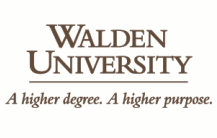

2019

Factors Affecting Employee Intentions to Comply With Password Policies

Ernest Tamanji Anye
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Ernest Anye

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. Christos Makrigeorgis, Committee Chairperson, Information Technology Faculty
Dr. Steven Case, Committee Member, Information Technology Faculty
Dr. Gail Miles, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2019

Abstract

Factors Affecting Employee Intentions to Comply With Password Policies

by

Ernest T. Anye

MIT, Walden University, 2017

MS, Northwestern State University, 2010

BS, Grambling State University, 2003

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2019

Abstract

Password policy compliance is a vital component of organizational information security. Although many organizations make substantial investments in information security, employee-related security breaches are prevalent, with many breaches being caused by negative password behavior such as password sharing and the use of weak passwords. The purpose of this quantitative correlational study was to examine the relationship between employees' attitudes towards password policies, information security awareness, password self-efficacy, and employee intentions to comply with password policies. This study was grounded in the theory of planned behavior and social cognitive theory. A cross-sectional survey was administered online to a random sample of 187 employees selected from a pool of qualified Qualtrics panel members. Participants worked for organizations in the United States and were aware of the password policies in their own organizations. The collected data were analyzed using 3 ordinal logistic regression models, each representing a specific measure of employees' compliance intentions. Attitudes towards policies and password self-efficacy were significant predictors of employees' intentions to comply with password policies (odds ratios ≥ 1.257, $p < .05$), while information security awareness did not have a significant impact on compliance intentions. With more knowledge of the controllable predictive factors affecting compliance, information security managers may be able to improve password policy compliance and reduce economic loss due to related security breaches. An implication of this study for positive social change is that a reduction in security breaches may promote more public confidence in organizational information systems.

Factors Affecting Employee Intentions to Comply With Password Policies

by

Ernest T. Anye

MIT, Walden University, 2017

MS, Northwestern State University, 2010

BS, Grambling State University, 2003

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2019

Dedication

This doctoral study is dedicated first to God, who sustains me, gives me strength, and gives me purpose in life's journey. And to my family for their steadfast support throughout my doctoral study. Without them, this accomplishment would not be possible.

Acknowledgments

I give special thanks to my chair, Dr. Christos Makrigeorgis, for his mentorship and support throughout the doctoral study process. His encouragement and guidance made it possible for me to complete this study. Also, I would like to say thank you to my committee members, Dr. Steven Case and Dr. Gail Miles, for their invaluable guidance and input throughout this process. Their comments and feedback strengthened my doctoral study. I would like to acknowledge my parents, Daniel Anye and Esther Anye, for their support and inspiration all through this process. Thank you to my wife, Emeline Anye, and our daughters, Sarah, Rebecca-Grace, and Abigail, for their patience and encouragement. Finally, thank you to my siblings and my church family, who were a constant source of strength and support.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Threats to the confidentiality, integrity, and availability of information are a concern to organizations of all sizes (Jouini, Rabai, & Aissa, 2014). Due to such threats, organizations continue to invest in technical information security controls such as firewalls and intrusion detection systems (Hwang et al., 2017). However, such necessary investments and controls are not sufficient in addressing threats associated with authorized users, such as employees' risky usage behaviors (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014). Risky behaviors are varied and include how employees handle their passwords or how they use network resources (Guo, 2013). In addition to technical controls safeguarding against risky user behavior, organizations also rely on the application of information security policies to protect their information systems (Lebek et al., 2014). In this study, I examined the factors that affect employee compliance with information system security policies. A better understanding of such factors may help IT leaders and policy makers to design more effective information security policies.

Background of the Problem

Information system security is becoming a priority for many organizations as the number of detected security incidents continues to rise (Hull, 2015; Udo, Bagchi, & Kirs, 2018). User authentication can be the first line of defense against security breaches (Ranjan & Om, 2016). The use of passwords remains the most common form of authentication (Zhao & Luo, 2017); many organizations rely on passwords as a simple, inexpensive method of employee authentication (Zheng, Cheng, Zhang, Zhao, & Wang, 2018). Although password policies may be implemented in part using technological

methods, employees still play a significant role in the implementation of such policies. For example, employees are often expected to create complex passwords, memorize passwords for multiple accounts, and change passwords frequently. As such, many security breaches involve negligence by current employees (Elifoglu, Abel, & Tasseven, 2018; Opderbeck, 2016). Such neglect and lack of employee compliance may cause information security policies to become inadequate (Lowry & Moody, 2015). Mandatory tightening of policies to increase compliance may have unexpected side effects or may be entirely counterproductive (Guo & Zhang, 2017). It is therefore crucial that IT leaders and policy makers gain a better understanding of policy compliance behavior from the perspective of employees. The focus of this study was on examining the factors that affect employees' intentions to comply with organizational password policies.

Problem Statement

Information security policy compliance is a key component of organizational information security with users often being the weakest link in information system security (Ifinedo, 2016). In a survey conducted in 2016, more than 50% of participating organizations reported credential-based attacks as being the most severe attacks they experienced (U.S. Government Accountability Office, 2016, p. 14). Furthermore, the authors of a password security survey found that 17% of users wrote down their passwords, 20% shared their passwords, and 53% reused their passwords (Solic, Ocevcic, & Blazevic, 2015). The general IT problem is that even though most medium-sized companies have clear IT compliance guidelines, employees' behavioral motivations related to policy compliance with such guidelines need to be better understood. The

specific IT problem is that some information technology leaders lack knowledge of the relationship between employees' attitudes towards password policy, information security awareness, and password self-efficacy, and employee intentions to comply with password policies.

Purpose Statement

The purpose of this quantitative correlational design study was to quantify the relationship between employees' attitudes towards password policies, information security awareness, and password self-efficacy, and employee intentions to comply with password policies. The independent variables were employees' (a) attitudes towards password policies, (b) information security awareness, and (c) password self-efficacy. The dependent variables were employees' overall intentions to comply with password policies, intentions to comply by protecting information and technology resource according to the password policy, and intention to comply by carrying out their responsibilities prescribed in the password policy. I mapped composite scores from survey items to the three independent latent variables. Regarding participants, I selected a representative sample of employees who work for organizations in the United States which have an information security password policy. I focused on employees who work in organizations which have a password policy. This study may contribute to positive social change, as findings from the study could lead to a reduction in the likelihood of security breaches, and an increase in the integrity of customers' personally identifiable information. A potential reduction in security breaches could promote customers'

confidence in enterprise information systems, reduce revenue loss due to identity theft, and enhance customer satisfaction.

Nature of the Study

I used a quantitative, correlational design for this study. Quantitative methods are appropriate when a researcher collects numeric data and compares relationships between variables (Claydon, 2015). In this study I focused on assessing the relationship between several independent latent or composite continuous variables and a dependent or continuous outcome variable, so a quantitative approach was appropriate. I considered but opted against using a qualitative approach. Researchers use qualitative methods in studies in which they seek to describe a phenomenon or achieve a deeper understanding of an issue, using descriptive data that is non numeric (Jervis & Drake, 2014). Because I did not seek to explore or identify the factors affecting password compliance, as the factors have already been identified in the literature (Mwagwabi, McGill, & Dixon, 2014; Safa et al., 2015), I concluded that a qualitative paradigm was not appropriate for this study. A mixed methodology study involves the analysis of a combination of qualitative and quantitative data to solve problems in which one data source may be insufficient (Gibson, 2017). As discussed, this study did not include a qualitative component, so a mixed-methods approach was not suitable.

Quantitative research designs include descriptive, correlational, and experimental designs (Ingham-Broomfield, 2014). A researcher would use a descriptive design when the focus of a study is to describe the characteristics of variables without investigating relationships between the variables (Ingham-Broomfield, 2014). In this study I examined

the relationships between variables, so a descriptive design was not suitable. An experimental design was also not applicable to this study. An experimental design is used when a research endeavor involves the manipulation of the conditions of variables or participants (Cho et al., 2016). Researchers also use experimental designs to make causal inferences between independent and dependent variables (Vargas, Duff, & Faber, 2017). This study did not involve manipulation of the study variables or causal inference between variables, but rather an examination of the relationships between variables. I chose a correlational design because of its ability to answer the research questions, which concerned the magnitude of associations between non manipulated variables. I examined the ability of several latent predictor variables to determine employees' intentions to comply with security policies. Data were collected with a survey instrument.

Research Question

What is the relationship between employees' attitudes towards information system password policies, employees' security awareness, employees' password self-efficacy, and employees' intentions to comply with password policies?

Hypotheses

I operationalized the research question into the following testable statistical hypotheses.

$H_0$1: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' overall intentions to comply with password policies.

$H_1$1: There is a statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' overall intentions to comply with password policies.

$H_0$2: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply by protecting information and technology resources according to the password policy.

$H_1$2: There is a statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply by protecting information and technology resources according to the password policy.

$H_0$3: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply by carrying out their responsibilities as prescribed in the password policy.

$H_1$3: There is a statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply by carrying out their responsibilities as prescribed in the password policy.

Theoretical Framework

In this study, I used three composite independent variables to predict one composite dependent variable. All variables were latent or composite, implying that they were not directly observable or measured but instead represented a complex construct composed of various variables (Bartolucci, Bacci, & Mira, 2018). A theoretical framework was provided to support each of these constructs. The first independent variable was attitudes towards password policies, and the second independent variable was information security awareness. The dependent variable was intention to comply with password policies. These three variables were based on the theory of planned behavior (TPB). The last independent variable was password self-efficacy and was based on social cognitive theory (SCT). Table 1 shows the constructs and their underpinning theoretical frameworks.

Table 1

Constructs and Their Corresponding Theoretical Frameworks

Construct	Theoretical framework
Attitudes towards password policies	Theory of planned behavior
Information security awareness	Theory of planned behavior
Password self-efficacy	Social cognitive theory
Intentions to comply with password policies	Theory of planned behavior

Ajzen (1991) developed TPB. The TPB is a derivative of the theory of reasoned action by Fishbein and Ajzen (1975). The TPB suggests that the performance of a

behavior can be predicted by intentions to perform the behavior and perceived behavioral control (Ajzen, 1991). This theory further postulates that there are three determinants of intention: attitude towards behavior, subjective norm, and perceived behavioral control. Attitude towards the behavior refers to the level to which a person appraises a behavior as favorable or unfavorable (Ajzen, 1991). Subjective norm has to do with the perceived social pressure to perform the behavior. Perceived behavioral control refers to what people view as the level of ease or difficulty in performing a behavior (Ajzen, 1991). In general, as attitude becomes more positive and subjective norms and perceived behavioral control become greater, the intention to perform a behavior becomes stronger (Ajzen, 1991). Applying TPB to this study, employees' intention to comply with password policies can be predicted by their attitudes towards policy compliance, and attitudes towards compliance can be influenced by information security awareness as a background factor. Ajzen also suggested that based on SCT, self-efficacy towards a behavior may play a role in intention to perform the behavior. Bandura (1986) presented the concept of self-efficacy in his SCT. Bandura described self-efficacy beliefs as "people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances" (p. 391). Bandura suggested that how people behave is influenced by their beliefs about their capabilities. In the context of this study, employees' intentions to comply with password policies may be affected by their beliefs in their abilities to comply with policies.

Definition of Terms

Information security: Information security involves the safeguarding of information and information systems from unauthorized access, disclosure, use, modification, disruption or destruction to preserve the confidentiality, integrity, and availability of information (Da Veiga & Martins, 2015).

Information security awareness: Information security awareness can be described in terms of an employee's general knowledge about information security and his or her organization's information security policy (Bulgurcu, Cavusoglu, & Benbasat, 2010).

Information security policy: An information security policy is a set of directives that outlines expectations with regards to information security and consequences for not meeting the expectations (Karlsson, Hedström, & GoldKuhl, 2017; Niemimaa & Niemimaa, 2017).

Self-efficacy: Self-efficacy is an individual's perceptions of his or her capabilities or an individual's judgment of his or her ability to successfully perform a task (Hwang, Lee, & Shin, 2016).

Assumptions, Limitations, and Delimitations

Assumptions can be viewed as beliefs about proposed research that are necessary to conduct the research, but cannot be proven (Casson & Farmer, 2014; Scherdin & Zander, 2014; Yang, Liang, & Avgeriou, 2017). Tavakol and Sandars (2014) described assumptions as norms in a study that researchers take for granted or accept without verification. Limitations are issues or shortcomings that may arise in a study which are beyond the researcher's control (Helmich, Boerebach, Arah, & Lingard, 2015).

Delimitations are factors controlled by the researcher, but which the researcher chooses to bound, that may affect a study (Ellis & Levy, 2009). Delimitations may affect a study's generalizability and applicability but are often needed to delineate the scope of the study (Ellis & Levy, 2009).

Assumptions

Researchers typically stipulate assumptions regarding several elements of a study. These include (a) the phenomenon being studied, (b) the theory being investigated, (c) the participants, (d) the instrument used for data collection, (e) the study methodology, (f) the data analysis, (g) the power to find significance, and (h) the results of the study (Dusick, 2015). In this study, I made assumptions regarding the theoretical framework, the participants, and the study methodology.

I based the theoretical framework for this study on TPB and SCT. A tenet of TPB is that perceptions towards behavior and subjective norms are related to intentions to perform the behavior (Ajzen, 1991); SCT suggests a relationship between self-efficacy and behavioral intentions (Bandura, 1986). Drawing from TPB, I assumed that employees' information security awareness and perceptions of password policies affect their intentions to comply with password policies. Drawing from SCT, I assumed a relationship between self-efficacy and behavioral intentions.

With regards to the participants, I assumed that each participant was indeed an employee in an organization in which there is an information security policy, and this condition was one of the selection criteria. Secondly, I assumed that participants had the necessary knowledge and qualifications to answer the survey questions and that they

responded honestly and accurately. Concerning the study methodology, the assumption was that the cross-sectional survey design methodology selected would cogently address the problem under study. A quantitative survey design was deemed the most appropriate for this study, as such a design is useful when exploring the relationships between variables (Claydon, 2015).

Limitations

Similarly, researchers state limitations regarding (a) the phenomenon being studied, (b) the theory being investigated, (c) the participants, (d) the instrument used for data collection, (e) the study methodology, (f) the data analysis, (g) the power to find significance, and (h) the results of the study (Dusick, 2015). For this study, the principal limitations included the instrument, the study methodology, and the power to find significance.

The ability of the survey instrument to measure the central constructs in the research question could limit the accuracy of the findings of this study. Even though the survey instrument has demonstrated reliability and validity (Bulgurcu et al., 2010), the extent to which the survey could address the research questions may have limited the study results. I used an existing survey instrument in this study. The use of an existing instrument was favored over the development of a new survey instrument due to constraints in time and resources associated with completing a doctoral study.

Another possible limitation was related to the study methodology. One key pillar of cross-sectional research is that the sample must accurately represent the population so that the analysis of the sample can be used to infer the characteristics of the population.

The limitation with such one-time snapshot samples is that they do not consider the effects of additional exposures on the subjects over time. A longitudinal methodology may overcome this limitation. However, a longitudinal methodology was not feasible for this study due to time constraints.

The choice of a statistical test can affect the outcome of a study. An essential characteristic of statistical tests is the power to find significance, or the power to detect correlations or differences between variables. The results of this study could be limited by the power of the regression analyses to discover significant relationships between the study variables. The power of a statistical test is affected by the sample size. As a measure to minimize the limitation of the power to find significance in this study, analysis was made to determine a sample size which favors higher test power.

Delimitations

Delimitations are constraints in a study that are anticipated by the researcher and that influence the interpretation of study results (Sampson et al., 2014). Delimitations help to demarcate the parameters of a study. The identification of delimitations should be informed by the research questions and purpose (Newman, Hitchcock, & Newman, 2015). A researcher can control delimitations, as they are chosen by the researcher to limit the scope of a study (Soilkki, Cassim, & Anis, 2014).

Participants in this study were limited to employees who work in an organization that has an information security policy. The study population was limited to employees because they pose a significant threat to organizational information security. Although many organizations have well-defined information security policies in place, compliance

with such policies is often lacking (Bulgurcu et al., 2010; Elifoglu et al., 2018). The study was also limited geographically to organizations in the United States, to maintain a reasonable scope for the research.

Another delimitation of this study is that the dependent variable assessed employees' intentions to comply with password policies, rather than actual compliance. Although it may be possible to measure actual compliance through approaches such as participant observation (Dahlke, Hall, & Phinney, 2015), this study did not include such a design. The extant literature supported this choice. Several researchers assessed employees' intentions to comply with information security policies (Guo & Zhang, 2017; Lowry & Moody, 2015). Furthermore, Bulgurcu et al., (2010) showed a positive relationship between intentions to comply and actual compliance.

Significance of the Study

Contribution to Information Technology Practice

As the number of security breaches experienced by organizations continues to increase (Hull, 2015), information security management has become a top area of concern (Bulgurcu et al., 2010). Many security breaches have originated from employees through unintentional negligence or malicious intent to steal insider information for personal gain (Opderbeck, 2016). This study captured both aspects in regression models that assessed the significance of perceptions of employees towards password policies, information security awareness, and password self-efficacy, and how they affect employees' intentions to comply with password policies. The use of regression models to capture these composite variables enabled an examination of the contribution of each unit

of each variable towards employees' intention to comply. Knowledge gained from this study may help employers to focus on the most impactful variables as they seek ways to promote policy compliance with password security policies.

Implications for Social Change

Results from the current study may have a significant economic and social impact. The security of information systems in enterprise environments is of vital importance because of the possible economic ramifications of security breaches in such settings. A better understanding of factors that affect information security policy compliance may help reduce noncompliance, and thus increasing the security and integrity of information systems in enterprise environments. Safeguarding enterprise information systems may also help prevent financial loss in the form of identity theft or theft of data assets. In the area of social change, the prevention of security breaches related to employee noncompliance with policies may promote public confidence in enterprise information systems. Furthermore, a reduction in security breaches will also enhance the integrity of customers' sensitive personal information. Results from this study will also be valuable to information security policy designers by providing them with knowledge of determinants of employee compliance, enabling them to design better policies.

A Review of the Professional and Academic Literature

The purpose of this quantitative correlational design study was to examine the relationship between employees' attitudes towards password policy, information security awareness, and password self-efficacy, and employee intentions to comply with password

policies. The use of passwords is a simple, inexpensive method of user authentication (Zhao & Luo, 2017; Zheng et al., 2018). Employees play an important role in the implementation of password policies and other information security measures in an organization (Lowry & Moody, 2015). For example, employees are often expected to create complex passwords, memorize passwords for multiple accounts, and change passwords frequently. In this study I focused on the factors that affect employees' intentions to comply with password policies.

The goal of this literature review was to provide background information for my study by examining published information on the core concepts of the study. I have divided the literature review into five central subsections:

- review of underlying theories,
- causes of information security breaches,
- information security policy compliance,
- factors affecting policy compliance, and
- applications of linear regression.

In Subsection 1, I provide a comprehensive review of the underlying theories for this study. This subsection also includes a discussion of some competing theories applicable to information security behavior. Subsection 2 focuses on the causes of information security breaches. I examine the role of factors internal to organizations, as well as external causes. For internal causes, a distinction is made between intentional and unintentional actions of employees that may result in security breaches. In the third subsection I focus on information security policy compliance and how it affects the

overall information security of an organization. For the fourth subsection, I examine the factors that influence policy compliance. I reviewed both intrinsic and extrinsic factors. Subsection 5 focuses on regression analyses and its application in determining relationships between variables.

I searched several sources for peer-reviewed articles, books, dissertations, and web pages relevant to the study. The primary resource portal searched was the Walden University Library, and included databases such as Business Source Complete, ProQuest, EBSCOhost, IEEE Xplore Digital Library, Academic Search Complete, and Computers & Applied Sciences Complete. Also, I searched Google Scholar for peer-reviewed articles, books, and relevant web pages. The following search terms were used: *information security policies*, *employee compliance*, *security awareness*, *self-efficacy*, *security breach*, *data breach*, *security compliance*, *security policy violation*, *employee compliance*, *password policy*, *password authentication*, *user authentication*, and *access control.* I included a total of 99 articles in the literature review. Of these, 94% were peer-reviewed articles and 88% were 5 years old or less. Table 2 shows a summary of the references used in the literature review.

Table 2

Characteristics of the Literature Review References

	Literature review		All references	
Reference status	Count	Percentage	Count	Percentage
Peer-reviewed	93	93%	200	95%
Non-peer-reviewed	4	4.0%	8	3.7%
Books	3	3.0%	3	1.4%
Web pages	0	0%	2	0.9%
Other	0	0%	1	0.5%
Total	100	100%	214	100%
Reference age	Count	Percentage	Count	Percentage
5 years old or less	87	87%	197	92.5%
More than 5 years old	13	13%	16	7.5%
Total	100	100%	214	100%

Review of Underlying Theories

Two key theories underpinned the research framework for this study: the TPB, which stipulates that behavioral intention can be predicted by an individual's attitude towards the behavior, perceived behavioral control, and subjective norm (Ajzen, 1991), and SCT, which suggests that self-efficacy is a principal determinant of human action (Bandura, 1989). In this section, I discuss these theories as well as some other competing theories applicable to information security behavior.

Theory of planned behavior. Ajzen (1991) developed TPB based on the theory of reasoned action (Fishbein & Ajzen, 1975), which he extended to explain human

behavior in certain contexts. Ajzen proposed TPB in his article "From Intentions to Actions: A Theory of Planned Behavior." A central focus of the TPB is explaining people's intentions to perform certain behaviors. Intentions refer to motivations that influence behavior and indicate how much effort people are willing to put into performing a specific behavior (Ajzen, 1991). In general, a strong intention to perform a behavior should correlate with a higher likelihood of performing the behavior (Ajzen, 1991). However, a behavioral intention can be translated into an actual performance of the behavior only if the person can decide at will whether to perform the behavior or not (Ajzen, 1991). In addition to intention and volitional control, the performance of a behavior also depends on the availability of resources such as the ability to perform the behavior or cooperation of others (Ajzen, 1991).

The TPB postulates that three factors determine an individual's intention to perform a behavior: the attitude towards the behavior, subjective norms, and perceived behavioral control. Figure 1 shows the constructs of the TPB.

