & McElhattan, D. (2014). Comparing data characteristics and results of an online factorial survey between a population-based and a crowdsource-recruited sample. *Sociological Science, 1*(August), 292–310. http://doi.org/10.15195/v1.a19

Weng, C.-H., & Tang, Y. (2014). The relationship between technology leadership strategies and effectiveness of school administration: An empirical study. *Computers & Education*, *76*, 91–107. http://doi.org/10.1016/j.compedu.2014.03.010

Whicher, D., Kass, N., Saghai, Y., Faden, R., Tunis, S., & Pronovost, P. (2015). The views of quality improvement professionals and comparative effectiveness researchers on, ethics, IRBs, and oversight. *Journal of Empirical Research on Human Research Ethics*, *10*(2), 132–144. http://doi.org/10.1177/1556264615571558

Wiedermann, W., & Von Eye, A. (2013). Robustness and power of the parametric t test and the nonparametric Wilcoxon test under non-independence of observations. *Psychological Test and Assessment Modeling*, *55*(1), 39–61. Retrieved from http://p16277.typo3server.info/fileadmin/download/ptam/1-2013_20130326/02_Wiedermann.pdf

Williams, M., Grajales, C. A. G., & Kurkiewicz, D. (2013). Assumptions of multiple regression: Correcting two misconceptions. *Practical Assessment, Research & Evaluation*, *18*(11), 1–14.

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

Wilson, M., & Hash, J. (2003). *Building an information technology security awareness and training program*. *NIST Special Publication*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Wolf, E. J., Harrington, K. M., Clark, S. L., & Miller, M. W. (2013). Sample size requirements for structural equation models: An evaluation of power, bias, and solution propriety. *Educational and Psychological Measurement*, *76*(6), 913–934. http://doi.org/10.1177/0013164413495237

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers* *in Human Behavior*, *24*(6), 2799–2816. http://doi.org/10.1016/j.chb.2008.04.005

Wu, Z. J., Lei, J., Yao, D., Wang, M. H., & Musa, S. M. (2013). Chaos-based detection of LDoS attacks. *Journal of Systems and Software*, *86*(1), 211–221. http://doi.org/10.1016/j.jss.2012.07.065

Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: An extension of the theory of planned behavior. *Industrial Management & Data Systems*, *117*(1), 68–89. http://doi.org/10.1108/IMDS-01-2016-0017

Yang, H., Novick, S. J., & LeBlond, D. (2015). Testing assay linearity over a pre-specified range. *Journal of Bopharmaceutical Statistics*, *25*(2), 339–50. http://doi.org/10.1080/10543406.2014.972513

Yazdanmehr, A., & Wang, J. (2015). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36–46. http://doi.org/10.1016/j.dss.2016.09.009

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, *48*(2), 311–325. http://doi.org/doi:10.1111/ejed.12014

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321–332. http://doi.org/10.1177/1356389013497081

Yin, R. K. (2014). *Case study research* (5th ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Yin, S., Wang, G., & Yang, X. (2014). Robust PLS approach for KPI-related prediction and diagnosis against outliers and missing data. *International Journal of Systems*

Science, *45*(7), 1375–1382. http://doi.org/10.1080/00207721.2014.886136

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, *26*(4), 401–419. http://doi.org/10.1108/ITP-12-2012-0147

Yoshikawa, H., Weisner, T. S., Kalil, A., & Way, N. (2013). Mixing qualitative and quantitative research in developmental science: Uses and methodological choices. *Qualitative Psychology*, *1*(S), 3–18. http://doi.org/10.1037/2326-3598.1.S.3

Young, M. D., Plotnikoff, R. C., Collins, C. E., Callister, R., & Morgan, P. J. (2014). Social cognitive theory and physical activity: A systematic review and meta-analysis. *Obesity Reviews*, *15*(12), 983–995. http://doi.org/10.1111/obr.12225

Zemore, S. E., & Ajzen, I. (2014). Predicting substance abuse treatment completion using a new scale based on the theory of planned behavior. *Journal of Substance Abuse Treatment*, *46*(2), 174–182. http://doi.org/10.1016/j.jsat.2013.06.011