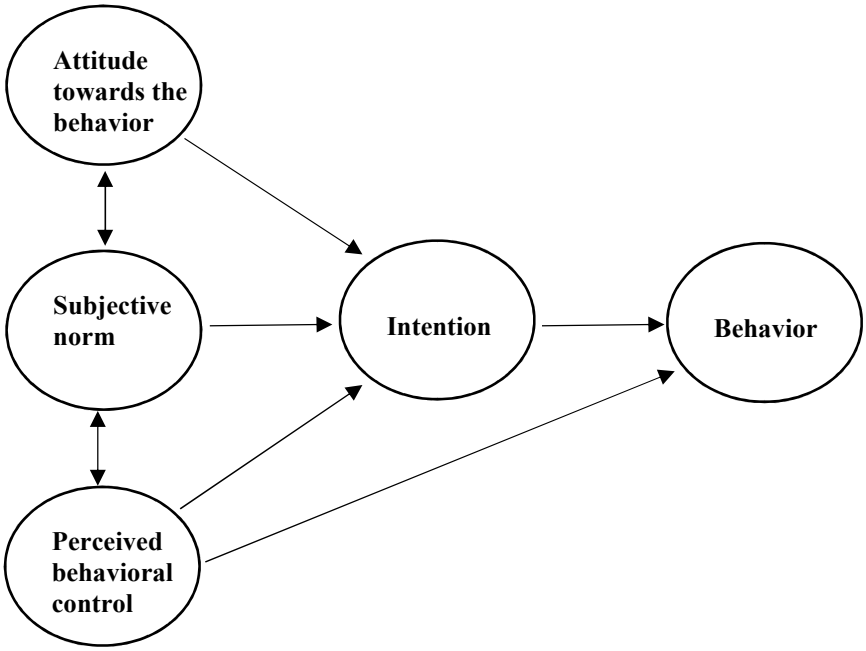

Figure 1. Constructs of the theory of planned behavior.

Attitude towards a behavior refers to an individual's appraisal of a behavior or the extent to which someone evaluates a behavior as favorable or unfavorable. Ajzen (1991) suggests that attitudes towards a behavior are shaped by information about the behavior or beliefs about the behavior. Similarly, normative beliefs are the determinants of subjective norms. Subjective norm has to do with an individual's perception of social pressure to perform or not to perform a behavior (Ajzen, 1991). Perceived behavioral control refers to the level to which an individual sees a specific behavior as easy or difficult to perform (Ajzen, 1991). Perceived behavioral control is assumed to be affected by experience as well as anticipated obstacles to completing the behavior (Ajzen, 1991). The concept of perceived behavioral control is compatible with the concept of perceived self-efficacy put forth by Bandura (1989). Perceived behavioral control distinguishes the

TPB from the theory of reasoned action, which explains behavioral intention in terms of attitude towards behavior and subjective norm only (Ajzen, 1991).

The TPB proposes that perceived behavioral control can also be used directly to predict actual behavior. Ajzen (1991) argued that increased behavioral control can be associated with a greater likelihood of more effort to be put towards accomplishing a behavior. According to Ajzen, an individual who has high confidence in his or her ability to perform a task will persevere more than an individual who is doubtful of his or her abilities. Second, Ajzen asserted that perceived behavioral control can be used as a measure of actual behavioral control, which in turn can be used to predict actual behavior. Such an estimation of behavioral control is dependent on the accuracy of the perceptions (Ajzen, 1991).

In addition to the three central constructs in the TPB, other factors may interact with the main factors to affect behavioral intention. According to the TPB, the three factors discussed in this subsection (attitude towards behavior, subjective norm, and perceived behavioral control) may not be the only factors affecting behavior (Ajzen & Albarracin, 2007). In addition to these factors, other background factors may influence behavior indirectly. Background factors include factors which differ among individuals, such as experience, demographics, disposition, or knowledge (Ajzen & Albarracin, 2007). Background factors can affect behavioral intention indirectly by shaping behavioral, normative, and control beliefs (Ajzen & Albarracin, 2007). The TPB explains behavior in terms of attitudes, subjective norms, and behavioral control, as well as other background factors that may play an indirect role.

Researchers have used the TPB as a theoretical framework in several studies in the behavioral sciences (see Beville et al., 2014; Chan, Ng, & Prendergast, 2014; Tipton, 2014). Chan et al. (2014) used the TPB to investigate healthy eating intentions in male and female adolescents. The authors examined how TPB factors such as attitude, self-efficacy, perceived barriers, and perceived behavioral control could predict intention to practice healthy eating (Chan et al., 2014). Chan et al. used a questionnaire to collect data from a probability sample of 544 adolescents and performed correlational and factor analysis. Results from the study showed a significant difference in healthy eating intentions and attitude between girls and boys, with girls showing a more positive attitude and greater intentions towards healthy eating (Chan et al., 2014). TPB factors accounted for 51% of the variance for healthy eating intentions in boys and 45% of the variance in girls (Chan et al., 2014).

In another study, Tipton (2014) used the TPB to address the issue of childhood obesity in non-Hispanic Black preschoolers. The authors analyzed the contributions of caregivers' attitudes towards serving sweetened beverages to the preschoolers, subjective norms, and perceived behavioral control to the variance in caregivers' serving intentions (Tipton, 2014). Caregivers' attitudes towards serving and subjective norms were significant predictors of their intentions to serve sweetened beverages to preschoolers, while perceived behavioral control had no significant contribution (Tipton, 2014). Similarly, Beville et al. (2014) reported that the TPB was able to explain 42.5% of the variance in female students' intentions and participation in leisure-time physical activity.

Social cognitive theory. Bandura (1989) developed SCT. According to SCT, determinants of human action include self-generated factors (Bandura, 1989). Bandura suggested that personal factors such as cognitive and affective factors interact with environmental factors in determining human behavior. The central construct in SCT is self-efficacy. Self-efficacy refers to an individual's beliefs in his or her capabilities. People's self-efficacy beliefs influence their ability to put effort into accomplishing a task, and their ability to persevere and overcome obstacles (Bandura, 1989). Bandura asserted that self-efficacy affects an individual's actions mediated by motivational, cognitive, and affective processes. Self-efficacy beliefs determine an individual's level of motivation (Bandura, 1989). Conversely, self-doubt causes people to reduce their efforts or settle for less ideal outcomes (Bandura, 1989).

Self-efficacy affects cognitive processes by influencing the self-appraisal of capabilities (Bandura, 1989). People who have a high self-appraisal of their problem-solving skills visualize positive results of their actions, and such a cognitive state enhances positive performance (Bandura, 1989). Self-efficacy impacts affective processes, as belief in one's capability affects one's level of motivation, stress in challenging situations, and depression (Bandura, 1989). Individuals with high self-efficacy view themselves as capable of coping with stressful situations. Bandura (1989) also suggests that in risky situations, people act based on their perceptions of their coping efficacy. SCT, therefore, indicates that people's behavior could be affected by their self-efficacy. The effect of self-efficacy could be manifested through a person's choice of

activities, the way he or she prepares for the activity, or the level of motivation and effort exerted during the activity (Bandura, 1989).

I based the current study on the TPB and SCT. I adopted two constructs of the TPB: attitudes towards behavior and perceived behavioral control (or self-efficacy to behave). In addition, I examined information security awareness as a background factor that may influence password policy behavior. This approach is consistent with the view of Ajzen and Albarracin (2007) that background factors may play a role in predicting behavioral intention and behavior in the TPB. Also, individual differences and affective factors can exert an influence on the components of the TPB (Conner, McEachan, Taylor, O'Hara, & Lawton, 2015). Furthermore, Bulgurcu et al. (2010) found that information security awareness significantly influenced attitude towards compliance, acting as a background factor in the TPB. I drew the construct of self-efficacy from SCT. According to Ajzen (1991), perceived behavioral control in the TPB is compatible with Bandura's (1989) self-efficacy variable, as both variables measure the same element of human behavior. Figure 2 shows the constructs and underlying theories that support the study.

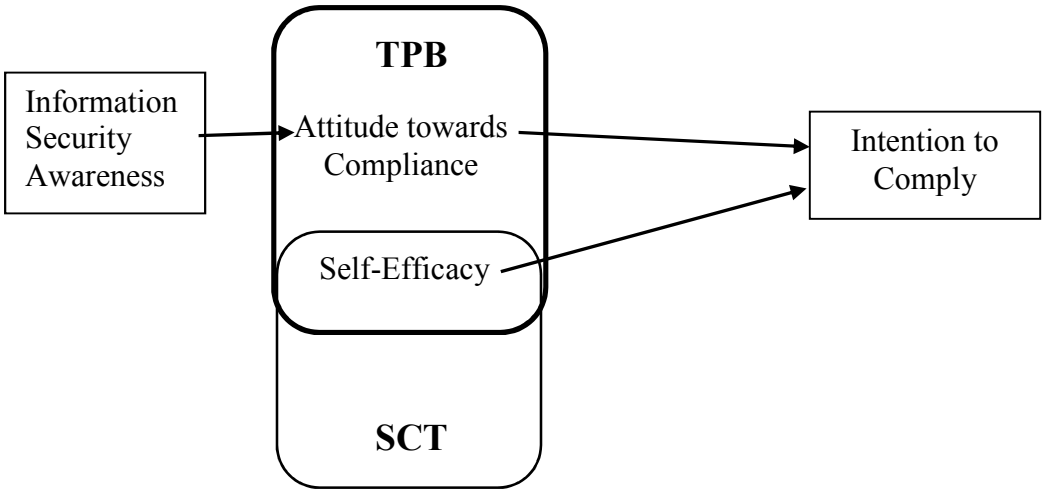

Figure 2. Study constructs and theories.

Competing theories. Researchers used several other theories in the extant literature to predict user intentions to comply with information security policies. In the next section, I discuss three of the other commonly used theories in behavioral information security: protection motivation theory, general deterrence theory, and the technology acceptance model.

Protection motivation theory. Rogers (1975) proposed the protection motivation theory. Protection motivation theory provides a set of important stimulus variables which interplay in fear appeal and explains the cognitive processes which mediate an individual's acceptance of suggested sets of actions or recommendations in a fear appeal scenario (Rogers, 1975). Fear appeal refers to the contents of communications which describe unfavorable consequences that may occur if a specific set of recommendations are not followed (Rogers, 1975). According to protection motivation theory, there are three stimuli variables in a fear appeal: the level of noxiousness of a specific event, the

probability that the given event will occur, and the effectiveness of a coping response that may counter the noxious stimulus. Rogers suggested that the three variables in a fear appeal initiates cognitive processes, and these processes are used to evaluate communicated information regarding noxiousness, the probability of occurrence, and efficacy of the coping responses to the event (Rogers, 1975). The theory assumes that the cognitive processes appraising a fear appeal are responses to environmental stimuli which have been received and understood by the individual processing the fear appeal. Rogers suggests that the cognitive processes affect an individual's attitude by arousing a protection motivation, and the amount of resultant protection motivation will determine the intention of the individual to comply with communicated recommendations. In sum, the protection motivation theory postulates that protection motivation stems from the assessment of an event as unpleasant and likely to occur and the belief that responding with recommended coping actions may prevent the event from happening.

Herath and Rao (2009) applied the protection motivation theory to information security behavior. In this context, security threats can be considered the noxious event, and security policies are the recommended coping mechanisms to deal with the threat. Individuals may find security policies useful or relevant based on their beliefs of how effective the policies are as a coping mechanism against security threats (Herath & Rao, 2009). Results from their study suggested that employees' perceptions about the severity of a security breach, response efficacy, and self-efficacy had a positive effect on their attitudes towards compliance with information security policies (Herath & Rao, 2009).

Although the protection motivation theory has been used to explore behavioral change in information security (Hanus & Wu, 2016; Menard, Bott, & Crossler, 2017; Tsai et al., 2016), I did not adopt this theory in the current study. The protection motivation theory focuses on attitude change based on fear appeal and explores a limited set of components and cognitive processes that may affect persuasion (Rogers, 1975). This theory was therefore not suitable for the current study, which explored a broader set of factors that affect password policy compliance intentions.

General deterrence theory. The general deterrence theory was put forth by Nagin & Pogarsky (2001) and applied in the field of criminology. The general deterrence theory seeks to explain the effectiveness of punishment certainty, punishment severity and punishment celerity as deterrents of criminal behavior. Nagin & Pogarsky postulate that in general, an individual will offend if the benefits gained from the offense are higher than the cost of the crime and the perceived risk of being sanctioned. In other words, an individual's offense probability is affected by the certainty and severity of sanctions. Furthermore, an individual's intention to offend is also affected by the swiftness of the sanctions (Nagin & Pogarsky, 2001). However, the effect of sanction celerity depends on whether the offender prefers a delay in sanction (Nagin & Pogarsky, 2001).

In the context of information security compliance behavior, the general deterrence theory suggests that an individual's intention to violate information security policies will be affected by the certainty and severity of sanctions (Cheng, Li, Li, Holm, & Zhai, 2013). Based on the general deterrence theory, sanctions may serve as an essential means of deterrence for information security policy violation. Cheng et al. (2013) examined the

applicability of the general deterrence theory to information security policy compliance. Results from their study indicated that employees' intentions to violate information security policies were affected significantly by the severity of sanctions, while the certainty of sanctions had no significant effect. These results differed from findings by Johnston, Warkentin, McBride & Carter (2016) who reported that both the severity of sanctions and certainty of sanctions were significant predictors of employees' policy violation intentions. I chose not to base the current study on the general deterrence theory because of its focus solely on factors external to the individual (sanctions) in predicting behavioral intention.

Technology acceptance model. The technology acceptance model was put forth by Davis (1989) to predict and explain the use of technology systems. The primary constructs in this model are perceived usefulness and perceived ease of use, two fundamental determinants of system use according to the model. Perceived usefulness is a measure of the extent to which people believe an application will help them in the performance of their job (Davis, 1989). A system will be regarded as highly useful if the user thinks there is a positive relationship between the use of the system and performance (Davis, 1989). Perceived ease of use, on the other hand, is an individual's belief of how much the use of a system is free of effort (Davis, 1989). Davis claims that an application that is perceived to be easier to use is more likely to be accepted. Davis (1989) points out that perceived ease of use is similar to Bandura's (1989) self-efficacy construct.

In the context of behavioral information security, the technology acceptance model suggests that two factors can predict an individual's intentions to comply with

information security policies. These factors are the extent to which they perceive compliance with the policy as useful, and the perceived ease of use of the security measures (Lebek et al., 2014). This view assumes that information security policies can be considered a system, and compliance with policies can be considered as system use. However, Davis (1989) applied the model to technology systems and applications rather than policies. I did not deem this model appropriate for my study, which will focus on compliance with password policies.

Causes of Information Security Breaches

An information security breach can have a tremendous impact on an organization in the form of financial loss, loss of consumer confidence, or increased liability (Sen & Borle, 2015). Information security breaches are violations of the confidentiality, integrity, or availability of information in an information system (Laube & Bohme, 2016; Zafar, Ko, & Osei-Bryson, 2016). Information security breaches often involve unauthorized access to sensitive or confidential information such as personally identifiable information, personal health information, or private financial information (Sen & Borle, 2015). Compromised information in security breaches may come from electronic records or paper records (Wikina, 2014). Information security breaches affect diverse sectors such as healthcare, financial, retail, education, and government (Sen & Borle, 2015). Information security violations may occur due to events such as unauthorized disclosure, improper disposal, hacking, accidental loss, or information theft (Wikina, 2014). Information security breaches can, therefore, affect diverse types of information, and different types of security breaches have different causes.

Information security breaches can be classified into categories such as insider threats from within the organization and threats from malicious outsiders (Fritz & Kaefer, 2017). Insider threats can be due to human causes or technical causes. Human threats from within an organization may be intentional or unintentional. Threats related to technical issues could be due to system glitches or process failures (Foresman, 2015). In the following sections, I discuss these main threat categories.

Insider Threats. Individuals within an organization can hamper the security of organizational information systems. The threat posed by insiders such as employees is significant even in organizations that have complex cybersecurity programs (Wang, Gupta, & Rao, 2015). In an analysis of data breaches reported in 2014, Hauer (2015) reported that insiders were involved in approximately 60% of data breaches. It may, therefore, be beneficial for organizations to focus more information security resources towards mitigating threats from within the organization. Insider threats can be intentional or unintentional (Hills & Anjali, 2017; Opderbeck, 2016), and may have different causes (Gheyas & Abdallah, 2016; Hills & Anjali, 2017). A comprehensive information security program should consider both unintentional and intentional insider threats.

Employee actions may result in a breach of information security even if they did not intend to cause such a violation. Unintentional, risky behavior by employees is often due to a lack of security awareness (Safa et al., 2015). Unintentional insider actions could be actions such as visiting websites that are not work-related, selecting passwords that are insecure, writing down passwords on sticky notes, or clicking on phishing links on web sites (Niblett, 2016; Safa et al., 2015). Internal information system users may also engage

in omissive security behavior. Omissive security behavior occurs when employees are aware of security actions that can be taken to mitigate threats, but choose to do nothing about them (Guo, 2013). Such behavior may include failure to change passwords or unwillingness to apply updates. Omissive security behavior may be non-malicious, and although it may be risky, such action may not cause direct damage (Guo, 2013). Insiders may also leak data inadvertently by carelessly posting information on social media, improper disposal of paper records, or improper handling of mobile devices containing sensitive information (Hauer, 2015).

Insider threats may also be intentional. Attacks against an organization's information system by insiders can cause significant damage as employees often have access to the system and may be familiar with the security configurations of the system (Akhunzada et al., 2015). The behavior of insiders may range from non-malicious to malicious acts (Helkala & Hoddø Bakås, 2014; Jouini et al., 2014; Niblett, 2016). Thus, an employee's actions may be unintentional and due to carelessness or ignorance, intentional but non-malicious, or intentional and malicious. Guo (2013) distinguishes between different kinds of intentional insider threats such as computer abuse, information system misuse, violation of policy, and information security policy abuse. Employees may engage in computer abuse in the form of hardware or software theft, data modification, or computing service disruption (Guo, 2013). Employees can also engage in system misuse. Information system misuse may include actions such as using company computers for non-work-related activities, or unauthorized access to confidential information (Guo,

2013). Intentional behavior also includes information theft, sabotage, or espionage (Hills & Anjali, 2017).

Employees may also perform more direct, malicious and intentional violations of information security policies that may cause harm to information systems. For example, employees may transfer sensitive data to their mobile devices, modify security configurations, or share confidential information with third parties outside the organization (Guo, 2013). Malicious activity by insiders has also been associated with scams, fraud, and social engineering incidents (Hauer, 2015). Such intentional, malicious actions by employees can have negative effects on the confidentiality, integrity, and availability of data in an organization's information systems. Intentional violation of security policies by employees may be more common when employees have a negative attitude towards security controls or when employees are non-cooperative with security policies (Hauer, 2015). Insiders with malicious intent pose a major threat to information systems, and this is especially so because they often have easy access to such systems.

Intentional actions by insiders may not always be with malicious intent. Employees may put information systems at risk due to carelessness or ignorance. For example, employees may leave an unattended computer in a logged-in status out of negligence. Also, insiders who are being mischievous or insiders who have an attitude of resistance towards information security policies may cause security incidents (Safa et al., 2015). Non-malicious, risky actions by employees may be due to lack of knowledge or awareness of the consequences of such actions. Such actions may include clicking insecure links or opening attachments in emails, password sharing, or writing down

passwords (Safa et al., 2015). Although insiders may lack malicious intent, their interactions with information systems lead directly or indirectly to security breaches.

Insiders often have elevated privileges and are knowledgeable of an organization's information system, and this makes it easy to bypass security measures and harm the system (Burns, Posey, Roberts, & Lowry, 2017; Wang et al., 2015). Detecting and preventing insider threats may be more challenging than other threats because perimeter countermeasures such as firewalls and intrusion detection systems are ineffective against insider threats (Wang et al., 2015). Furthermore, risky insider behavior may affect an organization's information security indirectly by creating security vulnerabilities that can be exploited by malicious outsiders (Hills & Anjali, 2017).

Malicious outsiders. Malicious outsiders represent a significant source of security breaches in organizations' information systems. Threats to an information system from outside the organization may include unauthorized system access, hackers, theft of information assets, and viruses (Jouini et al., 2014). Organizations can face information security threats from hackers, industrial espionage, social engineering, business partners, retributive action, or environmental sources such as natural disasters (Jouini et al., 2014; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Cybercriminals often target specific information systems and exploit security vulnerabilities that may be present in such systems. From the preceding, it is clear that threats to information systems from malicious outsiders are varied and diverse and may affect technical systems directly or exploit weaknesses in the human aspect of information security.

Hackers use various methods to achieve security breaches. Activity by hackers accounts for a significant number of information security breaches. In a study of mega breaches that occurred between 2005 to 2015, Fritz and Kaefer (2017) reported that hackers were responsible for 43% of the violations. Hackers may attempt to circumvent technical security controls such as firewalls, encryption and intrusion detection systems (Fritz & Kaefer, 2017). Hackers also employ techniques such as the creation of fake websites to lure internet users into revealing sensitive information (Safa et al., 2015). Furthermore, many security breaches occur because of hackers' exploitation of weak passwords used by companies, or the use of network traffic sniffing to obtain passwords of users (Fritz & Kaefer, 2017; Ranjan & Om, 2016). These techniques enable hackers to gain unauthorized access to sensitive information.

Social engineering is another primary technique used by malicious outsiders to breach the security of organizational information systems (Parsons et al., 2014). Social engineering attacks may take the form of phishing attacks via emails or websites. For example, internet users often skim emails and are likely to miss elements of the email message that indicate deception (Jensen, Dinger, Wright, & Thatcher, 2017; Perrault, 2018). Hackers may exploit such user behavior and introduce unsafe links or attachments within emails. Furthermore, hackers may design messages that target specific groups or aim to affect human emotions in particular ways (Vishwanath, 2015). Phishing messages with content based on authority or principles of persuasion are the most effective in convincing users to click on unsafe links (Parsons et al., 2014; Wright, Jensen, Thatcher, Dinger, & Marett, 2014). Hackers may target employees of organizations to manipulate

them to provide information which can be used to attack corporate networks. Spear phishing attacks involve attacks targeting an individual or an organization, while whaling is a form of phishing attack in which the target is someone in authority within an organization (Goel & Jain, 2017). Vishwanath (2015) suggests that targeted training centered around enabling users to recognize clues of deception in emails may be useful in reducing phishing susceptibility. In brief, social engineering involves the targeting of information system users within an organization by malicious outsiders through deception, persuasion or manipulation, aimed at causing users to perform actions that compromise the security of their information systems.

In addition to social engineering approaches, cybercriminals also use other methods to launch attacks on organizational information systems. Hackers may use denial-of-service attacks, website defacements, or web site redirects to target organizations (Jensen et al., 2017). Malicious attackers also use tools such as viruses, trojan horses, and worms to attack organizational networks (Jouini et al., 2014).