Zhai, Q., Lindorff, M., & Cooper, B. (2013). Workplace guanxi: Its dispositional antecedents and mediating role in the affectivity–job satisfaction relationship. *Journal of Business Ethics*, *117*(3), 541–551. http://doi.org/10.1007/s10551-012-1544-7

Appendix A: Research Instrument Permissions

Gmail by Google David Johnson <[redacted]@waldenu.edu>

Request for Research Instrument and Permissions

3 messages

David Johnson <[redacted]@waldenu.edu> Thu, May 14, 2015 at 7:30 PM
To: [redacted]

Hello Dr. Cox,

My name is David Johnson and I am a doctoral student in Walden University's Information Technology program. I have studied your article titled "Information systems user security: A structured model of the knowing–doing gap" published in *Computers in Human Behavior* and find it very interesting. I would like to ask if you would provide me with the survey instrument you used for this study along with permission to use it in my own doctoral studies.

Your approach fits well with my own concepts regarding how individuals react to information security and I am interesting in exploring similar concepts within the K-12 environment where I employed. I am currently deciding between a quantitative study for which I have developed a model similar to and based on your research, or a qualitative study that will add a different approach to the same concept. I believe this study will do well in adding to the body of knowledge regarding applying behavior sciences to study information security from the end-user perspective and address a population different from that of private corporations or higher academia. Of course, I will gladly provide you the results of my study with permissions in exchange for your information and assistance.

Thank you in advance,

David P. Johnson

Student ID # [redacted]

Doctor of Information Technology

[redacted]

[redacted] (H)

[redacted] (C)

[redacted] - Eastern Time Zone

James Cox <[redacted]>
To: David Johnson <[redacted]@waldenu.edu> Wed, May 20, 2015 at 12:49 PM

David,

Sorry for taking so long to respond. I'm traveling and haven't been keeping up with my email well. This article is based on my dissertation, which has all the analysis, questions, etc. You can retrieve it at UMI 3499909. That is the best way to understand how the questions were used. The questions were based on previous work, of course - just modified for my scenario.

You can certainly use the my work. Please remember the work is copyrighted - don't forget to include the citation!

Thanks for the interest,
Jim
[Quoted text hidden]

David P. Johnson <[redacted]waldenu.edu> Wed, May 20, 2015 at 11:13 PM
To: James Cox <[redacted]>

Hello Dr. Cox,

Thank you very much for your reply and permissions. I will certainly provide the citation and my work in return.

[redacted]

Thanks again,
David Johnson
[Quoted text hidden]
--
Using Opera's mail client: http://www.opera.com/mail/

Gmail by Google

David Johnson <[redacted]@waldenu.edu>

Request Permissions to Use Research Instrument (NPI-16)

Ames, Daniel <[redacted] Sat, Aug 6, 2016 at 8:18 AM
To: David Johnson <[redacted]@waldenu.edu>

Thanks for your interest. You are welcome to use the NPI 16 for research. You can find more about the scale, including a sample scale and scoring instructions, here:

http://www.columbia.edu/~da358/npi16/

Good luck with your work.

Best regards,

Daniel

From: David Johnson <[redacted]@waldenu.edu>
Sent: Friday, August 5, 2016 4:17 PM
To: Ames, Daniel
Subject: Fwd: Request Permissions to Use Research Instrument (NPI-16)

Hello,

I am forwarding the below message to the slightly different e-mail address located on the [redacted] site.

If received in duplicate, please accept my apologies.

Thank you,
David Johnson

---------- Forwarded message ----------
From: **David Johnson** <[redacted]@waldenu.edu>
Date: Fri, Aug 5, 2016 at 4:14 PM
Subject: Request Permissions to Use Research Instrument (NPI-16)
To: [redacted]

Hello Dr. Ames,

My name is David Johnson and I am a doctoral student in Walden University's Information Technology program. I have studied your article titled "The NPI-16 as a short measure of narcissism" published in the Journal or Research in Personality. I would like to ask permission to use the NPI-16 instrument in my doctoral study.