Industrial espionage is another threat to organizational information systems. Industrial espionage is an effort to collect and steal information and knowledge such as trade secrets (Soilen, 2016). Industrial espionage typically involves one company spying on another company, although individuals can also carry out espionage (Lee, 2015). The use of computers on the internet to carry out industrial espionage is a less risky, less expensive method of espionage than traditional in-person approaches (Soilen, 2016). Malicious actors, therefore, find such espionage appealing as they seek to get a competitive edge over business rivals. In some cases of industrial espionage, a malicious

actor may plant a third party within a target organization and use such an insider for data collection (Heickero, 2016). Also, disgruntled employees may engage in sharing of company information with competitors (Heickero, 2016; Laszka, Johnson, Schöttle, Grossklags, & Böhme, 2014). Lee (2015) asserts that most industrial espionage is carried out by current or former employees. All the researchers on industrial espionage agree that it involves the theft of information or trade secrets by business rivals or employees, often for financial gain.

Trusted business partners. Many organizations rely on business partners for functions and services. In the healthcare sector, for example, health care providers may rely on business partners to perform tasks such as data analyses, quality assurance, or benefits management (Wikina, 2014). Such partnerships may provide cybercriminals an avenue to access organizational information, as business partners often have some privileges in the organization's information network. An organization's sensitive information can also be exposed during business transactions such as mergers, consulting, auditing, or joint ventures (Hauer, 2015). Vulnerabilities created through such business transactions can be exploited by the business partners or by third-party malicious attackers (Hauer, 2015). Threats from business partners may be challenging to mitigate, as these external entities often require elevated privileges in an organization's network to perform their functions or offer their services (Hauer, 2015).

Lost or stolen devices. Removable or portable electronic devices are another significant source of data breaches. Wikina (2014) examined the causes of data breaches in health institutions. In breaches affecting individuals, the top locations for information

security breaches were laptops, portable electronic devices, and paper records (Wikina, 2014). Theft accounted for 47.5%, and loss accounted for 27.4% of the health information data breaches analyzed (Wikina, 2014). Also, Fritz and Kaefer (2017) reported that 29% of mega violations between 2005 and 2015 involved lost or stolen portable devices. These studies indicate that the loss or theft of information system devices poses a major threat to information system security in organizations. The loss of portable electronic devices such as laptops, tablets, storage disks, tapes, or CDs is often associated with carelessness by employees who are entrusted with such company devices (Safa et al., 2015). In this respect, the threat posed by lost devices may be considered an insider threat. Portable devices containing sensitive data can also be stolen by employees or by outsiders, who may exploit the data for personal purposes or sell the information for gain (Hauer, 2015). Theft of portable devices can also occur as part of an industrial espionage scheme (Hauer, 2015). Also, mobile devices may get lost during interactions with trusted business partners, or during repairs (Hauer, 2015). In essence, lost or stolen devices can negatively affect information system security, and this threat is often associated with careless employees, business partners, or industrial espionage.

Information Security Policy Compliance

Information security policies play an essential role in the implementation of managerial information security (Soomro, Shah, & Ahmed, 2016). An information security policy allows an organization to communicate the expectations to be met in information security, as well as the consequences for not meeting those expectations (Almeida, Carvalho, & Cruz, 2018; Niemimaa & Niemimaa, 2017). Information security

policies address issues such as the acceptable use of technology, social media, and handling of sensitive information (Han, Kim, & Kim, 2017). An information security policy outlines rules and policies for employees with regards to access and use of information systems (Yazdanmehr & Wang, 2016). Information security policies guide users' security-related behavior as they interact with information systems. The policy should also describe information security training requirements for different groups of users, as well as responsibilities for various components of information security (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). Employee compliance with information security policies should, therefore, increase the security level of an organization (Sommestad et al., 2014). A common thread in the information security policy literature is that a security policy should provide training and guidance on acceptable use of information systems.

Information security policies are vital for the overall security posture of an organization. Securing the information assets of an organization involves the use of both technical controls and managerial or administrative tools. In addition to technical controls such as firewalls, antivirus programs, and intrusion detection systems, organizations rely on information security policies to address non-technical aspects of information security (Siponen, Mahmood, & Pahnila, 2014). A comprehensive approach to organizational information security should include people, processes, and technology. New hire orientation programs often provide an opportunity to expose employees to the information security policy of an organization (Bauer, Bernroider, & Chudzikowski, 2017). As part of the onboarding process, employees are often required to sign indicating

acknowledgment and acceptance of the information security policy (Bauer et al., 2017). By ensuring that employees understand the information security policy, organizations can reduce information security risks significantly (Mamonov, & Benbunan-Fich, 2018; Parsons et al., 2014). This risk reduction may be due to the knowledge gained by users about acceptable use of systems and existing security measures when they read the security policy. Bauer et al., (2017) suggest that knowledge of information security policies can influence attitudes towards the policy and intentions to comply with the policy. Awareness of the information security policy and its terms can also promote a sense of moral obligation to adhere to the policy (Yazdanmehr & Wang, 2016). In summation, the research indicates that information security policies are useful in providing education on acceptable use of information systems, influencing user attitudes and behavior, and increasing overall information security.

Karlsson et al. (2017) suggest some criteria for information security policies. An information security policy needs to be clear, well structured, and provide guidelines for action (Karlsson et al., 2017). They further suggest that information security policies should provide guidance that is unambiguous (Karlsson et al., 2017). Teh, Ahmed, & D'Arcy (2015) support this position and assert that ambiguity in information security policies can reduce user compliance with the policy. Using neutralization techniques, employees may deny their responsibility to comply with information security policies if the policies are ambiguous or employee roles are ambiguous (Teh et al., 2015). Therefore, information security policies should be relevant to current work practice (Karlsson et al., 2017; Teh et al., 2015). In sum, an information security policy should be

written in a manner that is clear and easy to understand, providing security behavior directions related to employees' day-to-day practices.

For information security policies to be effective, users must comply with the policies. Without compliance, even the most elaborate information security policy will be ineffective as a countermeasure to security issues (Yazdanmehr & Wang, 2016). Employees are not always compliant with organizational information security policies (Belanger, Collignon, Enget, & Negangard, 2017; Siponen et al., 2014). Noncompliant behaviors such as procrastination or intentional resistance to security policies can be detrimental to organizations (Belanger et al., 2017). Security policy violations such as violations of password policies or information sharing policies can lead to security breaches (Jouini et al., 2014). Such actions could be detrimental to an organization as security breaches may result in financial loss, damaged reputation, liability, or loss of consumer confidence (Jouini et al., 2014). These reports suggest that compliance with information security policies is a key factor in their effectiveness, as lack of compliance may result in negative information security outcomes.

Types of Information Security Policies. Information system security policies contain the expectations of an organization's management concerning the behavior of users of the system. Policies specify what is acceptable use and what is not. The security policy also lays out expectations for the organization's security program, as well as specifications for system controls (Almeida et al., 2018; Helil & Rahman, 2017). Organizational security policies can be designed to address information security

requirements at the corporate level, the user level, the security program level, or the system and control level.

Information security policies can provide security expectations at several levels. At the organizational or corporate level, security policies may provide directives for overall information security and rules for handling and sharing sensitive data (Cram, Proudfoot, & D'Arcy, 2017). Organizational leaders may use an executive-level security policy document to articulate the security vision or overarching strategic direction for all security efforts (Cram et al., 2017). In addition to executive-level security policies, organizations may provide a user-level security policy that addresses information security issues at a more granular level. User level policies focus on providing expectations for acceptable use of systems, including elements such as password policies, email policies, and internet use policies (Belanger et al., 2017; Gallagher, McMenemy, & Poulter, 2015). User level policies provide directives for end-users while executive level or corporate level policies guide information security leaders.

At the security program level, security policies specify required components of the security program, assigns responsibilities for implementation of security program elements, and addresses general oversight of the security program. Policies covered at this level may include incidence management at the organizational level. For example, security program policies may spell out steps to ensure business continuity in case of major information security incidents (Steinbart, Raschke, Gal, & Dilla, 2016).

At the system and control level, policies focus on data and information system classification based on data sensitivity levels or criticality of information system

components. System and control policies also establish controls for the handling, labeling, transportation, and destruction of sensitive data (Helil & Rahman, 2017). Other aspects of information system security that system and control policies may address include data recovery procedures or incident management procedures. System and control policies may target specific system components or hardware, such as data servers, network components, or applications. Examples of policies that fall under the system and control level include the network access policy, web server security policy, acceptable encryption policy, application service provider policy, extranet policy, and the authentication credentials or password policy (Auxilia & Raja, 2016; Mangili, Martignon, & Paraboschi, 2015).

In addition to policies, an information security program may provide standards, guidelines, baselines, and procedures to shape employees' information security behavior. In the following section, I describe these documents.

Standards: Information security standards are an important component of an organization's information security program. Information security standards provide additional details to information security policies, such as details about methods, techniques, or devices (Niemimaa & Niemimaa, 2017). Senior management is often responsible for issuing information security standards, which are often mandatory (Chul Ho, Xianjun, & Raghunathan, 2016). For example, standards for user passwords may specify requirements such as the minimum number of characters, types of characters, password lifetime, and password reuse rules. Standards may also be a collection of best practices established by regulatory bodies in specific industries (Niemimaa & Niemimaa,

2017). Organizations often use such industry-wide security standards to regulate security controls (Chul Ho et al., 2016; Niemimaa & Niemimaa, 2017). In a nutshell, information security standards provide additional details to security policies and may be established internally or by industry-wide regulatory bodies.

Guidelines: Information security guidelines are similar to information security standards, as they also provide additional elaborations on security policies. However, unlike information security standards, security guidelines are not mandatory (Flowerday & Tuyikeze, 2016). Security guidelines suggest best practice methods or techniques. Security guidelines may not go through a formal approval process (Flowerday & Tuyikeze, 2016).

Baselines: Baselines are mandatory and are used to reduce security risk within applications. Information security baselines (or benchmarks) provide additional information on security requirements in information security policies relating to devices or applications where specific settings or parameters are required (Ahuja, 2015). The establishment of baselines or benchmarks can help an organization identify and adopt information security best practices (Ahuja, 2015). Security baselines control security settings or parameters based on known vulnerabilities.

Procedures: Information security procedures help provide a uniform way of implementing policies in areas where multiple individuals with various roles are involved in the process. Information security procedures provide detailed instructions, often step-by-step, for implementing security controls specified in information security policies, standards, or guidelines (Flores, Antonsen, & Ekstedt, 2014). Procedures document the

order in which employees should perform tasks, as well as the roles and responsibilities of all parties involved in the process (Flores et al., 2014). Organizations can use formal procedures to coordinate information security (Flores et al., 2014).

Security policy management. The development of IT policies such as information security policies and privacy policies can help organizations achieve their IT objectives. Information security policies are often a part of a broader Information Technology (IT) governance strategy. IT governance can be viewed as having two primary purposes: (a) to ensure alignment between IT activities and organizational goals, and (b) to provide value from IT (Wilkin, Couchman, Sohal, & Zutshi, 2016). IT governance includes the provision of guidelines and policies related to the actions of employees as they interact with organizational information systems (Alreemy, Chang, Walters, & Wills, 2016). In this way, IT governance is useful in controlling IT decisions and practices and seeking to increase benefits from IT investments (Alreemy et al., 2016). Organizations use several strategies to achieve their information technology goals. Also, organizations in sectors such as healthcare and financial institutions may be required to meet regulatory requirements in areas such as information privacy and information security (Narain Singh, Gupta, & Ojha, 2014; Wilkin et al., 2016). IT policies are useful in helping organizations meet such needs. In addition to such industry-wide standards, organizations must also meet other legal, regulatory or compliance requirements, and the establishment of sound security management practices and policies helps confirm compliance with such requirements (Narain Singh et al., 2014).

Support from organizational management is an essential prerequisite for the success of IT policies. Without adequate stakeholder involvement, the implementation of information security policies and other IT policies will not succeed (Alreemy et al., 2016; Flowerday & Tuyikeze, 2016). The alignment of IT outcomes with business objectives is one of the goals of IT governance, and this will not be possible without the participation of organizational stakeholders. Steinbart, Raschke, Gal, and Dilla (2013) identified top management investment in information security and encouragement of employees by management to practice secure behaviors as critical determinants of information security effectiveness.

Information security policy management involves several activities. After the establishment of information security policies, employees should be made aware of the policies and provided the education and training necessary to comply with them. In addition to policy awareness and training, other components of policy management include the provision of employee education and training, policy enforcement, policy monitoring, and policy review (Soomro et al., 2016; Siponen et al., 2014).

Policy awareness and training. Information security policy awareness and training are essential components of information security management. An information security policy will not be effective without employee awareness of the existence of the policy (Soomro et al., 2016). The role of policy awareness is to provide employees with knowledge of the reasons why they should safeguard organizational information assets from attackers and vulnerabilities (Soomro et al., 2016). Training on information security policies enables employees to efficiently carry out the policy (Soomro et al., 2016). An

information security plan should include steps to ensure that employees have both an awareness of security threats and the importance of protecting information assets, but also adequate training to be able to comply with the policy (Almeida et al., 2018; Siponen et al., 2014). Training employees about changing threats, vulnerabilities, and information security requirements helps to create a workforce that is aware of security risks and can act as a line of defense to secure organizational information assets (Montesdioca & Maçada, 2015; Narain Singh et al., 2014). The provision of training and awareness on information security policies is therefore useful in encouraging policy compliance and improving the overall security posture of an organization.

Policy monitoring. Monitoring is a critical component of information security governance (Steinbart et al., 2013). Policy monitoring involves controlling and evaluating the lifecycle of the policy, managing the policy, and updating the policy when necessary (Estevez, Janowski, & Lopes, 2016). Information security policy monitoring can be performed by IT personnel, or by internal auditors delegated by organizational management (Steinbart et al., 2013). Policy monitoring may involve the use of reports showing how policy objectives and impact are received, policy implementation processes, and progress reports on policy outputs and outcomes (Estevez et al., 2016). Policy evaluators may also rely on feedback from policymakers and end-users.

Policy enforcement. The establishment of information security policies is vital in securing organizational information systems. However, to be effective, security policies need to be enforced (Choi, 2016). Security managers can enforce information security policies through measures such as surveillance and monitoring of employee activities to

identify violations or deter potential violators (Choi, 2016). Moreover, security managers can proactively use security software to prevent contravention of policies (Choi, 2016). For example, organizations can enforce a password policy by mandating the use of passwords of a specified strength (Florêncio, Herley, & Van Oorschot, 2016; Guo & Zhang, 2017). Policy enforcement may also involve sanctioning employees who violate policy, as well as providing education for offenders (Choi, 2016). Some researchers argue that rather than focusing on sanctions and incentives to enforce security policies, organizations should seek to involve employees in the process by creating a shared security vision (Li, Sarathy, Zhang, & Luo, 2014; Sommestad et al., 2014). Organizations can achieve information security policy enforcement through methods such as surveillance, software-based controls, sanctions, or increased employee involvement in information security endeavors.

Policy review. Information security policies should be reviewed to ensure that they remain relevant and address practical security needs. As the information technology environment changes and new threats and vulnerabilities emerge, information security policies need to be reviewed and updated to reflect current information security needs (Choi, 2016). Security policy reviews help to determine whether the policy is still effective and to determine whether the policy needs to be updated to reflect organizational changes (Almeida et al., 2018). During a policy review, information security managers collect feedback about the security policy from stakeholders and analyze the findings to determine policy effectiveness, policy relevance, and monitor policy compliance (Estevez et al., 2016). The review process also involves examination

of security incident data and identification of areas of the security policy that need to be modified (Estevez et al., 2016). Policy review can is useful as a means to ensure the relevance of information security policies as well as to identify any policy shortcomings.

Factors Affecting Compliance

Organizations institute information security policies as a means of safeguarding their information systems and technology assets. The effectiveness of such policies is affected by the compliance behavior of members of the organization (Elifoglu et al., 2018). In this section, I will review the factors influencing employees' compliance with policies, including intrinsic as well as extrinsic factors.

Intrinsic Factors. Intrinsic factors are factors affecting behavior from within the individual (Safa et al., 2015). Intrinsic factors may be self-sustaining and may include internal motivations such as attitudes towards the policy, ethical beliefs, or perceptions about the ability to comply with the policy (Shibchurn & Yan, 2015; Chatterjee, Sarker, & Valacich, 2015). Such factors can affect a user's compliance behavior either positively or negatively. For instance, users are more likely to engage in a behavior if they expect some intrinsic benefit from the behavior (Shibchurn & Yan, 2015). Employee compliance behavior may also be affected by other intrinsic factors such as self-efficacy, information security awareness, and employee stress.

Attitude towards IS policy. The attitude of an individual towards a specific behavior refers to the orientation of the individual's feelings towards engaging in the behavior, and the feelings can be positive or negative (Safa et al., 2015). Formation of an attitude involves the evaluation of an idea, event, or activity, and attitude can range from

very positive to very negative (Safa et al., 2015). In the context of information security, Siponen et al. (2014) assert that there is a positive relationship between an employee's attitude towards information security policies and actual policy compliance. For example, results of a study by Menard et al. (2017) indicated that when managers used security messages that appealed to employees individually or provided choices to users, there was a higher intention to comply with security requirements. This research suggests that employees may have a more positive attitude towards compliance when they are involved in the process of securing information systems. Sommestad et al. (2014) identified threat appraisal and response cost as predictors of attitude towards security policy compliance. Kim, Yang, and Park (2014) also suggest attitude towards misuse of information security policies as a factor affecting IS policy compliance, with perceived severity of sanctions being a predictor of attitude. In sum, these studies provide evidence that user attitudes towards information security policies can affect their compliance behavior.

Kim et al. (2014) investigated behavioral factors affecting employee compliance with IS security policies. Based on the theory of reasoned action, they found that attitude towards compliance, normal belief and self-efficacy affect compliance. Kim et al. (2014) suggest that users will consider the cost and benefits of compliance when deciding whether to comply with or violate the policy. Attitude towards compliance would be more favorable when the benefit of compliance outweighs the cost of compliance or the benefit of noncompliance (Kim et al., 2014). Similarly, this study investigated how employees' attitudes towards compliance with IS security policies affect their intentions to comply with policies.

Safa et al. (2015) found that factors such as commitment, involvement, and employees' attitudes towards compliance with IS policies can influence policy compliance. Information security involvement has to do with aspects such as the sharing of information security knowledge, information security experience, intervention, and collaboration (Safa et al., 2015). Information security knowledge sharing can be used as an approach to increase information security awareness. Information security collaboration helps users to gain knowledge about security breaches while reducing the cost of knowledge acquisition. Information security experience refers to employees' level of familiarity with information security incidents and skills, as well as their ability to mitigate information security risks. Information security knowledge and experience influence proper information security behavior (Safa et al., 2015). Employee commitment to organizations could be due to aspirations for promotion, personal achievement or reputation. When employees are committed to their organization, they are less likely to take the risk of breaking the rules and violating information security policies as this could jeopardize their career aspirations (Safa et al., 2015). Belanger et al. (2017) examined the determinants of early conformance with information security policies. Attitude towards compliance with IS policies was found to be determined by two constructs: perceived severity of the security threat, and vulnerability (Belanger et al., 2017). The more vulnerable users felt, the more likely they were to comply with a password change policy (Belanger et al., 2017). In sum, these researchers all identified attitude towards compliance as a factor affecting compliance with security policies. These findings were relevant to my study, as I also investigated how employees' attitudes towards password policies may influence their intentions to comply with such policies.

Contrary to the studies mentioned above, Herath and Rao (2009) found that employees' attitude towards security policies does not affect their intention to comply with the policies in organizations which have high organizational commitment and monitoring of compliance. Rather, they found self-efficacy, social influence, and perception of threat severity as significant contributors to employees' compliance intention (Herath & Rao, 2009).

Self-Efficacy. In the context of information security policy compliance, Johnston et al. (2016) described self-efficacy as an individual's perception of confidence in his or her ability to comply with information security policies. A review of the literature revealed conflicting reports on the effects of self-efficacy on employees' intentions to comply with information security policies. Several researchers found a positive influence of self-efficacy on intention to comply with information security policies (Bulgurcu et al., 2010; Johnston et al., 2016; Mwagwabi et al., 2014; Siponen et al., 2014). In a study to explore user compliance with password policies, Mwagwabi et al. (2014) found that password self-efficacy had a strong influence on users' password policy compliance intentions. Users' confidence in their ability to create strong passwords correlates with their likelihood to comply with password guidelines (Mwagwabi et al., 2014).

Similarly, in an exploratory field study of employees' adherence to information security policies, Siponen et al. (2014) showed that self-efficacy had a positive, significant effect on employees' intentions to comply. These results agree with findings by Bulgurcu et al. (2010) which suggested that self-efficacy, along with information security awareness and normative beliefs, positively affects employees' intentions to

comply with information security policies. In the same vein, Elifoglu et al. (2018) assert that having the relevant capability and competence in implementing security measures makes employees more likely to adhere to their organization's information security policies.

However, Belanger et al. (2017) suggest that security self-efficacy does not significantly influence the intention to conform to information security policies. This result echoes findings by Kim et al. (2014) that higher self-efficacy of employees does not affect intentions to comply with security policies. These differences in the effects of self-efficacy on compliance intentions may be due to differences in sensitivity of the instruments used in these studies. Belanger et al. (2017) also suggest that employees with high self-efficacy may try to circumvent information security policies, resulting in a negative influence on policy compliance. In the current study, I examined self-efficacy as a factor which may influence employees' intentions to comply with security policies. Based on the social cognitive theory, I investigated the role played by self-efficacy in employees' intentions to comply with password policies.

Information Security Awareness. Information security awareness can be viewed in terms of general information security awareness and information security policy awareness. General information security awareness refers to an employee's overall knowledge and understanding of security threats and their consequences (Bulgurcu et al., 2010). Information security policy awareness focuses on knowledge of the requirements of the information security policy and the purpose of those requirements (Bulgurcu et al., 2010). Information security policy awareness is necessary for change in behavior because

a basic knowledge of an expected change in behavior is needed to carry out the behavioral change (Belanger et al., 2017). Compliance with information security policies may involve a change in user behavior. Therefore, it is important to understand how employees' awareness of security policies affects policy compliance.

Bulgurcu et al. (2010) examined the relationship between information security awareness and employees' attitudes towards compliance with information security policies. Both general information security awareness and information security policy awareness significantly contributed to employees' attitudes towards compliance (Bulgurcu et al., 2010). Also, attitude towards policy compliance directly affected intentions to comply (Bulgurcu et al., 2010). Similarly, Belanger et al. (2017) reported that awareness of security policy change had a positive impact on attitude towards the security policy change in a study focusing on determinants of early conformance with information security policies.

Determinants of information security awareness include information security collaboration, knowledge sharing, and information security experience (Safa et al., 2015). Other studies have shown that information security collaboration, and knowledge sharing affect users' attitudes towards information security policies (Flores et al., 2014; Tamjidyamcholo, Baba, Shuib, & Rohani, 2014). Furthermore, better knowledge and attitudes towards security policies are associated with information security behavior that is less risky (Ogutcu, Testik, & Chouseinoglou, 2016; Parsons et al., 2014). An awareness of what is occurring in information security has a positive bearing on users' ability to recognize potential threats (Ogutcu et al., 2016). Employees who are

knowledgeable about potential threats may be less susceptible to security threats such as phishing attacks. A poor understanding or situational awareness of information security may be correlated with unintentional insider threats such as user errors (Moody, Siponen, & Pahnila, 2018; Parsons et al., 2014). Employees can obtain information about security threats through internal organizational channels such as e-learning, company-wide newspapers, or posters (Bauer et al., 2017). Information security awareness can also be increased through external sources like self-organized learning, or traditional media such as TV and radio (Bauer et al., 2017). Bulgurcu et al. (2010) suggest that information security awareness has a positive influence on a user's attitude towards compliance. In this study, I investigated the relationship between employees' information security awareness and their attitudes towards password policies, as well as the effects of security awareness on intentions to comply with password policies.

Employee Stress. Organizations depend on various technologies to manage the security of their information systems. In response to the diverse nature of security threats they face, organizations are adopting sophisticated technologies such as network firewalls, document encryption technologies, network monitoring technologies, and device control technologies (Hwang & Cha, 2018). Although these technical solutions are beneficial, the adoption of such technologies may be stressful and challenging for employees (D'Arcy, Herath, & Shoss, 2014). Furthermore, organizational information security goals may sometimes conflict with employees' goals, as employees may focus more on performance and efficiency objectives (Hwang & Cha, 2018; Montesdioca & Maçada, 2015). Bulgurcu et al. (2010) argued that employees might choose not to comply

with information security requirements if the cost of compliance outweighs the benefits of compliance. Hwang and Cha (2018) explored the possibility that the adoption of complex technologies to improve information technology adversely affected employee compliance with security policies. The researchers found that employee stress related to information security negatively affected employees' organizational commitment and intentions to comply with security policy (Hwang & Cha, 2018). These findings were consistent with results from other studies which suggested that employees were more stressed when faced with continuously changing technologies, resulting in adverse outcomes such as dissatisfaction and decreased productivity (Gaudioso, Turel, & Galimberti, 2015; Lee, Lee, & Kim, 2016; Tarafdar, Bolman Pullins, & Ragu-Nathan, 2014). In brief, employees may experience stress related to the use of technologies or the implementation of information security measures, and such stress can negatively influence compliance with security policies.

Intention to Comply. An employee's intention to comply with information security policies can be viewed as his or her intention to follow recommended guidelines and safeguard their organization's information system resources from potential threats (Bulgurcu et al., 2010; Mwagwabi et al., 2014). Several researchers made a distinction between intention to comply and actual compliance with security policies (Bulgurcu et al., 2010; Belanger et al., 2017; Sommestad et al., 2014). Although these constructs are distinct, intention to comply is widely viewed as an antecedent to actual compliance (Ajzen, 1991; Bulgurcu et al., 2010; Belanger et al., 2017; Siponen et al., 2014), and

there is evidence in the literature to support this link (Bauer et al., 2017; Belanger et al., 2017; Siponen et al., 2014).

Several factors may determine the intention to comply with information security policies. Among the factors mentioned most in the extant literature are users' self-efficacy, information security awareness, and attitude towards compliance (Bulgurcu et al., 2010; Kim et al., 2014; Menard et al., 2017; Siponen et al., 2014). Other constructs that were associated with intentions to comply include normative beliefs (Belanger et al., 2017; Safa et al., 2015), and social influence (Herath & Rao, 2009). Mwagwabi et al. (2014) found that threat appraisal factors such as perceptions of vulnerability, threats or severity of information security risks could influence internet users' intentions to comply with password policies. These results were in line with findings by Herath and Rao (2009) suggesting that the severity of threats may affect employees' intentions to comply with security policies. These findings on factors determining intentions to comply with security policies are particularly relevant to my study. The current study focused on an examination of the relationship between employees' intentions to comply with password policies, and factors such as self-efficacy, attitudes towards compliance, and information security awareness.

Extrinsic factors. An employee's intentions to comply with information security policies can also be affected by extrinsic factors. Extrinsic behavioral factors refer to factors that are external to the individual (Safa et al., 2015). Extrinsic factors include those that come from the organization or environment, such as policy promotion, or behavioral consequences such as rewards or punishment (Shibchurn & Yan, 2015).

Information Security policy promotion. Managerial support is critical for the effectiveness of an information security policy. Top management involvement and the number of resources invested in information security can increase the efficiency of information security programs (Steinbart et al., 2013). Organizational factors that may affect information security policy compliance include the development of the policy, the creation of awareness, compliance enforcement, and implementation of best practices regarding information security (Soomro et al., 2016). The establishment of well-defined policies and management processes for the implementation of information security objectives is crucial for the effectiveness of information security policies and programs (Narain Singh et al., 2014). Awareness and training may help provide a better understanding of the policies and an appreciation of the importance of securing organizational information security assets. Ayyagari and Figueroa (2017) reported that information security policy training was more effective when it involved showing employees the possible effects of noncompliance with policies, rather than just being presenting the requirements. This study highlighted the importance of providing employees the reasons behind written security policies (Ayyagari & Figueroa, 2017). In short, organizations can promote information security policies through management involvement, provision of training and awareness, policy enforcement, user involvement.

Information security policy implementation and enforcement. Organizational management plays an essential role in the formation of social norms in the workplace. For example, organizations can develop an information security culture that favors compliant behavior and makes it the norm. Bauer et al. (2017) found that social norms

positively influenced employees' intentions to comply with security policies. Social norms refer to perceptions employees have about what is acceptable information security behavior in their organizations (Bauer et al., 2017). Social norms related to security are affected by the general information security culture of the organization. Establishment of an information security-oriented culture can promote a holistic approach to information security, involving people, processes, and technologies (AlHogail, 2015; Da Veiga & Martins, 2015; Ritzman & Kahle-Piasecki, 2016). The role played by management in information security effectiveness has also been examined by others (Choi, 2016; Dang-Pham, Pittayachawan, & Bruno, 2017). For example, Choi (2016) found that inspirational motivation by information security managers increased levels of enforcement of information security policies (Choi, 2016). Information security managers can use information security policies as mediators as they seek to inspire or influence employees towards security compliant behavior (Choi, 2016). Management can take several measures to implement information security policies. These include promotion of user education about the policy, the use of monitoring and surveillance programs to enforce policies, and implementation of sanctions for policy violators (Choi, 2016). Such proactive measures would help establish an organizational culture that favors information security compliance.

Another useful approach to enhance information security policy compliance is through sanctions and rewards. Sanctions are penalties suffered by employees for noncompliance with the information security policy (Bulgurcu et al., 2010). Sanctions can be in the form of reprimands, demotions, monetary penalties, or unfavorable mention

in assessment reports (Bulgurcu et al., 2010). Cheng et al. (2013) studied the violation of information security policies in organizations. The severity of sanctions was found to affect employees' intentions to violate information security policies positively. Sanctions, therefore, serve as a deterrent factor in information security policy violation. Moody et al. (2018) opined that the deterrent element of sanctions was more effective when employees see examples of policy violators who are caught and punished.

Rewards may also influence employee compliance with information security policies. When users expect to benefit from an activity, they are more likely to perform the activity (Shibchurn & Yan, 2015). Kim et al. (2014) hypothesized that employees' perceptions of the benefits of compliance with information security policies positively influence their intentions to comply with policies. In a survey-based study, results indicated that the benefit of compliance has a high influence on employees' intentions to comply with security policies (Kim et al., 2014). In other words, employees had high intentions to comply with security policies when they perceived that they had great benefits for complying with policies.

Similarly, Bulgurcu et al. (2010) reported a positive influence for rewards on employee compliance intentions. However, in the study by Bulgurcu et al. (2010), perceived benefit of compliance affected employees' attitudes towards compliance, which in turn affected intentions to comply with security policies. Perceived benefits of compliance encompass three constructs: intrinsic benefits (such as feelings of satisfaction, fulfillment, and accomplishment), the safety of resources, and rewards (Bulgurcu et al., 2010). Rewards for compliance can include financial benefits, favorable

promotion prospects, pride, or satisfaction (Kim et al., 2014). In brief, these studies suggest that rewards, both intrinsic and extrinsic, may have a positive effect on employees' attitudes towards compliance and their intentions to comply.

Gap in the Literature. Several sources in the literature discussed compliance with information security policies (Bauer et al., 2017; Belanger et al., 2017; Parsons et al., 2014; Yazdanmehr & Wang, 2016; Siponen et al., 2014). There were also several studies focusing on the factors that influence policy compliance (Elifoglu et al., 2018; Menard et al., 2017; Safa et al., 2015; Shibchurn & Yan, 2015; Sommestad et al., 2014). Antecedents of information security policy compliance identified in the literature included intrinsic factors and extrinsic factors. Intrinsic factors included employees' information security awareness, self-efficacy, attitudes towards policy compliance, and employee stress (Bulgurcu et al., 2010; D'Arcy et al., 2014; Hwang & Cha, 2018; Johnston et al., 2016; Mwagwabi et al., 2014; Siponen et al., 2014). Researchers also identified extrinsic factors such as the promotion of security policies by management, policy implementation, and enforcement through strategies such as sanctions and rewards (Bulgurcu et al., 2010; Cheng et al., 2013; Choi, 2016; Kim et al., 2014). Although these studies examined compliance with information security policies in general, there was a paucity of studies focusing on password policies. Mwagwabi et al. (2014) examined how user perceptions of passwords influenced their intentions to comply with password policies. Mwagwabi et al. (2014) showed that increasing users' coping appraisal through training interventions could enhance users' compliance intentions. Belanger et al. (2017) investigated the determinants of early conformance to new password policies in a

university setting. The authors suggested that attitudes towards conformance and self-efficacy had a positive influence on intentions to conform and actual policy conformance (Belanger et al., 2017). The main gap identified in the policy compliance literature was the paucity of studies focusing on compliance with password policies, even though a significant proportion of security breaches are password-related.

This study focused on assessing how factors such as employees' information security awareness, password self-efficacy, and attitudes towards password policy compliance, affect employees' intentions to comply with password policies. Using a survey design, I addressed factors affecting password policy compliance from the employees' perspective. The focus on password policy compliance by employees is relevant, as ill-intentioned agents such as cybercriminals highly exploit password-related vulnerabilities, and this can lead to costly security breaches (Belanger et al., 2017; Lebek et al., 2014). Also, employees play a central role in organizational information security, so it is necessary to examine information security policy compliance from the employees' perspective. My study focused on the role played by employees, and this is important because, even though organizations are investing more in technical information security controls, security breaches are still on the rise (Hull, 2015).

Applications of Regression Analyses

A key theme in my literature review was the application of regression analysis. This theme was selected for me as a researcher to gain an adequate understanding of the principles of linear regression and its application in the literature. Regression analysis is used to make inferences about the effects of predictor variables on an outcome variable

(Hall, 2016). Researchers use the regression model to describe the relationship between variables (Constantin, 2017). The regression model can also be used to control and predict the behavior of an outcome variable based on the evolution of one or more predictor variables (Constantin, 2017). Several forms of regression exist, including linear regression, multi-linear regression, probit regression, and logistic regression (Granato, de Araújo Calado, & Jarvis, 2014). The choice of the specific regression technique or variant depends on both the nature of the dependent and independent variables. For example, ordinary least squares regression (OLS) is the simplest regression model and assumes a linear relationship between variables under study (Constantin, 2017). It also assumes that both the dependent and independent variables are continuous. In the case of ordinal logistic regression, the independent variables can contain a mix of continuous and discrete variables. Also, the dependent response variable is discrete and ordered (ordinal). Discrete and ordered responses are common in Likert item responses (Hedeker, 2015). Ordinal logistic regression is the specific linear regression model applied in this study.

Researchers use linear regression when the model involves one independent variable and one dependent variable (Constantin, 2017). Regression techniques can be used to predict the value of the dependent variable from the value of the independent variable (Hazra & Gogtay, 2016). In linear regression, a simple mathematical function, the regression equation, quantifies the straight-line relationship between the independent and dependent variables. The following general formula expresses the regression equation:

$$\mathbf{y} = \mathbf{X}b + \mathbf{e} \quad (1)$$

where **y** is a data matrix associated with the response variable, **X** is a matrix representing the predictor variable and the number of observations, and e is an error term (Chen, Pourahmadi, & Maadooliat, 2014). Multiple regression is widely used by researchers and business analysts due to its versatility and ease of use. Multiple regression is appropriate when two or more independent variables are affecting a dependent variable (Constantin, 2017). Essentially, a regression model is used to fit a line among a series of independent variables to best predict a dependent variable.

Certain general assumptions should be satisfied in ordinal logistic regression analyses. These include the assumption of proportional odds, the assumption of no multicollinearity, and the assumption of ordinal level dependent variables (Brown, MacDonald, & Mitchell, 2015; Peng, Lee, & Ingersoll, 2002). The ordinal logistic regression approach and assumptions are discussed in greater detail in Section 2.

Applications of Multiple Regression. Multiple regression has been used to describe relationships between variables and predict outcomes in diverse domains. Multiple regression has been applied in healthcare, environmental science, transportation, agriculture, bioinformatics, and education (He, Kuhn, & Parida, 2016; Khan & Al Zubaidy, 2017; Liu, Ko, Willmann, & Fickert, 2018; Morin, Thomas, & Saadé, 2015; Owen, Smith, Osei-Owusu, Harland, & Roberts, 2017; Taki, Ajabshirchi, Ranjbar, & Matloobi, 2016). In the following section, I present a brief discussion of applications of multiple regression.

Khan & Al Zubaidy (2017) used a multiple linear regression model for predicting student performance in different learning environments. The authors examined student performance as an outcome variable and explored how other factors influenced performance. Study variables included physical training, academic aptitude, and training need analysis. The regression model was useful in predicting student performance based on at least one of the independent variables. Selection of the final model was based on an approach in which p-values of selected parameters had to be less than 0.05 (Khan & Al Zubaidy, 2017). The researchers were also able to predict student attrition, which can be useful in developing strategies for student mentoring.

Owen et al. (2017) investigated factors that determined football players' attitudes towards different types of playing turfs. Using a survey, the authors captured the sentiments of players towards natural and artificial turf pitches. The researchers used ordinal logistic regression, a variant of linear regression, to develop a model to analyze players' responses regarding perceptions about playing surfaces. Owen et al. used a survey which they administered to 1,129 players. Results from the ordinal logistic regression analyses indicated that overall, the majority of players preferred pitches with a natural turf, and players considered the quality of the playing surface as an important factor which determined their preferences. Using an ordinal logistic regression model enabled the authors to relate players' perceptions to several predictive variables.

Liu et al. (2018) performed a study to explore the perceptions of teachers towards professional development to promote the use of iPads. Using multiple linear regression, the authors found teachers' self-efficacy in the use of mobile devices as a significant

predictor of teachers' attitudes towards professional development training. Liu et al. (2018) used two regression models: one to analyze teacher's perspectives towards professional development training at mid-year, and a second model for end-year analyses. Both regression models showed statistically significant results, with factors such as self-efficacy, type of school, and previous experience with mobile technology being significant predictors of teacher's response to professional development training.

Researchers also used multiple regression analysis in the field of Agriculture. For example, Taki et al. (2016) used a regression model to predict roof temperature, inside soil humidity, soil temperature, and inside air humidity in greenhouses. In this study, there were multiple independent variables and multiple dependent variables as well. The authors used several regression models, one for each dependent variable. Taki et al. (2016) also used an Artificial Neural Networks (ANN) model and a Multilayer Perceptron (MLP) algorithm to investigate the relationships between their study variables. Results showed that the multiple regression model was able to predict roof temperature with low error, and soil temperature with high error. Overall, the multiple regression model was not as good as the ANN model or the MLP algorithm in analyzing data with more than one outcome variable (Taki et al., 2016).

He et al. (2016) applied multiple output regression in a study focusing on multiple genetic trait predictions. He et al. (2016) made the distinction between the use of regression to predict a single trait from a set of biological samples using single regression, and prediction of multiple traits from a set of samples using multiple output regression. The authors argue that when the output traits for a sample set are correlated,

such correlations can be leveraged to improve prediction accuracy (He et al., 2016). Using an avocado dataset and predicting traits such as seed weight, fruit weight, fruit length, fruit diameter, fruit width and number of fruits, He et al. (2016) showed that the multiple outcome regression model was very competitive with other existing statistical methods in predicting genetic traits.

Morin et al. (2015) built a multiple regression model to predict perceived problem-solving skill acquisition in a convenience sample of college students. The predictor variables in this study were research skills, critical thinking skills, and creative idea generation skills. The researchers used a survey to assess student's perceptions of how research skills, creative idea generation, or critical thinking skills helped them solve problems. Morin et al. (2015) used correlation analysis and Tukey-Kramer posthoc tests for analysis of variance. Multiple regression analysis showed that research and critical thinking skills were the most significant predictors of problem-solving skill acquisition.

Transition and Summary

This study aimed to explore factors that affect employees' compliance with information security policies. In this section of the study, I provided background and context for the problem and discussed the purpose and nature of the study. I also discussed two main theories, the theory of planned behavior and the social cognitive theory, which will provide a theoretical framework for the study. Furthermore, I presented other competing theories in the literature, outlining their main constructs. The literature review included three main themes. Theme one focused on the causes of information security breaches and included an examination of insider threats, malicious

outsiders, and threats from business partners. Theme two centered around information security policy compliance. I reviewed information security policy types, and aspects of security policy management such creation of awareness, training, monitoring, and enforcement. For the third theme, I examined factors affecting security policy compliance. The main factors that emerged from the literature included both intrinsic and extrinsic factors. Intrinsic factors or factors from within the individual included attitudes towards security policies, self-efficacy, information security awareness, and employee stress. Extrinsic factors included organizational factors such as policy promotion, implementation, enforcement, and organizational culture. The final theme of the literature review focused on a discussion of multiple regression analysis and its application in diverse fields of study including the field of information security behavior. This concludes Section 1 of this study.

Section 2 of the study includes a detailed discussion of research methodology and design, including the population and sampling, ethical considerations, data collection, and analysis techniques. In Section 3, I present the findings of the study, its applications to professional practice, implications for social change, and discuss recommendations for further study.

Section 2: The Project

Purpose Statement

The purpose of this quantitative correlational design study was to quantify the relationship between employees' attitudes towards password policies, information security awareness, and password self-efficacy, and employee intentions to comply with password policies. The independent variables were employees' (a) attitudes towards password policies, (b) information security awareness, and (c) password self-efficacy. The dependent variables were measures of intention to comply with password policies including employees' overall intentions to comply with password policies, intentions to comply by protecting information and technology resources according to the password policy, and intention to comply by carrying out their responsibilities as prescribed in the password policy. The three independent variables are constructs or latent variables that were operationalized from composite scores of participants' responses to survey items.

The survey instrument is shown in Appendix A. I used the survey platform Qualtrics (Qualtrics, 2018). I guided Qualtrics to select a cross-sectional sample of employees who work for organizations in the United States that have an information security password policy in place. Such a qualified sample was easy for Qualtrics to administer because it already had the required sample frame of participants as defined for this study (see "Participants").

This study may contribute to positive social change, as findings from this research could lead to a reduction in the likelihood of security breaches and an increase in the integrity of customers' personally identifiable information. A potential reduction in

security breaches could promote customers' confidence in enterprise information systems, reduce revenue loss due to identity theft, and enhance customer satisfaction.

Role of the Researcher

An important consideration in research studies is the role played by the researcher. Based on the research paradigm that is adopted, the role of the researcher may vary. Murshed and Zhang (2016) stated that a researcher's observation, description, and classification of a phenomenon is affected by the researcher's school of thought and worldview. Quantitative researchers often adopt an objectivist epistemology and use statistical methods to investigate relationships between variables (Yates & Leggett, 2016). In the quantitative paradigm, the researcher views his or her role as separate and independent from the object of the study and takes an objective stance towards the research (McCusker & Gunaydin, 2015; Yates & Leggett, 2016). Irrespective of research approach, however, a researcher can introduce bias in a study (Kuru & Pasek, 2016). Bias can occur at several stages of the research process such as during data collection, data analysis, or data interpretation, and it may be intentional or unintentional (Boulesteix, Stierl, & Hapfelmeier, 2015; Kuru & Pasek, 2016). Researchers should be aware of the sources of bias and endeavor to minimize it (Kuru & Pasek, 2016). Moreover, any research involving human subjects can be ethically challenging and may require standards to guide researchers (Bracken-Roche, Bell, Racine, & Macdonald, 2017). For example, the Belmont Report provides guidance on ethical issues such as protecting the welfare of research participants, having proper participant recruitment practices, and using informed consent (Bracken-Roche et al., 2017).

My personal experience with information systems includes formal education in computer science and information technology. In addition, I have held several work positions in which I provided technical assistance to users of information systems. Currently, I work in an enterprise environment where I use information systems with information security policies including password policies. I am therefore familiar with information systems and subject to compliance with information system password policies. In this study, I adopted a quantitative research paradigm. True to the quantitative tradition, I distanced myself as the researcher from the subject of the research. One way that I did so was using statistical methods to perform an objective, independent analyses of the relationships between the study variables. To further mitigate any possible bias, I used an online survey approach for data collection. Online surveys are beneficial in research situations where respondents are required to provide sensitive information (Roster, Albaum, & Smith, 2014). The anonymity presented by the online survey format helps reduce respondents' bias due to fear of punitive actions associated with their responses (Roster et al., 2014). My role in this study was limited to sending out the survey, collecting the responses, analyzing the data, and reporting the findings. Also, I adhered to the guidelines provided by the Belmont Report (Bracken-Roche et al., 2017) concerning the protection of participants. For example, participants were allowed to choose to participate or withdraw from the study at their free will. Also, I protected the identity of participants throughout the study.

Participants

Qualtrics, an online-based marketing research company based in the United States (Qualtrics, 2018), executed my survey. Qualtrics sent out e-mail invitations to panel members who were most likely to qualify for the study. Qualtrics uses hundreds of profiling attributes to build specialized panels, and also partners with third-party panels (Qualtrics, 2018). The company uses demographic information from panelist profiles to match members with surveys (Qualtrics, 2018). For example, my study was limited to employees who work for organizations in the United States. Qualtrics used this criterion to identify panel members who work for organizations within the United States, including employees from organizations in diverse sectors of the economy. After identifying panel members who were likely to qualify, Qualtrics sent out e-mail invitations randomly to a subset of these members. The e-mail invitation did not contain details about the questions in the survey. Panel members who responded to the invitation were further screened using a set of screening questions which I provided (see Appendix B). The screening questions were used to limit participants to employees who (a) worked for an organization in the United States, (b) had an explicitly written information security policy which includes a password policy, and (c) were aware of the requirements of the password policy. These criteria were broad and relaxed allowing a broad spectrum and thus cross-sectional sample of participants. Also, this choice was consistent with the selection criteria used in a similar study (Bulgurcu et al., 2010). Qualtrics selected the final set of participants randomly from the list of qualified panel members.