Your measure fits well with my study as I would like to integrate this type of personality test into my research survey but would prefer a shorter measure than others as my study extends into Information Security questions as well. I believe my study will do well in adding to the body of knowledge regarding applying behavior sciences and concepts to study information security from the end-user perspective. Of course, I will gladly provide you the results of my study with permissions in exchange and provide proper citation of your work in my study.

Thank you in advance,

David P. Johnson

Student ID # [redacted]

Doctor of Information Technology

[redacted] (H)

[redacted] (C)

[redacted] - Eastern Time Zone

Gmail by Google

David Johnson <[redacted]@waldenu.edu>

Permissions Request to Use Research Instrument

2 messages

David Johnson <[redacted]@waldenu.edu> Wed, Oct 19, 2016 at 6:49 PM
To: [redacted]

Hello Dr. Workman,

My name is David Johnson and I am a doctoral student in Walden University's Information Technology program. I have studied your article titled "Security lapses and the omission of information security measures: A threat control model and empirical test" published 2008 in Computers in Human Behavior. I would like to ask permission to use questions from the study's measurement instrument in my doctoral study.

Your measurement instrument questions fit well with my study as I am applying the theory of planned behavior to an information security related subject. I believe my study will do well in adding to the body of knowledge regarding applying behavior sciences and concepts to study information security from the end-user perspective. Of course, I will gladly provide you the results of my study with permissions in exchange and provide proper citation of your work in my study.

Thank you in advance,

David P. Johnson

Student ID #[redacted]

Doctor of Information Technology

[redacted](H)

(C)

[redacted]- Eastern Time Zone

Mike Workman <[redacted] Fri, Oct 21, 2016 at 7:17 AM
Reply-To: [redacted]
To: [redacted] David Johnson <[redacted]@waldenu.edu>

Greetings David,

Of course, feel free to use the instrument. Thank you for note, and yes, I would be interested in your results.

Best Regards,
Mike Workman

[redacted]

Gmail by Google

David Johnson <[redacted]@waldenu.edu>

Permissions Request to Use Research Instrument

3 messages

David Johnson <[redacted]@waldenu.edu> Wed, Oct 19, 2016 at 6:56 PM
To: [redacted]

Hello Dr. Bommer,

My name is David Johnson and I am a doctoral student in Walden University's Information Technology program. I have studied your article titled "Security lapses and the omission of information security measures: A threat control model and empirical test" published 2008 in Computers in Human Behavior. I would like to ask permission to use questions from the study's measurement instrument in my doctoral study.

Your measurement instrument questions fit well with my study as I am applying the theory of planned behavior to an information security related subject. I believe my study will do well in adding to the body of knowledge regarding applying behavior sciences and concepts to study information security from the end-user perspective. Of course, I will gladly provide you the results of my study with permissions in exchange and provide proper citation of your work in my study.

Thank you in advance,

David P. Johnson

Student ID # [redacted]

Doctor of Information Technology

[redacted] (H)

(C)

[redacted] - Eastern Time Zone

Bill Bommer [redacted] Wed, Oct 19, 2016 at 7:11 PM
To: David Johnson <[redacted]@waldenu.edu>

David,
You are free to use anything published in that article.
Good luck with your research.
Thank you
Bill Bommer

[Quoted text hidden]

David Johnson <[redacted]@waldenu.edu> Wed, Oct 19, 2016 at 7:34 PM
To: Bill Bommer <[redacted]>

Hello Dr. Bommer,

Thank you for your permissions and quick reply.

David Johnson

Gmail by Google

David Johnson <[redacted]@waldenu.edu>

Permissions Request to Use Research Instrument

2 messages

David Johnson <[redacted]@waldenu.edu> Wed, Oct 19, 2016 at 7:00 PM
To: [redacted]

Hello Dr. Straub,

My name is David Johnson and I am a doctoral student in Walden University's Information Technology program. I have studied your article titled "Security lapses and the omission of information security measures: A threat control model and empirical test" published 2008 in Computers in Human Behavior. I would like to ask permission to use questions from the study's measurement instrument in my doctoral study.

Your measurement instrument questions fit well with my study as I am applying the theory of planned behavior to an information security related subject. I believe my study will do well in adding to the body of knowledge regarding applying behavior sciences and concepts to study information security from the end-user perspective. Of course, I will gladly provide you the results of my study with permissions in exchange and provide proper citation of your work in my study.

Thank you in advance,

David P. Johnson

Student ID # [redacted]

Doctor of Information Technology

[redacted] (H)

(C)

[redacted] - Eastern Time Zone

Detmar William Straub, Jr. <[redacted]> Thu, Oct 20, 2016 at 8:49 AM
To: David Johnson <[redacted]@waldenu.edu>

You have my permission to use the instrument. If it appeared in the article, then it becomes public anyhow.

Have you asked Mike Workman and Bill Bommer? Please ask them as well.

Detmar

Detmar W. Straub

[redacted]

Appendix B: Research Instrument Questions

Questions Measuring Attitude Construct

Attitude factor being measured: Organizational narcissism

Questions with an asterisk (*) denote narcissistic response.

1. When people compliment me I sometimes get embarrassed

   I know that I am good because everybody keeps telling me so*

2. I prefer to blend in with the crowd

   I like to be the center of attention*

3. I think I am a special person*

   I am no better nor worse than most people

4. I don’t mind following orders

   I like having authority over people*

5. I find it easy to manipulate people*

   I don’t like it when I find myself manipulating people

6. I insist upon getting the respect that is due me*

   I usually get the respect that I deserve

7. I am apt to show off if I get the chance*

   I try not to be a show off

8. Sometimes I am not sure of what I am doing

   I always know what I am doing*

9. Sometimes I tell good stories

   Everybody likes to hear my stories*

10. I like to do things for other people

    I expect a great deal from other people*

11. It makes me uncomfortable to be the center of attention

    I really like to be the center of attention*

12. Being an authority doesn't mean that much to me

    People always seem to recognize my authority*

13. I hope I am going to be successful

    I am going to be a great person*

14. I can make anybody believe anything I want them to*

    People sometimes believe what I tell them

15. There is a lot that I can learn from other people

    I am more capable than other people*

16. I am an extraordinary person*

    I am much like everybody else

    (Ames et al., 2006)

Attitude factor being measured: Perceived vulnerability

17. The likelihood of a computer or information security incident occurring to me is:

    Response choices: Unlikely, Somewhat unlikely, Neither likely nor unlikely, Somewhat likely, Likely (Cox, 2012)

Attitude factor being measured: Perceived severity

18. Threats to the security of my sensitive information at work are:

Response choices: Harmless, Somewhat harmless, Neither harmless nor severe, Somewhat severe, Severe (Cox, 2012)

Attitude factor being measured: Reward

19. Could you and/or your co-workers receive any potential rewards by not following the organization's computer and information security rules? (Cox, 2012; Posey et al., 2014; Siponen et al., 2014)

    Response choices: Unlikely, Somewhat unlikely, Neither likely nor unlikely, Somewhat likely, Likely

Questions Measuring Subjective Norm Construct

Subjective norm factor being measured: Normative beliefs

20. My co-workers follow the organization's computer and information security rules:

    Response choices: Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree (Cox, 2012)

21. Those important to me at work follow the organization's computer and information security rules:

    Response choices: Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree (Cox, 2012)

22. Those important to me at work think that I should follow the organization's computer and information security rules:

    Response choices: Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree (Cox, 2012)

Questions Measuring Perceived Behavioral Control Construct

Perceived behavioral control factor being measured: Locus of control

23. The primary responsibility for protecting my sensitive information at work belongs to:

    Response choices: My employer, Mostly my employer, Both myself and my Employer, Mostly myself, Myself (Cox, 2012)

Perceived behavioral control factor being measured: Self-efficacy

24. I have the necessary skills to protect myself from computer and information security violations:

    Response choices: Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree (Cox, 2012)

Questions Measuring Intention Dependent Variable

25. I intend to follow the organization's computer and information security rules:

    Response choices: Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree (Cox, 2012)

26. I try to follow the organization's computer and information security rules:

    Response choices: Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree (Cox, 2012)

27. In the future, I plan to follow the organization's computer and information security rules:

    Response choices: Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree (Cox, 2012)

Demographic/Qualification Questions

28. Are you currently employed in the role of principal, associate principal, or assistant principal?

    Response choices: Yes, No

29. Are you over the age of 18?

    Response choices: Yes, No

30. Please select your age category:

    Response choices: 24 years or younger, 25 to 34 years, 35 to 44 years, 45 to 54 years, 55 years or older

31. What is your gender?

    Response choices: Male, Female

32. How many years have you been with your current organization?

    Response choices: Less than 1 year, Between 1 and 5 years, Between 6 and 10 years, Between 11 and 15 years, More than 15 years

33. Do you use a computer for your job?

    Response choices: Yes, No

34. Does your organization have policies or procedures about computer security and protecting organizational information?