Qualtrics administered the survey (see Appendix C) through the Internet. Collection of data of a sensitive nature, such as data concerning employees' information security behavior, poses some challenges to researchers. Employees within an organization may be reluctant to disclose information about their information security behavior if they perceive a lack of privacy and confidentiality (Mueller, Straatmann, Hattrup, & Jochum, 2014; Roster et al., 2014). This challenge can be overcome by using an Internet-based survey, an approach which provides greater anonymity (Mueller et al., 2014). Roster et al. (2014) suggested that computer-assisted survey modes increase participants' willingness to answer questions of a sensitive nature. Furthermore, Internet-based surveys present advantages such as the ability to reach more diverse samples and lower survey administration costs (Rice, Winter, Doherty, & Milner, 2017).

Ethical considerations in the conduct of research include protecting the identity of participants, allowing freewill participation and withdrawal, and informing participants of the purpose of the study (Drazen et al., 2017; Gotterbarn, Bruckman, Flick, Miller, & Wolf, 2018; Grzyb, 2017). Participants were invited to participate via e-mail. The invitation e-mail contained an overview of the purpose of the study and requested participants to give their informed consent. E-mail communication of the goal of the research and the request for informed consent was useful in establishing a working relationship with the participants.

Research Method and Design

Researchers can use different methods to address research questions. Factors that may influence the choice of a research method include the nature of the research

questions and the researcher's worldview (Barczak, 2015; Yates & Leggett, 2016). Two principal methods used in research are qualitative and quantitative methods (Lewis, 2016). Researchers using mixed-methods approaches use a combination of qualitative and quantitative methodologies (Thaler, 2017). In this study, I used a quantitative method to address the research question. In this subsection, I will discuss the method and design selected for the study, including the justification for the selections.

Method

I used a quantitative research method with regression analyses for this study. First, I will provide an overview of the regression-based technique, and then justify its applicability to my research problem and questions.

Overview of regression. Regression analysis is used to make inferences about the effects of predictor variables on an outcome variable (Hall, 2016). Researchers use the regression model to describe the relationship between variables (Constantin, 2017). The regression model can also be used to control and predict the behavior of an outcome variable based on the evolution of one or more predictor variables (Constantin, 2017). Several forms of regression exist, including linear regression, multi-linear regression, probit regression, and logistic regression (Granato et al., 2014).

Regression techniques can be used to predict the value of the dependent variable from the value of the independent variable (Hazra & Gogtay, 2016). In linear regression, a simple mathematical function, the regression equation, quantifies the straight-line relationship between the independent and dependent variables. The following general formula expresses the regression equation:

$$\mathbf{y} = \mathbf{X}b + \mathbf{e} \quad (2)$$

The term **y** is a data matrix associated with the response variable. The matrix y contains m rows where m is the number of observations in the dataset. Similarly, **X** is a matrix containing m rows and n columns, where m is the number of observations and n is the number of independent or predictor variables. The term **e** is a matrix containing m rows and represents the error involved in the model (Chen et al., 2014).

Multiple regression is appropriate when two or more independent variables are affecting a dependent variable (Constantin, 2017). In multiple regression analyses, researchers estimate the influence of independent variables on a dependent variable after accounting for the impact of other independent variables (Woodside, 2013). Such analyses focus on whether specific independent variables have a significant or non-significant net effect on a dependent variable in the presence or absence of other independent variables (Woodside, 2013). Equation (2) shows the formula for multiple regression. In this equation, the index "i" represents the ith observation.

$$Y_i = b_0 + b_1X_{1i} + b_2X_{2i} + b_3X_{3i} + b_kX_{ki} + e_i \quad (3)$$

The term b_0 is a constant which denotes the intercept of the line on the Y-axis, and X_1, X_2, X_3 … X_k represent scores on different predictor variables. The term b_1 represents the slope of the line or the regression coefficient, and e is a random error by which Y (the dependent variable) is supposed to deviate from the mean (Constantin, 2017; Hazra & Gogtay, 2016). The constant b_1 also represents the change in Y per unit change in $X1_i$, holding all other variables the same. Establishing the values of b_0, b_1, b_2, b_3, etc. enables the creation of a model for predicting Y from X (Hazra & Gogtay, 2016).

Rationale for method selection. The nature of research questions can drive research method selection (Barnham, 2015). Quantitative methods are suitable when the research inquiry involves finding relationships between numerical variables (Claydon, 2015; McCusker & Gunaydin, 2015). The research question in this study centered around examining the relationships between three latent predictor variables and one latent outcome variable. Based on the nature of the research question, a quantitative method was considered most fitting for this study. A quantitative approach with regression analyses was adequate to determine the relationship between employees' attitudes towards information system password policies, employees' security awareness, employees' password self-efficacy, and employees' intentions to comply with password policies.

Another factor that may influence the choice of a research method is the researcher's thinking orientation or worldview (Murshed & Zhang, 2016). A positivist view of research favors the quantitative research paradigm, while post-positivist views are more aligned with the qualitative research paradigm. As a researcher, I support the positivist worldview or paradigm. According to the positivist worldview, the researcher is detached from the subject of the research and uses statistical methods to perform an objective inquiry into relationships between study variables (Clarke, 2016; Kock, Avison, & Malaurent, 2017). In such a paradigm, the researcher has a role restricted to observation, data collection, and interpretation in an objective way.

A qualitative methodology is not suitable for this study. A qualitative approach to research is appropriate when the research focus is on exploring a phenomenon or

assigning meaning to human actions (Barnham, 2015; Kyonne, 2015). Qualitative research focuses on understanding participants' views of social processes, practices, and phenomena in the context of their social environments (Green, 2015; Koch, Niesz, & McCarthy, 2014). The research questions being addressed in the current study are not centered around social processes or phenomena; rather this study aims to analyze the relationship between quantifiable variables. Qualitative methods favor a subjectivist epistemological orientation, in which the researcher may be the data collection instrument, using tools such as interviews, observation, and field notes to collect non-numeric data from participants (Green, 2015). This study involved collection and analyses of numeric data using a survey instrument. Thus a quantitative approach was more appropriate.

A mixed method approach, which combines qualitative and quantitative approaches, was not the best method for this study. Mixed methods are ideal when there is a need for multiple data sources to achieve data triangulation (Thaler, 2017). The use of quantitative or qualitative methods alone may not be sufficient in some instances of inquiry. Researchers use mixed methods to collect data from multiple sources and use diverse approaches for data analysis and interpretation (Annansingh & Howell, 2016; McKim, 2017). Mixed methods require higher amounts of research effort, involving expertise in both qualitative and quantitative techniques (Thaler, 2017; McKim, 2017). Due to the limited scope of this study with regards to time and resources, a mixed method approach was not appropriate. Furthermore, this study did not have a qualitative component, so the use of a mixed methods approach was not necessary.

Research Design

In this study, I used a correlational design with a cross-sectional survey. A correlational design is useful in assessing relationships between variables (Curtis, Comiskey, & Dempsey, 2016). Correlational designs are appropriate when a researcher does not have control over the independent or predictor variables but instead investigates how the variables are related to each other (Curtis et al., 2016; Claydon, 2015). Correlation can be used to examine the extent to which a change in one variable is related to differences in one or more other variables. Correlational analyses are typically used with variables that have an ordinal, interval, or ratio level of measurement (Curtis et al., 2016). A correlational design was appropriate for this study because the study will focus on examining the relationship between three independent variables and a dependent variable. The variables in this study (employees' attitudes towards information system password policies, employees' security awareness, employees' password self-efficacy, and employees' intentions to comply with password policies) had a ratio level of measurement. Also, a correlational design is appealing because it is straightforward, inexpensive, and sufficient to demonstrate an association between variables (Cowls & Schroeder, 2015).

A cross-sectional survey was administered in this study. Cross-sectional surveys are used to capture data from a cross-section of a population of interest at a single point in time (Van der Stede, 2014). The survey was administered to a random sample of employees, which allowed generalization of the results to the underlying population (El-Masri, 2017).

Other quantitative research designs include descriptive and experimental designs (Ingham-Broomfield, 2014). A descriptive study design was not adequate for this study. Researchers use descriptive designs when they need to describe the characteristics of variables without investigating the relationships between them. In descriptive studies, researchers may describe rare or unusual events of interest, or evaluate frequencies of variables (Ingham-Broomfield, 2014; Manterola & Otzen, 2017). Descriptive designs can be used to formulate hypotheses of risk factors or to study the degree of adherence to recommendations (Manterola & Otzen, 2017). The descriptive research design does not involve assessment of associations or relationships between variables. To address the research question in the current study, I assessed the relationships between several variables. A descriptive approach was therefore not aligned with the purpose of this study.

Experimental designs are used to investigate cause-and-effect relationships between variables (Cho et al., 2016; Zellmer-Bruhn, Caligiuri, & Thomas, 2016). In experimental designs, the researcher manipulates the predictor variable and assesses its effects on the outcome variable (Cowls & Schroeder, 2015). Although the variables in this study (such as employee information security awareness, self-efficacy, and policy compliance intentions) could have a cause-effect relationship, answering the research question for this study did not require an investigation of a cause-effect relationship. Also, experimental designs typically involve two groups of participants, a treatment group and a control group, and participants may be randomly assigned to treatment or control groups (Zellmer-Bruhn et al., 2016). The treatment group receives an intervention

while the control group receives no intervention (Barnighausen et al., 2017). In this study, there was no manipulation of variables and the study did not include an intervention on the participants. Therefore, an experimental design was not suitable for this study.

Population and Sampling

Population

As stated earlier, the sample of study participants was selected by Qualtrics, an internet-based market research firm. Using an internet-based market research firm such as Qualtrics was advantageous because such an approach provided access to a broad population, diverse samples, and required less time than other data collection approaches (Hays, Liu, & Kapteyn, 2015; Schoenherr, Ellram, & Tate, 2015). Qualtrics and its panel partners use rigorous profiling criteria to create niche member panels. Panelists are matched with surveys for which they are most likely to be eligible based on their demographic profiles. The sample frame for this study consisted of employees in the pool of Qualtrics' panel participants who worked for organizations in the United States which had an explicit information security policy. Participation was limited to employees who used information systems to perform their daily tasks. Also, only employees who were aware of the requirements of their organization's password policy were eligible. Qualtrics used the criteria mentioned above to delineate a sample frame which was aligned with the population of interest for this study. Participants were selected from diverse business sectors to ensure a cross-sectional sample was obtained.

The use of an internet-based research firm such as Qualtrics to collect data may have some drawbacks. For example, the extent to which samples from a research firm's data pool is representative of a broader population may be questionable (Schoenherr et al., 2015). In the context of this study, one possible concern may be whether employees in the Qualtrics pool of participants were representative of employees in the broader US population. Qualtrics has a nationally representative pool of about six million panel participants (Qualtrics, 2018). To further ensure that a representative sample of employees was obtained, Qualtrics was required to provide a sample containing employees from organizations in diverse business sectors such as education, healthcare, manufacturing, government, services, financial, and technology.

Another critique of such an Internet-based approach is that sampling bias may be introduced due to the methods used by the research companies to recruit participants. Sampling bias in such samples may occur due to the self-selection of participants or because the internet population may not be representative of the general population (Tsuboi et al., 2015). One approach to enhance the representative nature of the sample is by using screening questions so select participants who meet characteristics specified by the researcher (Schoenherr et al., 2015). In this study, screening questions were used to select participants who worked in organizations which had an information security password policy, and who were aware of the requirements of the password policy. Some researchers argue that because they have access to a broad population, samples obtained from internet-based survey research firms such as Qualtrics are more representative than samples from alternative sources such as professional organizations (Hays et al., 2015;

Schoenherr et al., 2015). Due to the ability to obtain a diverse, representative sample using specific selection criteria provided to Qualtrics, as well as the time savings involved, the use of this online-based sample selection approach was deemed appropriate for this study.

Sample

Qualtrics randomly selected the actual sample from its formed sample frame. A sample is a subset of participants drawn from a target population (Martinez-Mesa, González-Chica, Duquia, Bonamigo, & Bastos, 2016). The choice of a sampling technique for a study is important, as the internal and external validity of the study depend on the ability of the sample to address the research needs (Lobo et al., 2015). Two main types of sampling are probability and non-probability sampling.

Probability sampling was used in this study. Probability sampling involves the random selection of participants from a sample frame such that there is an equal probability of selecting any individual (El-Masri, 2017). A sampling frame refers to a subset of the target population that is available to researchers. The sampling frame for this study consisted of the list of individuals in the Qualtrics database who were eligible to participate in the study. For example, assume that Qualtrics has 6 million members in its participant database. Also, assume that 500,000 members satisfied the selection criteria for this study. These 500,000 individuals constituted the sample frame (i.e., a list of email addresses) from which Qualtrics drew a random sample. The actual sample for this study is described in detail in Section 3.

Probability sampling techniques include simple random sampling, stratified random sampling, systematic random sampling, and cluster random sampling. In simple random sampling, there is a random selection of participants from a uniform population. In this study, invitation emails were sent to a random sample of employees drawn from the sample frame of qualified members in the Qualtrics database. Probability sampling is beneficial because it yields samples which are representative of the target population, and results from studies using probability sampling are generalizable to the underlying population (Catania, Dolcini, Orellana, & Narayanan, 2015; Martinez-Mesa et al., 2016). One possible drawback with probability sampling is high cost compared to non-probability approaches (Catania et al., 2015). In this study, Qualtrics was responsible for performing the probability sampling at no extra cost. Furthermore, it can be argued that the time-saving benefit of using a market research firm such as Qualtrics outweighs the cost.

Although I adopted probability sampling for this study, I considered other non-probability techniques. Non-probability sampling is an approach in which the researcher selects a sample based on specific inclusion criteria. In non-probability sampling, not all members of the population have the same chance of being selected in the sample (Catania et al., 2015; Martinez-Mesa et al., 2016). Non-probabilistic samples are useful for some research objectives, based on the nature of the research questions (Haegele & Hodge, 2015; Martinez-Mesa et al., 2016). Researchers may favor non-probability sampling because it is more cost-effective than probability-based sampling methods (Catania et al., 2015). However, the disadvantages of non-probability sampling include low

representativeness and generalizability (Catania et al., 2015; Martinez-Mesa et al., 2016). Because all individuals in the population do not have an equal chance of being included in the sample, non-probability samples may not be representative of the population from which they are drawn. Types of non-probability sampling include purposive sampling and convenience sampling (Haegele & Hodge, 2015; Martinez-Mesa et al., 2016).

Purposive sampling is useful when researchers need to target a select group of participants based on specific inclusion criteria. Purposive sampling allows an investigator to select attributes of interest in a population and obtain participants who have those attributes (Barratt, Ferris, & Lenton, 2015; Haegele & Hodge, 2015). Purposeful sampling is also a proper sampling technique when a diverse sample is needed (Martinez-Mesa et al., 2016).

Convenience sampling is a non-probability sampling technique where participants are selected because they are readily available for a study (Haegele & Hodge, 2015; Peterson & Merunka, 2014). In this approach, sample selection is based primarily on participant availability. Convenience sampling is appealing because of its low cost. However, a significant flaw with convenience samples is that they are often not representative of the population (Martinez-Mesa et al., 2016) and sample bias is typical with such samples (Haegele & Hodge, 2015). Considering these drawbacks such as the non-probability nature and non-representative nature of convenience samples, I chose not to use a convenience sample.

Sample Size

Determination of the sample size appropriate for a study can be achieved by performing an a-priori power analysis using v 3.9 of G*power (Faul, Erdfelder, Buchner, & Lang, 2009; Fugard & Potts, 2015). My multiple linear regression model involved three latent predictor variables. However, these three latent or composite variables were projected from 16 underlying measurable variables using a summative index. Therefore, the model of interest for performing the G*power analysis was a linear multiple regression model with an alpha of 0.05 for testing the corresponding model H0 and H1. Figure 3 below shows results of G*power analyses. For input parameters, a one-tailed test was chosen because it is appropriate for a non-directional hypothesis such as the hypothesis for this study. The coefficient of determination, R^2, is often used as an estimate of effect size in a regression model (Faul et al., 2009). I used an R^2 value of 0.3, which is a medium effect size (Faul et al., 2009). A power level (1 – β err prob) of 0.95 was deemed adequate for the sample size determination analyses, as a power level above 0.80 is often considered acceptable (Dijkstra & Henseler, 2015). Figure 4 shows sample size as a function of achieved power.

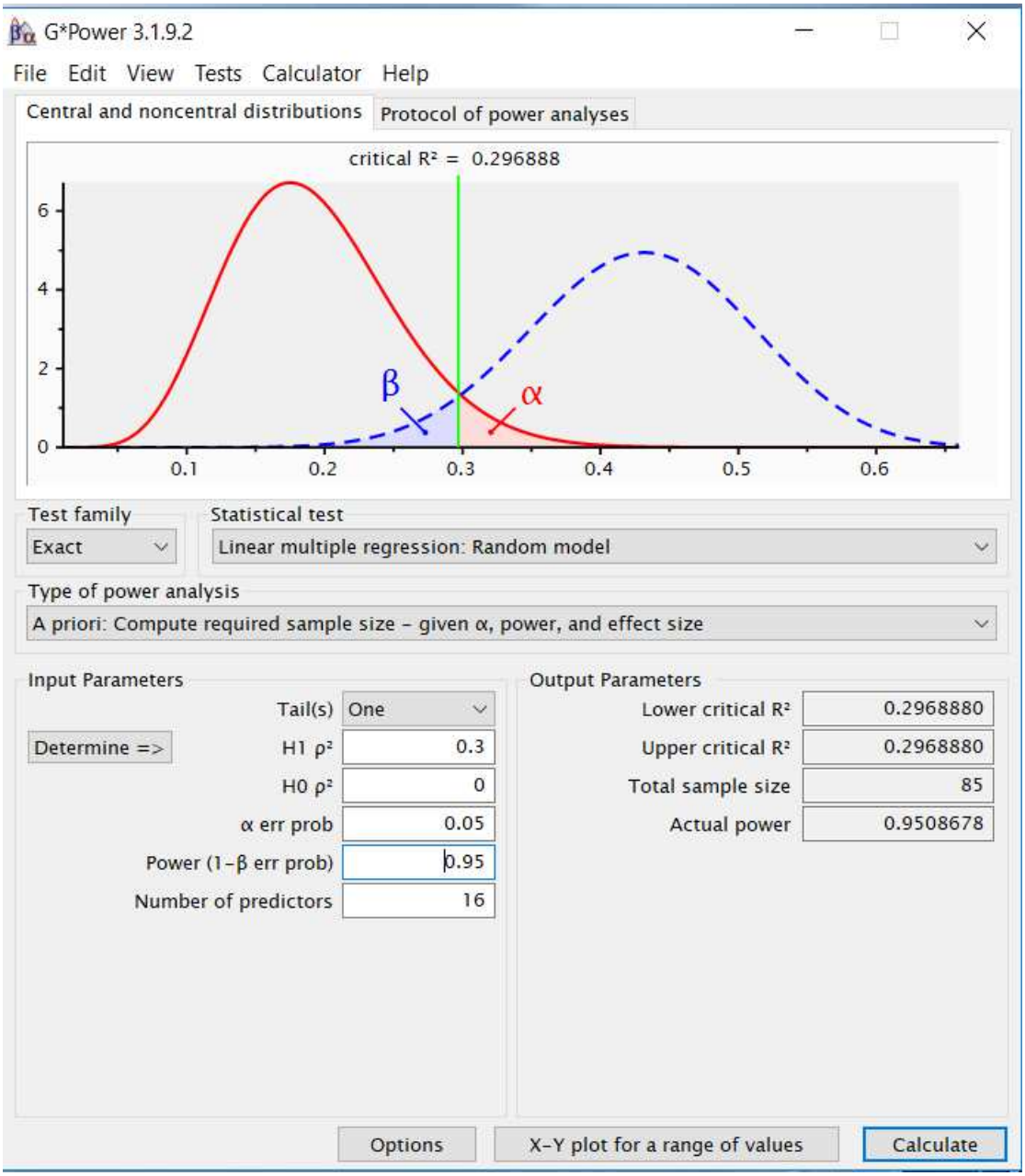

Figure 3. Sample size determination using G*Power software.

Based on the selection to achieve a power of 0.95 with $a = 0.05$, a sample size of 85 participants was indicated (Figure 3). Therefore, I intended to use at least 85 participants for this study. Figure 4 shows sample size as a function of power.

My survey was executed by Qualtrics, which was solely be responsible to deliver to me at least 85 completed surveys. Thus, response rate assumptions needed to calculate the number of survey invitations was inconsequential to my sample size determination.

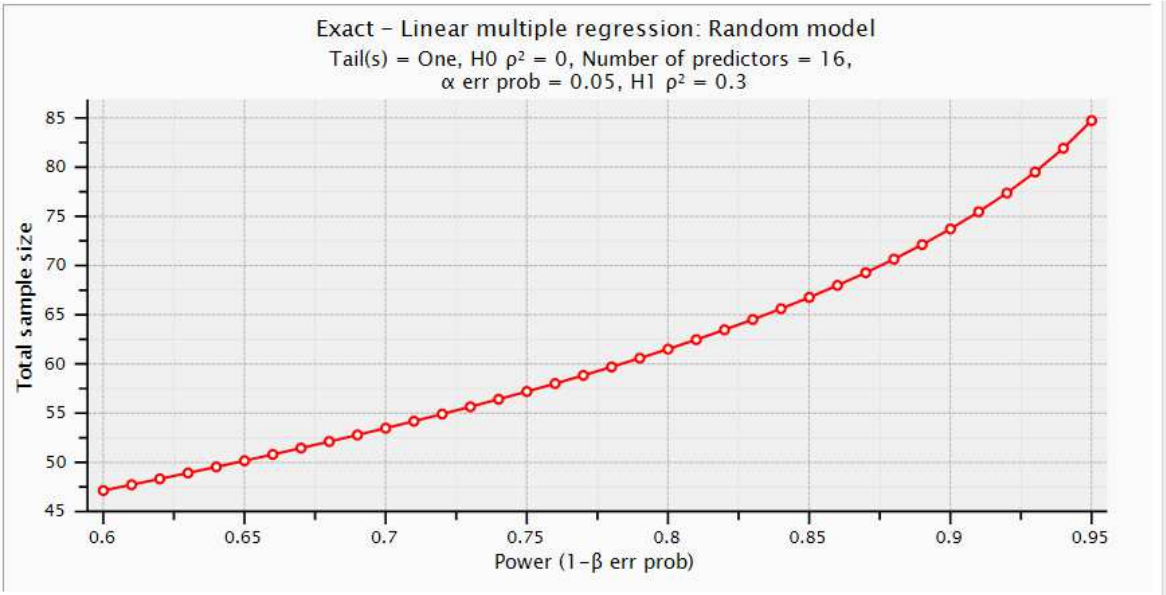

Figure 4. Power as a function of sample size.