    Response choices: Yes, No, I don’t know

Appendix C: Organizational Permissions

[redacted]

December 6, 2016

David P. Johnson
[redacted]

Re: File ID [redacted]

Dear Mr. Johnson:

This is to advise you that your research application, "How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention," ID Number [redacted] has satisfactorily met [redacted] Research Standards and was approved by the Institutional Review Board. This approval is valid beginning December 6, 2016 through January 31, 2017. Please note the following comments regarding your study:

- The proposed study is well-grounded in theory and takes a pragmatic approach to testing theory within the [redacted] professional community, which is entrusted with a substantial array of sensitive digital information and vulnerable information systems.

Please note the following requirements of you as a researcher in [redacted]

- A copy of this approval letter must be attached to any initial communication with a [redacted] school or office.
- The above File ID number must be included in the subject line of any communication with a [redacted] school or district office concerning this research study.
- If circumstances prevent you <u>and every member of your research team</u> from following these requirements, please let me know so that we can make alternative arrangements.

Note that schools and teachers may elect not to participate in your research study, even though the district has granted permission.

Please forward a copy of your results to me when they are completed.

Best wishes for a successful research project. Please call me at [redacted] if I may be of further assistance.

Sincerely,

[redacted]

[redacted] Executive Director
Research and Evaluation

cc: Dr. Timothy Perez, [redacted]@waldenu.edu
David P. Johnson, [redacted]

Appendix D: Reference Counts by Year and Source

Table D1

Reference Counts for Literature Review

Year	Source	Count
2017		
	Peer-reviewed journal	1
2016		
	Peer-reviewed journal	24
2015		
	Peer-reviewed journal	30
	Conference proceeding	2
	Government publication	1
	Industry report	2
2014		
	Peer-reviewed journal	38
	Conference proceeding	2
2013		
	Peer-reviewed journal	37
	Non peer review journal	2
	Industry report	1
2012		
	Peer-reviewed journal	6
2009		
	Peer-reviewed journal	1
2008		
	Peer-reviewed journal	1
2007		
	Peer-reviewed journal	1
2003		
	Government publication	1
2002		
	Peer-reviewed journal	1
2001		
	Peer-reviewed journal	2
1991		
	Peer-reviewed journal	2
1985		
	Book	1
1975		
	Book	1

Table D2

Reference Counts for Complete Study

Year	Source	Count
2017		
	Peer-reviewed journal	13
	Book	1
2016		
	Peer-reviewed journal	38
	Book	1
	Industry report	1
2015		
	Peer-reviewed journal	48
	Non-peer review journal	1
	Conference proceeding	2
	Government publication	2
	Industry report	3
	Software	1
2014		
	Peer-reviewed journal	72
	Conference proceeding	2
	Industry report	1
	Non-peer review journal	1
	Book	1
2013		
	Peer-reviewed journal	66
	Non-peer review journal	2
	Industry report	1
	Government publication	1
2012		
	Peer-reviewed journal	8
2011		
	Peer-reviewed journal	1
2009		
	Peer-reviewed journal	2
2008		
	Peer-reviewed journal	1
2007		
	Peer-reviewed journal	1
2006		
	Peer-reviewed journal	1

(table continues)

Year	Source	Count
2003		
	Government publication	1
	Peer-reviewed journal	1
2002		
	Peer-reviewed journal	1
2001		
	Peer-reviewed journal	2
2000		
	Peer-reviewed journal	1
1991		
	Peer-reviewed journal	2
1987		
	Peer-reviewed journal	2
1985		
	Book	1
1979		
	Peer-reviewed journal	1
1975		
	Book	1