Ethical Research

Any research involving human subjects should include a consideration of ethical rules and standards. The training of researchers in ethical practices is an essential step in ensuring ethical research (Gotterbarn et al., 2018; Spurlin & Garven, 2016). I completed training in the protection of human research participants provided by the National Institutes of Health Office of Extramural Research. Protection of participants includes elements such as ensuring freewill participation, informed consent, maintaining privacy and anonymity.

Researchers must ensure that participants in a study provide fully informed consent (Antonacopoulos & Serin, 2016). Valid informed consent involves participants'

receiving information about the purpose of the study, understanding the requirements for participation, and voluntarily agreeing to participate (Bromwich & Rid, 2015). Participants in this study were presented with an informed consent form, and I sought their informed consent. The informed consent form included information on the purpose of the study and assurance of confidentiality of all information provided by participants. Participants were required to sign the informed consent form before taking part in the study. Participants also had the option to terminate their freewill participation or withdraw from the study at any time. Qualtrics compensated participants who completed the survey, using a point-based system redeemable in the form of cash, airline miles, gift cards, or vouchers. To maintain the anonymity of participants, personally identifiable information such as names of participants or names of employers was not collected. All data collected will be stored on an encrypted disk which will be locked in a secure cabinet and maintained for five years. This study has been approved by the institutional review board of Walden University (IRB Approval number 12-05-18- 0563957).

Data Collection

For data collection, I used a survey instrument. I used items from an existing survey that has demonstrated reliability and validity (Bulgurcu et al., 2010). I performed data collection in an online format through Qualtrics, a third-party marketing research company. Data were analyzed using SPSS version 25.0 (IBM Corp, 2017)

Instrument

I used a survey instrument by Bulgurcu et al. (2010) with the author's permission (see Appendix D). The authors used the original survey in a study which focused on

assessing employees' information security policy compliance based on the theory of planned behavior. The original instrument measured 15 latent variables using 61 items (Bulgurcu et al., 2010). In this study, I quantified the relationships between three latent predictor variables and one latent outcome variable. I used 16 items from the survey by Bulgurcu et al. (2010) to measure four latent variables: information security awareness, password self-efficacy, attitude towards compliance, and intention to comply with information security password policies. Items 1-6 were used to measure employees' information security awareness. Item 7-9 measured password self-efficacy. Items 10-13 measured attitudes towards password policies. Items 14-16 measured intention to comply with password policies. Some survey items were slightly revised to better align with the purpose of this study. Specifically, the words "information security policy" were replaced with "password policy." Such a minor revision did not affect the validity of the survey instrument. Table 3 below shows the survey instrument.

Table 3

Survey Instrument

1. Overall, I am aware of potential security threats and their negative consequences.
2. I have sufficient knowledge about the cost of potential security problems.
3. I understand the concerns regarding information security and the risks they pose in general.
4. I know the rules and regulations prescribed by the IS Password Policy of my organization.
5. I understand the rules and regulations prescribed by the IS Password Policy of my organization.
6. I know my responsibilities as prescribed in the IS Password Policy to enhance the IS security of my organization.
7. I have the necessary skills to fulfill the requirements of the IS Password Policy.
8. I have the necessary knowledge to fulfill the requirements of the IS Password Policy
9. I have the necessary competencies to fulfill the requirements of the IS Password Policy
10. To me, complying with the requirements of the IS Password Policy is __ unnecessary…necessary
11. To me, complying with the requirements of the IS Password Policy is _____ unbeneficial…beneficial
12. To me, complying with the requirements of the IS Password Policy is ___unimportant…important
13. To me, complying with the requirements of the IS Password Policy is _____ useless…useful
14. I intend to comply with the requirements of the IS Password Policy of my organization in the future.
15. I intend to protect information and technology resources according to the requirements of the IS Password Policy of my organization in the future.
16. I intend to carry out my responsibilities prescribed in the IS Password Policy of my organization when I use information and technology in the future.

Scoring. The survey used a 1 to 7 Likert scale for all items. A Likert scale is a widely used ordinal scale which is divided into points or response categories associated with numeric values (Wu & Leung, 2017). Likert scales often use four to seven points, typically five points to capture neutrality (Wu & Leung, 2017). Table 4 shows a summary of the latent variables under study, the survey items used to measure them, and the scales used for each variable.

Table 4

Constructs and Corresponding Measurement Scales

Construct	Items	Scale
Information Security Awareness	1-6	1 = Not at all – 7 = very much
Password Self-Efficacy	7-9	1 = Almost Never – 7 = Almost Always
Attitude towards Policy Compliance	10-13	1 = Extremely Unnecessary – 7 = Extremely Necessary
Intention to Comply	14-16	1 = Strongly Disagree – 7 = Strongly Agree

The variables in this study were latent or composite by nature. A latent variable is an unobservable variable which can be quantified using several underlying observable variables (Bartolucci et al., 2018; Willaby, Costa, Burns, MacCann, & Roberts, 2015). Variable scoring will be done using a simple summative index method. In this approach, the score for each latent variable is obtained by summing the unweighted scores for all the underlying measurable variables used to quantify the latent variable (Willaby et al., 2015). For example, as per Table 4, items 1 through 6 were used to measure the information security awareness variable X1 that was fed to the regression model. To obtain the score for variable X1, I used equation (3) below:

$$X1 = I1 + I2 + I3 + I4 + I5 + I6 \quad (4)$$

Reliability and Validity. Reliability and validity of this instrument have been demonstrated previously (Bulgurcu et al., 2010). The authors assessed individual item reliability, composite reliability, convergent validity, and discriminant validity of the instrument. The reliability of an instrument refers to how consistent it is in its measurements (Korkmaz, Çakir, & Ozden, 2017). Researchers can measure reliability by evaluating homogeneity, stability, and equivalence. Cronbach's alpha is a commonly used measure of internal consistency of an instrument (Korkmaz et al., 2017). The validity of a survey instrument is the extent to which the instrument accurately measures the concept it was designed to measure (Korkmaz et al., 2017). Types of validity include content validity, construct validity, and criterion validity (Korkmaz et al., 2017; Larinkari et al., 2016).

To assess individual item reliability, Bulgurcu et al. (2010) examined factor loadings of individual measures as well as average variance extracted. All item loadings on constructs were above 0.707, which indicates that 50 percent or more of the variance in the item was shared with the construct (Bulgurcu et al., 2010). Furthermore, the authors used Cronbach's alpha analyses to test for scale reliability. Cronbach's alpha values for all constructs were higher than 0.88. Composite reliability was used to confirm the reliability of the scale. Composite reliability is an approach which uses structural equation modeling, and it is determined by dividing true score variance by observed score variance (McNeish, 2017; Padilla & Divers, 2016). Composite reliability and Cronbach's alpha values of 0.7 or more are viewed as acceptable (McNeish, 2017). Composite

reliability values for all the constructs in this instrument were above 0.90 (Bulgurcu et al., 2010).

Bulgurcu et al. (2010) also assessed the convergent validity and discriminant validity of the survey instrument. The authors evaluated convergent validity for this instrument by calculating the average variance extracted (AVE). For all study constructs, the AVE was higher than 0.5 which is the minimum value recommended (Bulgurcu et al., 2010). To assess discriminant validity, the authors performed confirmatory factor analyses and examined the cross-loadings of the items on constructs. All items had loadings above 0.78 on their intended constructs, and items loadings were less by at least 0.1 on other constructs (Bulgurcu et al., 2010).

Data Collection Technique

A cross-sectional survey design administered using the survey in Table 3 was used to collect data in this study. By definition, a cross-sectional survey is one that involves a cross-section or randomly selected and representative sample of participants (Fortin et al., 2014; Sedgwick, 2014). I chose this design due to the need to satisfy the random sample assumption of linear regression (Bun & Harrison, 2018). Qualtrics, a professional research firm, will administer the survey in a web-based format. Surveys are an appropriate research method when researchers study the relationships between variables (Connelly, 2016). The cross-sectional survey design is commonly used in social science research to collect data on behaviors, intentions, and attitudes (Connelly, 2016; Sedgwick, 2014). Cross-sectional surveys capture data from a representative

population sample at a single point in time, providing a snapshot of the variables under study (Schoenherr et al., 2015; Sedgwick, 2014).

The survey instrument for this study was uploaded to the Qualtrics internet-based survey tool. For a list of survey instructions and questions, see Appendix C. Qualtrics invited participants from its database who satisfied the selection criteria to take part in the study. A pilot study was not necessary for this study because I used a survey instrument which had previously been shown to demonstrate adequate validity and reliability (Bulgurcu et al., 2010). Once the required number of completed surveys was obtained, I transferred the data securely to the SPSS application for analysis.

The use of an Internet-based cross-sectional survey has several advantages. Cross-sectional surveys are relatively inexpensive compared to other survey types such as longitudinal surveys (Connelly, 2016). Cross-sectional surveys require less time and have lower attrition rates (Connelly, 2016). Also, due to the anonymity and privacy offered by this survey approach, internet-based surveys are a good option when dealing with sensitive topics such as information security compliance (Cope, 2014). Moreover, Internet-based surveys can access large, geographically diverse samples which can be selected using specific criteria (Cope, 2014).

Data Organization Techniques

The web-based data collection process through Qualtrics was monitored daily for completion. Once Qualtrics obtained the required number of responses, I securely transferred the data to the SPSS software package for analysis. All data collected for the

study will be stored in an encrypted disk and locked in a cabinet for five years, after which the data will be destroyed using standard data destruction procedures.

Data Analysis Technique

The research question for this study was as follows: What is the relationship between employees' attitudes towards information system password policies, employees' information security awareness, employees' password self-efficacy, and employees' intentions to comply with password policies? I tested the following hypotheses in this study:

$H_0$1: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' overall intentions to comply with password policies.

$H_1$1: There is a statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' overall intentions to comply with password policies.

$H_0$2: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply by protecting information and technology resource according to the password policy.

$H_1$2: There is a statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply by protecting information and technology resource according to the password policy.

$H_0$3: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply intention to comply by carrying out their responsibilities prescribed in the password policy.

$H_1$3: There is a statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intention to comply by carrying out their responsibilities prescribed in the password policy.

In this subsection, I explain the appropriateness of linear regression for this quantitative study and outline the required steps to execute the regression using SPSS.

Regression Methodology Background

Data analysis was performed using SPSS software. Data were analyzed using ordinal logistic regression, an inferential statistical technique. Inferential statistics enable researchers to make inferences about population parameters based on sample statistics (Gibbs, Shafer, & Dufur, 2015). Commonly used statistical inferences include *p*-values and confidence intervals (Gibbs et al., 2015). Inferential statistics can also be used to investigate the association between variables and to make predictions (Wagner, Goodin,

& Hammond, 2017). Associations between variables can be studied using techniques such as linear correlation, while predictions can be made using techniques such as linear regression (Chiou, Yang, & Chen, 2016; Hopkins & Ferguson, 2014).

Multiple linear regression was deemed the most appropriate approach for this study because it aligns with the research question. In this study, three predictor variables (employees' information security awareness, password self-efficacy, and attitudes towards password policies) were used to assess employees' intentions to comply with password policies. Multiple linear regression is appropriate when two or more predictor variables affect a dependent or outcome variable (Constantin, 2017). In multiple regression analyses, researchers estimate the influence of independent variables on a dependent variable while keeping other independent variables constant (Woodside, 2013). Such analyses focus on whether specific independent variables have a significant or non-significant net effect on a dependent variable in the presence or absence of other independent variables (Woodside, 2013). I used the regression model shown in equation (4) below. In this equation, the index "i" represents the ith observation.

$$Yi = b_0 + b_1X_{1i} + b_2X_{2i} + b_3X_{3i} + e_i \quad (5)$$

where Y = predicted score for employees' intention to comply with password policies,

b_0 = y-intercept of the regression line,

b_1 = change in Y per unit change in X_1 (information security awareness),

b_2 = change in Y per unit change in X_2 (password self-efficacy),

b_3 = change in Y per unit change in X_3 (attitude towards compliance)

e = error term.

Regression analysis is based on certain general assumptions. These include the assumptions of linearity, normality, homoscedasticity, and independence of errors. Following is a discussion of these assumptions.

Linearity Assumption. According to the assumption of linearity, there should be a linear relationship between the response variable and each predictor variable (Constantin, 2017; Hopkins & Ferguson, 2014). The response variable should be a linear function of the predictor variable. Williams, Gomez Grajales, & Kurkiewicz (2013) assert that a linear relationship between the response variable and the parameters (b1, b2, b3) is sufficient to satisfy this assumption. Violation of this assumption may affect the calculated coefficients negatively, which would lead to faulty conclusions about the relationships between the variables under study (Williams et al., 2013).

Normality Assumption. This assumption stipulates that errors associated with values of the predictor variables should have a normal distribution. Errors refer to the difference between values observed for the response variable and the values for the population predicted by the regression model (Williams et al., 2013). When there is a non-normal distribution of errors, the ability to make inferences about population parameters based on sample statistics is negatively affected (Williams et al., 2013). Violation of the normality assumption has a more significant effect when the sample size is small. Bootstrapping techniques can be used to improve the ability to make inferences in small samples with non-normal errors (Williams et al., 2013).

Homoscedasticity Assumption. Errors should be constant across the predictor variables (Constantin, 2017; Hopkins & Ferguson, 2014). Also known as the

homogeneity of variance assumption, violations of this assumption will result in unreliable population inferences. The homoscedasticity assumption can be violated due to outliers in a dataset, omitted variables, or when the model equation is not specified correctly (Klein, Gerhard, Buchner, Diestel, & Schermelleh-Engel, 2016). One way to detect homoscedasticity is by plotting standardized residuals against standardized predicted values of the response variable (Constantin, 2017). Homoscedasticity can also be detected using statistical tests such as the Levene test (Rosopa, Schaffer, & Schroeder, 2013) or the White test (Klein et al., 2016) available in SPSS.

Multicollinearity Assumption. The assumption here is that there are no correlations between the predictor variables in the regression model (Bedeian, 2014). Collinearity exists if there is a correlation between two predictor variables, while multicollinearity exists if there are relationships amongst three or more predictor variables (Williams et al., 2013). The presence of multicollinearity in a regression model can lead to an increase in Type I error (Bedeian, 2014). One approach for detecting multicollinearity is by calculating the variance inflation factor (VIF). A VIF higher than 10 is an indication of the presence of multicollinearity (Slade, Williams, Dwivedi, & Piercy, 2015). The VIF can be calculated using SPSS.

Regression Analysis Steps

I performed multiple linear regression analyses in SPSS using the steps listed below.

1. Imported Excel data from Qualtrics into SPSS.
2. Analyzed descriptive statistics and remove outliers if present.

3. Created composite variables using the TRANSFORM function in SPSS.
4. Tested instrument reliability using Cronbach's alpha.
5. Tested instrument validity using Correlation and Average Variance Extracted analyses.
6. Tested the assumptions of collinearity, linearity, and homoscedasticity.
7. Applied multiple linear regression on the transformed variables and the response variable.
8. Tested the assumption of residual error normality using PP-Plots.
9. Interpreted the results and decide whether to reject or fail to reject the null hypothesis, H0.

Reliability and Validity

Reliability

The reliability of a survey instrument refers to the extent to which the instrument is measuring the same thing consistently, and the measurements are reproducible (McNeish, 2017). I adapted survey items from a survey instrument that has been tested previously for reliability and validity (Bulgurcu et al., 2010). The authors performed two rounds of pilot testing during which preliminary adjustments were made to items (Bulgurcu et al., 2010). To test for individual item reliability, Bulgurcu et al. (2010) examined factor loadings of measurement items on their respective constructs. The authors reported that all item loadings on their underlying constructs were above 0.70. This result indicates that each measurement item shared at least 50 percent of its variance with the underlying construct (Bulgurcu et al., 2010). Also, the authors used Cronbach’s

alpha analyses to test for scale reliability. Cronbach's alpha values for all constructs were higher than 0.88. Composite reliability was used to confirm the reliability of the scale. Composite reliability is an approach which uses structural equation modeling, and it is determined by dividing true score variance by observed score variance (McNeish, 2017; Padilla & Divers, 2016). Composite reliability and Cronbach's alpha values of 0.7 or more are considered acceptable (McNeish, 2017). Composite reliability values for all the constructs in this instrument were above 0.90 (Bulgurcu et al., 2010).

Validity

Threats to the validity of a study can be internal or external. Internal validity refers to the extent to which one can make inferences about causal relationships between variables in the study (Torre & Picho, 2016). In general, internal validity applies to experimental or quasi-experimental studies (Torre & Picho, 2016). This study did not use an experimental design, so threats to internal validity was not an issue. External validity threats include threats that may affect the degree to which study outcomes are generalizable (Torre & Picho, 2016). These include statistical conclusion validity and issues related to sample selection.

Statistical conclusion validity is an important component of the validity of a study. Statistical conclusion validity is related to the extent to which appropriate statistical approaches are used, and study conclusions align with data (Anestis, Anestis, Zawilinski, Hopkins, & Lilienfeld, 2014). One method used to mitigate threats to statistical conclusion validity in this study is the choice of study design. As discussed in the "Data Analysis" section above, ordinal logistic regression, an approach which is well

suited for quantifying relationships between variables and which aligns well with the research question, was used for data analysis. I sought to reduce statistical conclusion validity threats by ensuring that the data assumptions for ordinal regression were not violated using techniques such as statistical tests for multicollinearity and proportional odds (Slade et al., 2015; Williams et al., 2013). The validity and reliability of instruments used in a study can also affect conclusion validity (Flores et al., 2014). As discussed in the section “Data Collection," an instrument that has been tested previously and demonstrated reliability and validity will be used for this study.

The sample size is another important factor which can affect the generalization of study outcomes. An a priori power analysis was conducted in this study to determine an appropriate sample size (Faul et al., 2009; Fugard & Potts, 2015), thus reducing the threat to the external validity of the study. Details of sample size determination were provided under "Population and Sampling" above.

Transition and Summary

Section 2 covered areas of the study such as the role of the researcher, a description of the participants, the research method and design. The target population for the study and sampling approach were discussed, including ethical issues that I considered during the study. Also, this section included a discussion of the data collection and data analyses techniques. Finally, I discussed threats to reliability and validity and presented measures to reduce such threats. Section 3 of this study includes an overview of the study, presentation, and discussion of findings, applications to professional

practice, and implication for social change. Section III concludes with recommendations for action and further research.

Section 3: Application to Professional Practice and Implications for Change

In Section 3 I present the findings of the study and discuss how they are applicable to the practice of information technology. I also discuss the implications of this study to social change and make recommendations for further action. This section concludes with some personal reflections.

Overview of the Study

The purpose of this quantitative correlational design study was to quantify the relationship between employees' attitudes towards password policies, information security awareness, and password self-efficacy, and employee intentions to comply with password policies. The independent variables were employees' (a) attitudes towards password policies, (b) information security awareness, and (c) password self-efficacy. The dependent variable was employees' intention to comply with password policies. The three independent variables are constructs or latent variables that were operationalized from composite scores of participants' responses to survey items.

Presentation of Findings

I collected data from December 14, 2018, to December 16, 2018, using an online survey through Qualtrics. The sample included employees from diverse economic sectors including health care, education, information technology, manufacturing, and retail/wholesale, among others. A total of 432 people participated in the survey. Of these participants, 233 were screened out for not meeting the eligibility criteria. There were 199 completed surveys. The first step I performed was to clean the data. I checked the data for incomplete responses. I eliminated one participant for incomplete responses.

Next, I checked for speeders, which are participants who completed the survey in a very short time. Nine responses were removed for completing the survey in under 90 seconds. Furthermore, two entries were eliminated because they chose the same Likert scale option for all survey questions. A total of 187 valid responses were retained. I imported the data into SPSS for analyses.

Table 5 shows the descriptive statistics. Variables ISA1 through ISA6 represent questions/responses measuring information security awareness, PSE1 through PSE3 represent questions/responses measuring password self-efficacy, ATC1 through ATC4 represent questions/responses measuring attitude towards password policies, and IC1 through IC3 represent questions/responses measuring intention to comply with password policies. The relatively high means and medians could be expected due to the self-reported nature of the data. The coefficient of variation or CV is computed as a percentage of the ratio standard deviation/mean and represents the degree of spread in the response data. The spread in each variable was less than 21% across all variables indicating responses that were very close around each mean. Because all questions are in the same units (because the same Likert scale was used), this indicates that all survey responses have low variability or a high degree of consistency across the responders.

Table 5

Descriptive Statistics

Survey item	Variable	*n*	*M*	*Mdn*	*SD*	CV
1	ISA1	187	6.01	6	0.991	16.48%
2	ISA2	187	5.66	6	1.150	20.32%
3	ISA3	187	6.03	6	0.949	15.74%
4	ISA4	187	6.05	6	0.841	13.88%
5	ISA5	187	6.06	6	0.864	14.27%
6	ISA6	187	5.09	5	0.913	17.95%
7	PSE1	187	5.99	6	1.053	17.58%
8	PSE2	187	6.05	6	0.972	16.08%
9	PSE3	187	6.00	6	1.011	16.85%
10	ATC1	187	6.35	7	0.886	13.96%
11	ATC2	187	6.37	7	0.856	13.43%
12	ATC3	187	6.38	7	0.768	12.05%
13	ATC4	187	6.29	7	0.915	14.55%
14	IC1	187	6.50	7	0.796	12.24%
15	IC2	187	6.52	7	0.740	11.34%
16	IC3	187	6.46	7	0.765	11.84%

The next step I performed was to create composite scores for the variables. Four composite or summative index variables were created from the 16 variables shown in Table 5. The four variables were Information Security Awareness (ISA), Password Self-Efficacy (PSE), Attitude towards Compliance (ATC), and Intention to Comply (IC). I created composite variables by computing the sum of scores for each construct, as shown in Table 6. For example, the summative index variable for ISA was created by summing the six ISA variables. The resultant variable had a range of values between 6 and 42 (because there were six underlying variables, each with a score ranging from 1 to 7). With this transformation, the composite ISA variable could be treated as a continuous variable in any regression model including ordinal logistic regression.

Table 6

Composite Variables

Composite variable	Score computation
Information Security Awareness (ISA)	ISA1+ ISA2 + ISA3 + ISA4 + ISA5 + ISA6
Password Self-Efficacy (PSE)	PSE1 + PSE2 + PSE3
Attitude Towards Compliance (ATC)	ATC1 + ATC2 + ATC3 + ATC4
Intention to Comply (IC)	IC1 + IC2 + IC3

Instrument Reliability and Validity

The next step in the data analyses was to test for instrument reliability using Cronbach's alpha. I tested the reliability of instrument subscales for ISA, PSE, ATC, and IC using SPSS. Results of reliability analyses are shown in Table 7. All subscales showed reliability coefficients above the required minimum of .75, demonstrating high reliability.

Table 7

Reliability Coefficients for Subscales

Composite variable	Number of items	Cronbach's alpha
Information Security Awareness (ISA)	6	.88
Password Self-Efficacy (PSE)	3	.92
Attitude Towards Compliance (ATC)	4	.86
Intention to Comply (IC)	3	.89

I tested instrument validity using correlation analyses. For each composite variable, I analyzed the correlations among survey items that make up the composite variables. For example, for the composite variable ISA, I checked the inter-item correlations for items ISA1 through ISA6. Table 8 shows the results of the correlational

analyses. The inter-item correlations for all constructs were significant at the 0.001 level. The inter-item correlation coefficients were all above .40. This result indicated adequate convergent validity for all subscales.

Assumptions of Multiple Linear Regression

Normality. The normality assumption in multiple linear regression is an assumption that errors associated with values of the predictor variables should have a normal distribution. To test for this assumption, I examined the normal Predicted Probability (P-P) plot. When there is a normal distribution of errors, a P-P plot shows errors conforming to the diagonal line in the plot. Figure 5 shows the P-P plot of standardized residuals. There was some deviation from the normal line, so it was questionable whether the normality assumption was met in my dataset.

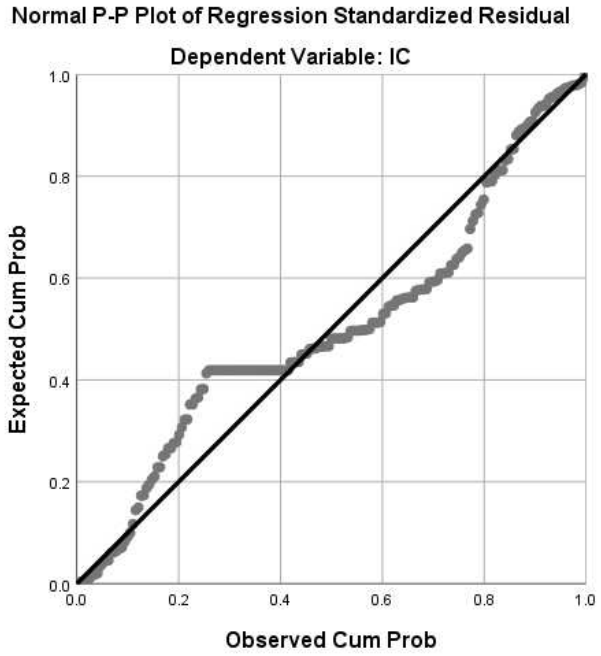

Figure 5. Normal P-P plot.

Table 8

Inter-Item Correlations for Study Constructs

Correlations

	ISA1	ISA2	ISA3	ISA4	ISA5	ISA6	PSE1	PSE2	PSE3	ATC1	ATC2	ATC3	ATC4	IC1	IC2	IC3
ISA1	1															
Sig.																
ISA2	.490**	1														
Sig.	0.000															
ISA3	.546**	.626**	1													
Sig.	0.000	0.000														
ISA4	.526**	.506**	.623**	1												
Sig.	0.000	0.000	0.000													
ISA5	.529**	.521**	.611**	.838**	1											
Sig.	0.000	0.000	0.000	0.000												
ISA6	.505**	.433**	.582**	.678**	.691**	1										
Sig.	0.000	0.000	0.000	0.000	0.000											
PSE1	.433**	.450**	.559**	.625**	.630**	.607**	1									
Sig.	0.000	0.000	0.000	0.000	0.000	0.000										
PSE2	.414**	.412**	.560**	.626**	.626**	.540**	.807**	1								
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000									
PSE3	.408**	.399**	.504**	.581**	.589**	.562**	.748**	.829**	1							
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000								
ATC1	.293**	.290**	.424**	.457**	.467**	.453**	.600**	.606**	.541**	1						
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000							
ATC2	.385**	.318**	.432**	.480**	.541**	.558**	.549**	.543**	.597**	.671**	1					
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000						
ATC3	.339**	.265**	.417**	.454**	.484**	.472**	.567**	.549**	.556**	.600**	.765**	1				
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000					
ATC4	.357**	.351**	.401**	.432**	.408**	.447**	.459**	.469**	.431**	.512**	.604**	.604**	1			
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000				
IC1	.389**	.278**	.495**	.502**	.464**	.529**	.557**	.555**	.566**	.652**	.734**	.612**	.556**	1		
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000			
IC2	.374**	.287**	.470**	.479**	.473**	.481**	.474**	.514**	.530**	.567**	.743**	.731**	.595**	.779**	1	
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000		
IC3	.315**	.252**	.458**	.484**	.503**	.529**	.547**	.523**	.520**	.582**	.664**	.699**	.557**	.708**	.757**	1
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	

To further verify normality, I ran a Shapiro-Wilk test for normality. For all three independent composite variables, the test statistic was significant (< .05) confirming that the assumption of normality was not met.

Multicollinearity. One of the assumptions of multiple linear regression is that there is no collinearity between the predictor variables. A test was performed to detect possible collinearity among the three composite predictor variables ISA, PSE, and ATC. Results of the test for collinearity are displayed in Table 9 below. The Variance Inflation Factor (VIF) for all three independent, composite variables is below 2.5. A VIF below and 10 indicates that there is no collinearity between variables. The assumption of no multicollinearity was met in my dataset.

Table 9

Test for Multicollinearity

	Collinearity Statistics	
Variable	Tolerance	VIF
ISA	0.483	2.072
PSE	0.401	2.491
ATC	0.505	1.982

Linearity. Another assumption of multiple linear regression is that there is a linear relationship between the dependent variable and each independent variable. To test the linearity assumption, I examined the correlations between the dependent composite variable (IC) and each independent variable. Table 10 shows the results of the correlation analyses. There was a positive correlation between intention to comply (IC) and each independent composite variable (information security awareness (ISA), password self-

efficacy (PSE), attitude towards compliance (ATC)) indicating a linear relationship between dependent and independent variables.

Table 10

Correlations between dependent and independent variables

Correlations

		IC	ISA	PSE	ATC
IC	Pearson Correlation	1			
	Sig. (2-tailed)	.000			
ISA	Pearson Correlation	.578**	1		
	Sig. (2-tailed)	.000	.000		
PSE	Pearson Correlation	.628**	.700**	1	
	Sig. (2-tailed)	.000	.000	.000	
ATC	Pearson Correlation	.826**	.599**	.683**	1
	Sig. (2-tailed)	.000	.000	.000	.000

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

To further investigate linearity, I examined scatterplots between the dependent variable and each independent variable. As shown in Figure 6, the relationship between IC and ISA was not linear, as there was some clustering of the datapoints. The relationship between IC and ATC was linear, as shown in Figure 7. The scatterplot for IC vs PSE also showed some clustering of the datapoints, indicating that the relationship between these two variables was not linear. In brief, results from the scatterplot analyses for linearity showed a linear relationship between IC and ATC, while the relationship between IC and the other independent variables was not linear. Hence, there was some violation of the linearity assumption.

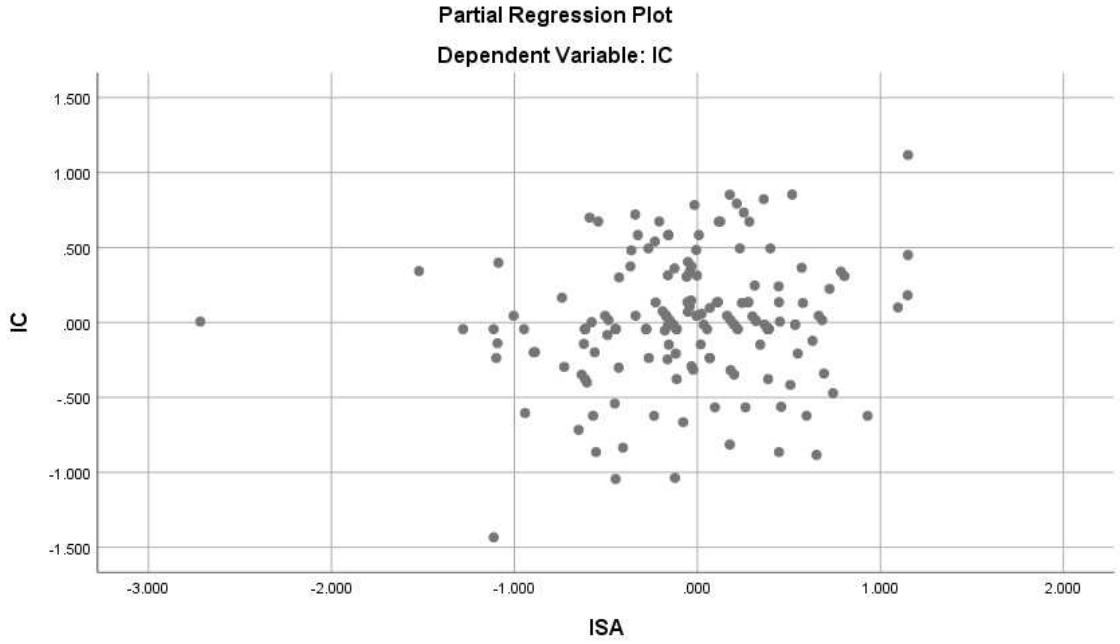

Figure 6. Scatter plot of Intention to Comply versus Information Security Awareness.

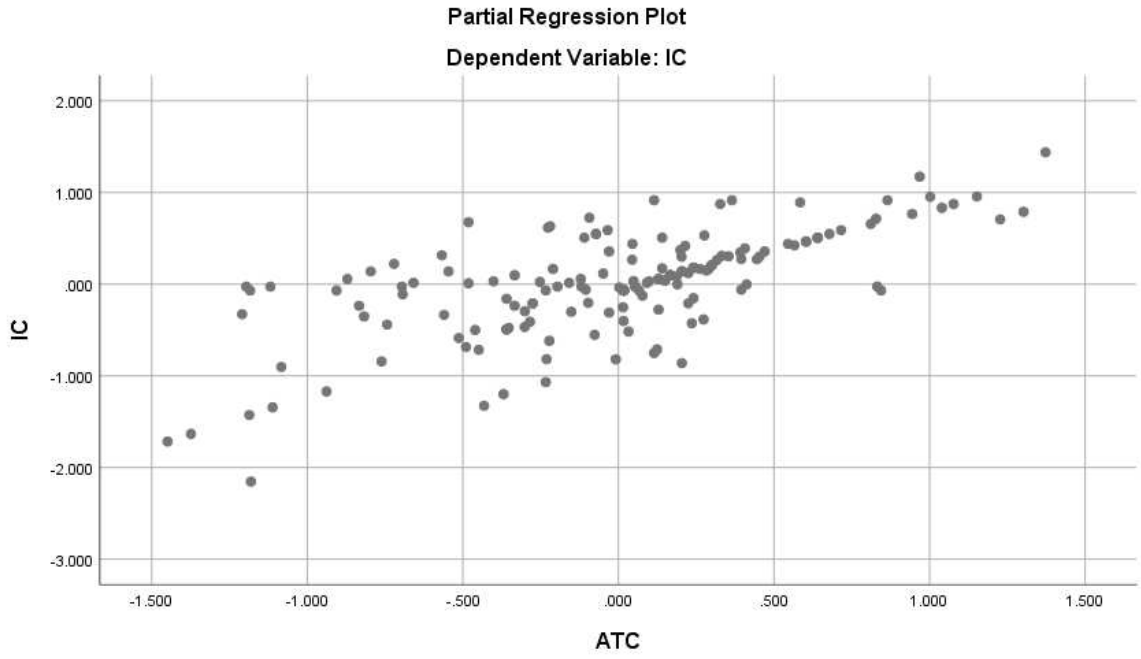

Figure 7. Scatterplot of Intention to Comply versus Attitude towards Compliance.

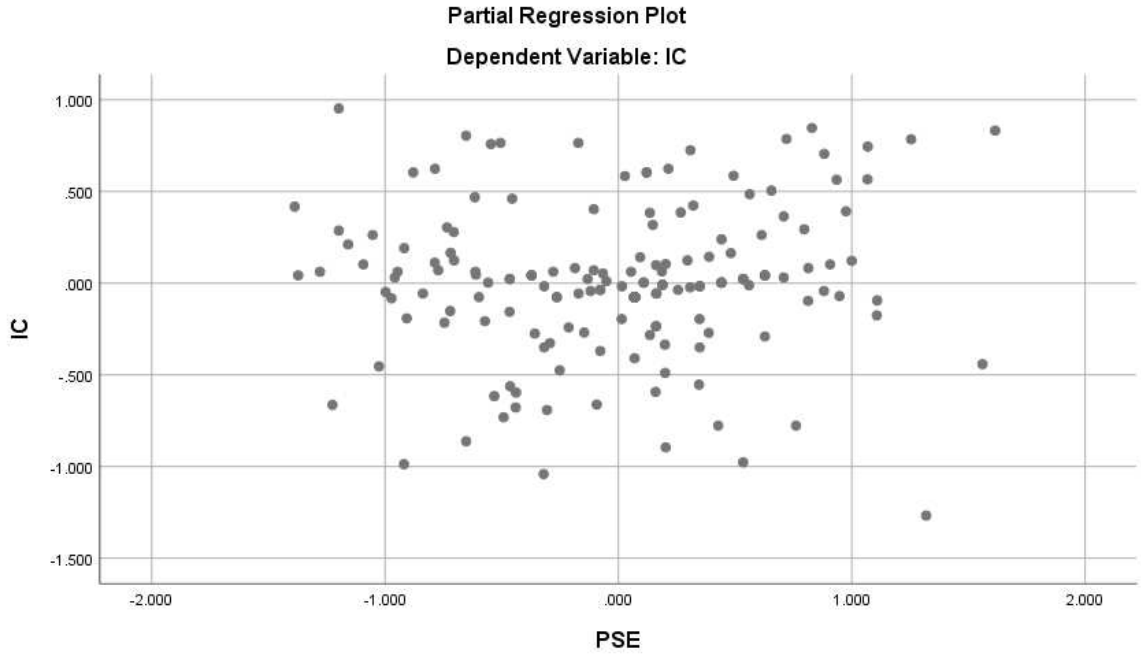

Figure 8. Scatterplot of Intention to Comply versus Password Self-Efficacy.

Homoscedasticity. The assumption of homoscedasticity requires that errors should be constant across the predictor variables (Constantin, 2017; Hopkins & Ferguson, 2014). I tested the assumption of homoscedasticity by plotting standardized residuals against standardized predicted values of the response variable in a scatterplot. Figure 9 displays the resultant scatterplot. There was indication that the errors were not uniformly distributed across the predictor variables as seen by the cone-shape of the plot. Furthermore, there was a clear pattern with linear clustering of datapoints. This suggested that the assumption of homoscedasticity was not met. A Levene's test for homogeneity of variance confirmed the violation of the assumption of homoscedasticity and the presence of heteroscedasticity ($p < .05$) (Rosopa, et al., 2013).

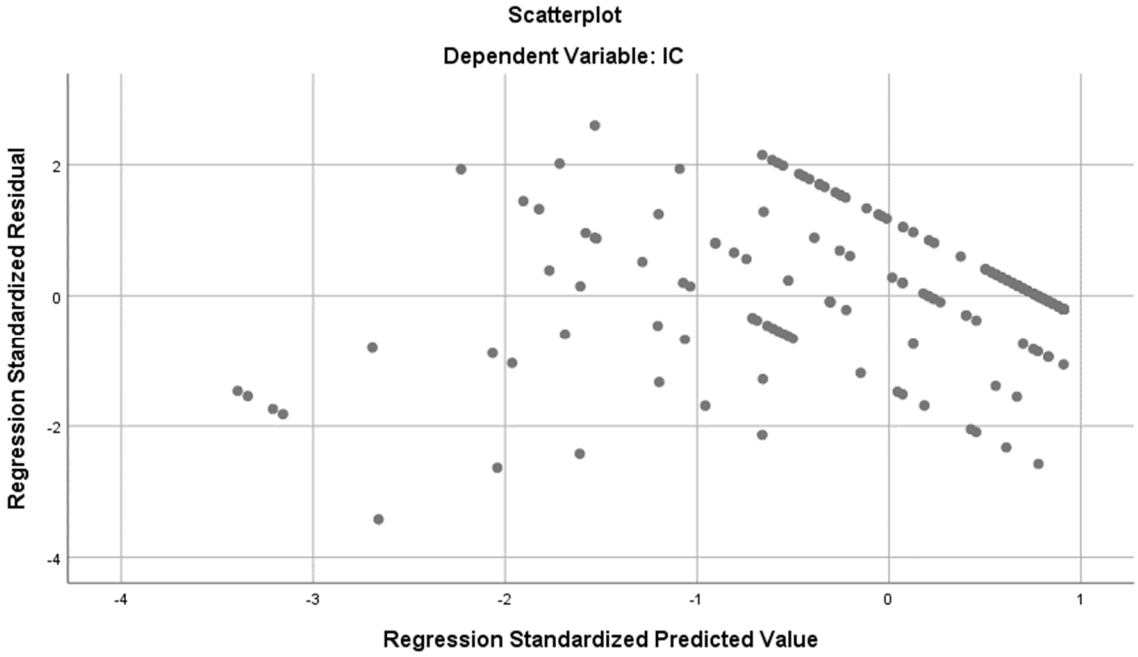

Figure 9. Scatterplot of standardized residuals and predicted values.

During the proposal phase of my study, I proposed to investigate the relationships between the independent variables and the dependent variable in my study using multiple linear regression. After collecting the data and testing the assumptions for multiple linear regression as discussed above, my dataset did not satisfy the assumptions of normality, linearity, and homoscedasticity. Therefore, I decided to use an alternate, more appropriate regression approach for my analysis.

Ordinary least squares regression (OLS), which is the basis of multiple linear regression, is the simplest regression model and assumes a linear relationship between variables under study (Constantin, 2017). It also assumes that both the dependent and independent variables are continuous. My dataset did not satisfy the linearity assumption, and the dependent variable was not continuous. In the case of ordinal logistic regression,

the independent variables can contain a mix of continuous and discrete variables. Also, the dependent response variable is discrete and ordered (ordinal). Discrete and ordered responses are common in Likert item responses (Hedeker, 2015). Table 11 shows linear regression approaches based on the nature of the independent and dependent variables. My dependent variable was discrete and ordered, so I considered ordinal logistic regression as best suited for my dataset. Ordinal logistic regression was, therefore, the specific linear regression model applied in this study.

Table 11

Linear Regression Approaches

Dependent Variable Y	**Independent Variable X1**	**Independent Variable X2**	**Linear Regression Approach**
Continuous	Continuous	Continuous	Ordinary Least Square Regression
Continuous	Continuous	Discrete	Categorical Regression
Discrete	Continuous	Discrete	Logistic Regression
Ordered Discrete	Continuous	Discrete	Ordinal Logistic Regression

Ordinal Logistic Regression analysis is based on certain general assumptions. These include the assumption of an ordinal outcome or independent variable, assumption of no multicollinearity, and assumption of proportional odds. Following is a discussion of the assumptions of ordinal logistic regression and how I tested my dataset for compliance with these assumptions.

Assumptions of Ordinal Logistic Regression

Ordinal logistic regression involves the use of the general linear model to predict a dependent variable based on one or more independent variables. In ordinal logistic regression, the dependent variable should be ordinal in nature while the independent variables can be nominal, ordinal, or continuous (Peng et al., 2002). Ordinal regression is based on four main assumptions: (a) the dependent variable should be measured at the ordinal level; (b) there should be one or more independent variables measured at the ordinal, nominal, or continuous level, and ordinal independent variables should be treated as either nominal or continuous; (c) there is no multicollinearity; and (d) there are proportional odds (Brown et al., 2015). In the next section, I test my dataset for compliance with these assumptions.

The assumption of ordinal-level outcome variable. One of the assumptions in ordinal logistic regression is that the dependent variable should be measured at the ordinal level or measurement. Ordinal logistic regression assumes that the errors associated with the outcome variable have a binomial distribution (Peng et al., 2002). When errors associated with the outcome variable do not have a binomial distribution, other approaches to linear regression such as ordinary least squares regression are more appropriate.

The outcome variable in this study was employee intention to comply with information security password policies. The outcome variable was measured using a seven-point Likert scale with responses ranging from *Strongly Disagree* to *Strongly*

Agree. The outcome variable was therefore measured at the ordinal level of measurement. The assumption of ordinal-level measurement for the outcome variable was met.

The assumption of continuous or categorical independent variables. Another assumption of ordinal logistic regression is that the independent or predictor variables are nominal or continuous (Bauer & Sterba, 2011). Ordinal regression may be used to analyze ordinal variables; however ordinal variables must be treated as nominal or continuous.

The independent variables for this study were employees' attitude towards password policy compliance, information security awareness, and password self-efficacy. Each of these composite variables was measured using a survey instrument with a Likert scale. Such data generated from a Likert scale is categorical (ordinal) in nature. Composite variables were created by computing the sum of scores for each construct, as shown in Table 7. For example, the summative index variable for ISA was created by summing the 6 ISA variables. The resultant variable had a range of values between 6 and 42 (since there were six underlying variables each with a score ranging from 1 to 7). With this transformation, the composite ISA variable could be treated as a continuous variable in the ordinal logistic regression model. Composite variables for PSE and ATC were created similarly and were treated as continuous variables in the regression model. During analysis, the data for the independent variables were treated as continuous. The assumption of continuous or categorical independent variables was met in the dataset for this study.

Multicollinearity assumption. The assumption here is that there are no correlations between the predictor variables in the regression model (Bedeian, 2014). Collinearity exists if there is a correlation between two predictor variables, while multicollinearity exists if there are relationships amongst three or more predictor variables (Williams et al., 2013). The presence of multicollinearity in a regression model can lead to an increase in Type I error (Bedeian, 2014). One approach for detecting multicollinearity is by calculating the variance inflation factor (VIF). A VIF higher than 10 is an indication of the presence of multicollinearity (Slade et al., 2015). The VIF can be calculated using SPSS.

A test was performed to detect possible collinearity among the three composite predictor variables ISA, PSE, and ATC with each being a continuous variable. Results of the test for collinearity are displayed in Table 12 below. The Variance Inflation Factor (VIF) for all three independent, composite variables is below 2.5. A VIF below 10 indicates that there is no collinearity between variables (Slade et al., 2015). Therefore, the dataset met the assumption of multicollinearity.

Table 12

Test for Multicollinearity

	Collinearity Statistics	
Variable	Tolerance	VIF
ISA	0.483	2.072
PSE	0.401	2.491
ATC	0.505	1.982

The assumption of proportional odds. Also called the assumption of parallel lines, the proportional odds assumption refers to the assumption that the effect of each covariate in

the set of independent variables would be the same across all combinations of the dichotomized outcome variable (Hedeker, 2015). Put in other terms, if the outcome variable Y has three categories and one ran two binary logistic regressions with dichotomized outcomes, the covariate effects would be the same for the two analyses. The proportional odds assumption is a foundational assumption in ordinal logistic regression (Williams, 2016).

I tested the assumption of proportional odds using the Test of Parallel Lines in SPSS. When the assumption of proportional odds is met, the difference in model fit (Chi-Square) is small and not statistically significant ($p > .05$). As shown in Table 13 below, the test for the assumption of proportional odds resulted in a Chi-square value of 13.995, $p = .981$. The Chi-square value was not statistically significant (i.e., p was greater than .05) indicating that the assumption of proportional odds was met.

Table 13

Test for Assumption of Proportional Odds

Test of Parallel Lines[a]

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Null Hypothesis	359.455			
General	345.461[b]	13.995[c]	27	.981

The null hypothesis states that the location parameters (slope coefficients) are the same across response categories.

a. Link function: Logit.

b. The Chi-Square statistic is computed based on the log-likelihood value of the last iteration of the general model. The validity of the test is uncertain.

Sample Size Determination for Ordinal Logistic Regression

Determination of the sample size appropriate for a study can be achieved by performing an a-priori power analysis using v 3.9 of G*power (Faul et al., 2009; Fugard & Potts, 2015). My multiple regression model involved three latent predictor variables. Therefore, the model of interest for performing the G*power analysis was a logistic regression model with an alpha of 0.02 for testing the corresponding model H_0 and H_1. Figure 3 below shows the results of G*power analyses. For input parameters, a one-tailed test was chosen because it is appropriate for a non-directional hypothesis such as the hypothesis for this study. A power level (1 – β err prob) of 0.80 was deemed adequate for the sample size determination analyses, as a power level of 0.80 or above is often considered acceptable (Dijkstra & Henseler, 2015).

Based on the selection to achieve a power of 0.80 with $a = 0.02$, a sample size of 123 participants was indicated (Figure 10). The power analyses above provided an estimation of sample size for logistic regression, but there is no standard method for a priori sample size estimations for ordinal logistic regression. For this study, I adopted the method in which the *ordinal* logistic regression sample size estimate is obtained by multiplying the logistic regression sample size by 1.5. As described above, G*Power analyses indicated a logistic regression sample size of 123. Therefore, the sample size estimate for ordinal logistic regression was 123 x 1.5 = 185.

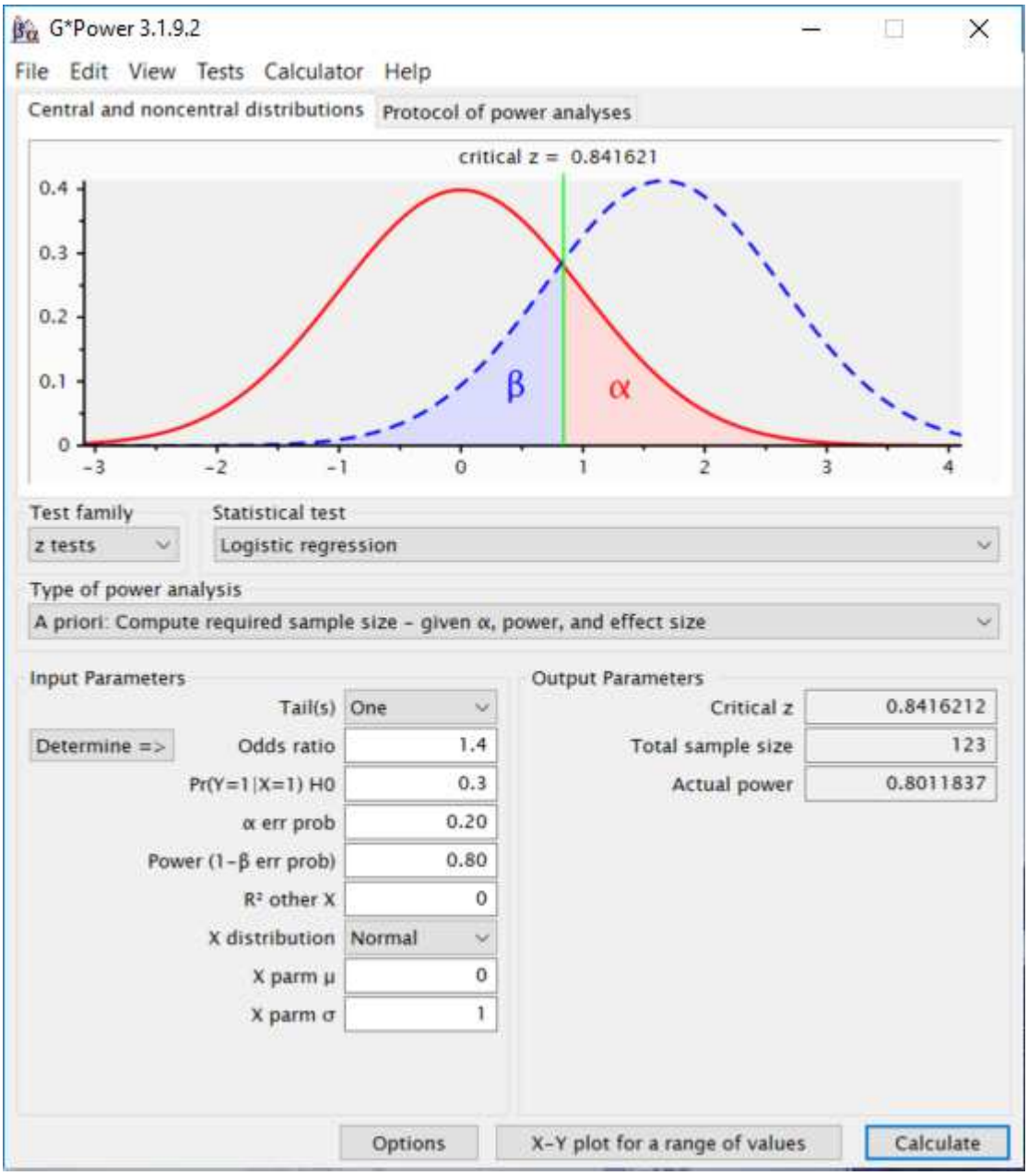

Figure 10. Sample size determination for ordinal logistic regression.

Another approach to sample size determination for logistic regression was suggested by Peduzzi, Concato, Kemper, Holford, and Feinstein (1996). In this approach, the minimum number of cases that should be included in regression analyses is given by the formula n = 10 x k / p, where k is the number of covariates (the number of continuous independent variables) in the model. For this study, I used a summative index to create three continuous composite variables from 16 underlying discrete variables. Details of how composite variables were created are provided under the subsection "Scoring" below. So for sample size determination for this study, k had a value of 3.

The term "p" in the equation above represents the lesser of the proportions of positive or negative cases in the sample. To obtain "p" we compare the proportion of cases which provide positive responses to the proportion of cases which provide negative responses and select the proportion that is less. In this study, participants provide responses based on a Likert scale ranging in scores from 1 = Strongly Disagree to 7 = Strongly Agree. Positive responses would be responses in the range 5 – 7, while negative responses would be responses in the range 1 – 4. Positive responses would indicate that participants have self-reported high scores in areas such as attitudes towards password policy compliance and password self-efficacy. I estimated that for this study, 75% of participants would provide positive responses (in the range 5 – 7), while 25% would provide negative responses (in the range 1 – 4). Therefore, I used a value of 0.25 which was the lesser proportion, for "p". Based on this approach, the minimum number of cases indicated for my logistic regression model was 120 (obtained by n =10 x 3 / 0.25). For my ordinal logistic regression model, I intended to use a sample size of 1.5 x 120 = 180.

This sample size is close to the sample size suggested by using the G*power analyses method above. Ordinal Logistic Regression

Ordinal logistic regression is used to predict an outcome variable, which is measured at the nominal or ordinal level, based on one or more predictor variables. In this study, the outcome or dependent variable is employees' intention to comply with password policies (IC). There are three such IC variables each measuring a different aspect of intention to comply: IC1, IC2, IC3. Each IC variable was run through an ordinal logistic regression model. Thus three independent ordinal logistic regression models were run and reported below. Instead of creating one composite dependent variable, each IC variable remained as an ordinal variable. This approach was chosen because if all the IC's were added into a single summative index variable, then we would essentially lose the nominal or ordered nature of the variable we are trying to assess. Another possible approach was to use the mean of the three IC variables as a single measure for intention to comply. However, using a mean score on Likert scale responses may not be meaningful, as a Likert scale is categorical in nature. Thus, three independent ordinal logistic regression runs were made.

Outcome variables IC1, IC2, and IC3 were measured using three survey items and a 7-point Likert scale using response options ranging from "Strongly Agree" to "Strongly Disagree." The three survey items measuring aspects of intention to comply were as follows: (a) I intend to comply with the requirements of the Information Security Password Policy of my organization in the future, denoted IC1; (b) I intend to protect information and technology resources according to the requirements of the Information

Security Password Policy of my organization in the future, denoted IC2; (c) I intend to carry out my responsibilities prescribed in the Information Security Password Policy of my organization when I use information and technology in the future, denoted IC3. For regression analyses, I created a separate regression model for outcome variables IC1, IC2, and IC3. In the following sections, I present the results obtained from running the three ordinal logistic regression models.

Model 1

I ran the first ordinal logistic regression to test the null hypothesis below:

$H_0$1: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' overall intentions to comply with password policies (IC1).

I tested by executing a number of SPSS steps. First, I checked for the overall goodness of fit for the model using the deviance statistic. Overall goodness of fit provides an indication of how well the dependent variable is predicted by the ordinal logistic regression model. The Deviance goodness of fit test measures the difference in the log likelihood between the predicted model and the actual model. If the Deviance statistic is statistically significant (i.e., if $p < .05$), that indicates a lack of fit in the observed model. Conversely, when there is adequate goodness of fit in the observed model the deviance statistic should not be statistically significant (i.e., p should be $> .05$). Similarly, the Pearson goodness of fit test indicates lack of fit when $p < .05$ and indicates goodness of fit when $p > .05$ (Hilvert-Bruce, Neill, Sjoblom, & Hamari, 2018).

Table 14 shows the results of the goodness of fit test statistics. The Deviance goodness of fit test indicated that the model was a good fit ($\chi^2(505) = 174.828$, $p > .05$). However, the Pearson goodness of fit test indicated that there was some lack of fit in the model ($\chi^2(505) = 559.495$, $p = .047$).

Table 14

Model Goodness of Fit

	Chi-square	df	Sig.
Pearson	559.495	505	.047
Deviance	174.828	505	1.000

Link function: Logit.

To further test goodness of fit, I examined the model fitting information from a Likelihood-ratio test shown in Table 15. The Likelihood ratio test statistic can be obtained by comparing the difference in log likelihood between the full regression model and a reduced regression model. A reduced model is a model in which all the coefficients are set to 0 (i.e., predictors are removed from the model), such that the model has an intercept only (Koymen & Tomasello, 2018). When the Likelihood ratio test is statistically significant (i.e., when $p < .05$), it is indicative that there is goodness of fit. As shown in Table 15, there was statistical significance for the final model prediction of the dependent variable compared to the intercept-only model, $\chi^2(3) = 130.676$, $p < .001$.

Table 15

Model 1 Fitting Information

Model Fitting Information

Model	-2 Log Likelihood	Chi-square	df	Sig.
Intercept Only	313.011			
Final	182.335	130.676	3	.000

Link function: Logit.

Next, I sought to determine whether the independent variables in the model (information security awareness, ISA_SUM; password self-efficacy, PSE_SUM; and attitude towards compliance ATC_SUM) were able to predict the dependent variable (intention to comply, IC1). Table 16 below displays the test of model effects. Information security awareness did not have a statistically significant effect on the prediction of an employee's intention to comply with password policies, Wald $\chi^2(1) = 1.571$, $p > .05$. The second independent variable, password self-efficacy, had a statistically significant effect on the prediction of an employee's intention to comply with password policies (Wald $\chi^2(1) = 5.446$, $p = .02$). The third independent variable, attitude towards compliance, had a statistically significant effect on the prediction of an employee's intention to comply with password policies (Wald $\chi^2(1) = 35.778$, $p < .001$). In brief, two of the predictor variables had significant effects on prediction of an employee's intentions to comply with password policies, while one predictor variable did not have a significant effect on prediction of the outcome variable.

Table 16

Model 1 Test for Model Effects

Tests of Model Effects

Source	Type III Wald Chi-square	df	Sig.
ISA_SUM	1.571	1	.210
PSE_SUM	5.446	1	.020
ATC_SUM	35.778	1	.000

Dependent Variable: IC1
Model: (Threshold), ISA_SUM, PSE_SUM, ATC_SUM

The next step in the analyses was to determine how changes in the predictor variable affected the outcome variable for the two predictor variables which showed a statistically significant effect on predicting the outcome variable. As stated above, password self-efficacy and attitude towards compliance had significant effects on predicting intention to comply with password policies. Ordinal logistic regression uses odds ratios to indicate how changes in predictor variables affect the outcome variable. Table 17 shows the parameter estimates for Model 1. The findings from Model 1 are summarized below.

(i) An increase in an employee's score for password self-efficacy (PSE_SUM) was associated with an increase in the odds that the employee had higher intentions to comply with password policies, with an odds ratio of 1.257 (95% CI, 1.037 to 1.524), Wald $\chi^2(1) = 5.446$, $p < .05$). This means that for every unit increase in an employee's score for password self-efficacy, the odds of

having a higher intention to comply with password policies increases by 1.257 times.

(ii) An increase in an employee's score for attitude towards policy compliance (ATC_SUM) was associated with an increase in the odds that the employee had higher intentions to comply with password policies, with an odds ratio of 1.783 (95% CI, 1.475 to 2.155), Wald $\chi^2(1) = 35.778$, $p < .001$. This result suggests that attitude towards policy compliance is a significant predictor of an employee's intentions to comply with password policies.

(iii) An increase in an employee's score for information security awareness (ISA_SUM) was associated with an increase in the odds that the employee had higher intentions to comply with password policies, with an odds ratio of 1.074 (95% CI, 0.960 to 1.201), Wald $\chi^2(1) = 1.571$, $p = .210$. However, this outcome was not statistically significant, as p was greater than .05. This means that we cannot say with confidence that information security awareness scores were predictive of employees' intentions to comply with password policies.

Table 17 below shows the parameter estimates including odd ratios shown as the last three rows of Table 15, in column Exp(B).

Table 17

Model 1 Parameter Estimates

Parameter Estimates

Parameter		B	Std. Error	95% Wald Confidence Interval Lower	95% Wald Confidence Interval Upper	Hypothesis Test Wald Chi-Square	df	Sig.	Exp(B)	95% Wald Confidence Interval for Exp(B) Lower	95% Wald Confidence Interval for Exp(B) Upper
Threshold	[IC1=2]	12.243	2.2031	7.925	16.561	30.884	1	.000	207597.689	2766.496	1.5E+7
	[IC1=4]	15.301	2.1403	11.107	19.496	51.111	1	.000	4419118.927	66604.369	2.9E+8
	[IC1=5]	17.087	2.2476	12.682	21.493	57.794	1	.000	26356689.74	321875.513	2.2E+9
	[IC1=6]	20.403	2.5304	15.443	25.363	65.012	1	.000	725941019.9	5093149.52	1035E+11
ISA_SUM		.072	.0571	-.040	.183	1.571	1	.210	1.074	.960	1.201
PSE_SUM		.229	.0981	.037	.421	5.446	1	.020	1.257	1.037	1.524
ATC_SUM		.578	.0967	.389	.768	35.778	1	.000	1.783	1.475	2.155
(Scale)		1[a]									

Dependent Variable: IC1

Model: (Threshold), ISA_SUM, PSE_SUM, ATC_SUM

a. Fixed at the displayed value.

Based on the results above for Model 1, I rejected the null hypothesis. As discussed above, the null hypotheses stated that there was no relationship between the independent variables (ATC_SUM, PSE_SUM, ISA_SUM) and the dependent variable (IC1). Stated differently, the null hypothesis stated that an employees' intentions to comply with password policies could not be predicted by their attitude towards compliance, password self-efficacy, or information security awareness. However, the results above showed that both attitudes towards compliance (ATC_SUM) and password self-efficacy (PSE_SUM) were able to predict employees' intentions to comply with password policies (IC1). Therefore, the null hypothesis was rejected.

Model 2

I ran a second ordinal logistic regression model to test the null hypothesis below:

$H_0$2: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply by protecting information and technology resources according to the password policy (IC2).

I ran the second regression model using SPSS and analyzed the results. First, I checked for the overall goodness of fit for model 2. Overall goodness of fit indicates how well the ordinal logistic regression model predicts the dependent variable. When there is adequate goodness of fit in the observed model, the deviance statistic should not be statistically significant (i.e., p should be > .05). Similarly, the Pearson goodness of fit test indicates lack of fit when $p < .05$ and indicates goodness of fit when $p > .05$ (Hilvert-Bruce et al., 2018). Table 18 shows the results of the goodness of fit test. The Deviance goodness of fit test indicated that the model was a good fit ($\chi^2(378) = 161.635$, $p > .05$). Also, the Pearson goodness of fit test showed that the model was a good fit ($\chi^2(378) = 204.615$, $p > .05$).

Table 18

Model 2 Goodness of Fit

	Chi-square	df	Sig.
Pearson	204.615	378	1.000
Deviance	161.635	378	1.000

Link function: Logit.

To further test goodness of fit, I examined the model fitting information from a Likelihood-ratio test. The Likelihood ratio test statistic is obtained by calculating the difference in log likelihood between the full regression model and a reduced regression model. When the Likelihood ratio test is statistically significant (i.e., when $p < .05$), it is indicative that there is goodness of fit. As shown in Table 19, there was statistical significance for the final model prediction of the dependent variable compared to the intercept-only model, $\chi^2(3) = 130.676$, $p < .001$. This indicated that the goodness of fit for model 2 was adequate.

Table 19

Model 2 Fitting Information

Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	298.924			
Final	170.632	128.292	3	.000

Link function: Logit.

The next step was to investigate whether the independent variables were able to predict the outcome variable, which in model 2 was IC2. I used the test of model effects shown in Table 20. The independent variable attitude towards compliance had a significant effect on the prediction of an employee's intention to comply with password policies in model 2, Wald $\chi^2(1) = 44.91$, $p < .001$. The other two independent variables (information security awareness and password self-efficacy) did not show a statistically significant prediction of intention to comply with password policies in model 2.

Table 20

Model 2 Test for Model Effects

Tests of Model Effects

Source	Type III Wald Chi-Square	df	Sig.
ISA_SUM	2.819	1	.093
PSE_SUM	.014	1	.906
ATC_SUM	44.910	1	.000

Dependent Variable: IC2
Model: (Threshold), ISA_SUM, PSE_SUM, ATC_SUM

Having established that prediction of intention to comply based on attitude towards compliance was statistically significant, I used parameter estimates (shown in Table 21) to determine how a change in attitude towards compliance affected an employee's intention to comply with password policies. An increase in an employee's score for attitude towards compliance was associated with an increase in the odds that the employee had higher intentions to comply with password policies, with an odds ratio of 2.046 (95% CI, 1.659 to 2.522), Wald $\chi 2(1) = 44.910$, $p < .05$). This means that when there is a unit increase in an employee's score for attitude towards compliance, the odds of having a higher intention to comply with password policies increases by 2.046 times. In model 2, information security awareness and password self-efficacy were not statistically significant predictors of employees' intentions to comply with policies by protecting information technology resources.

Table 21

Model 2 Parameter Estimates

Parameter Estimates

Parameter		B	Std. Error	95% Wald Confidence Interval Lower	95% Wald Confidence Interval Upper	Hypothesis Test Wald Chi-Square	df	Sig.	Exp(B)	95% Wald Confidence Interval for Exp(B) Lower	95% Wald Confidence Interval for Exp(B) Upper
Threshold	[IC2=4]	15.799	2.2091	11.469	20.129	51.145	1	.000	7266023.990	95694	5517E+5
	[IC2=5]	16.745	2.2595	12.317	21.174	54.927	1	.000	18727112.397	223468	1569E+6
	[IC2=6]	20.747	2.5949	15.661	25.833	63.923	1	.000	10240438289	6331502	1656E+11
ISA_SUM		.101	.0600	-.017	.218	2.819	1	.093	1.106	.983	1.244
PSE_SUM		-.012	.1002	-.208	.185	.014	1	.906	.988	.812	1.203
ATC_SUM		.716	.1068	.506	.925	44.910	1	.000	2.046	1.659	2.522
(Scale)		1[a]									

Dependent Variable: IC2

Model: (Threshold), ISA_SUM, PSE_SUM, ATC_SUM

a. Fixed at the displayed value.

The results of the ordinal logistic regression model 2 suggested that although password self-efficacy and information security awareness were not significant predictors, employees' intentions to comply with policies by protecting information technology resources could be predicted by their attitudes towards compliance. Therefore, I rejected the null hypothesis $H_0$2.

Model 3

I ran a third ordinal logistic regression model to test the H_0 below:

$H_0$3: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-

efficacy, and employees' intentions to comply intention to comply by carrying out their responsibilities prescribed in the password policy (IC3).

First, I checked for goodness of fit. Overall goodness of fit for model 3 was satisfactory, as displayed in Table 22. The Deviance goodness of fit test indicated that the model was a good fit ($\chi^2(378) = 181.559$, $p > .05$). However, the Pearson goodness of fit measure was statistically significant ($\chi^2(378) = 1105.085$, $p < .05$), indicating that model 3 may not be a good fit for the dataset.

Table 22

Model 3 Goodness of Fit

Goodness-of-Fit

	Chi-Square	df	Sig.
Pearson	1105.085	378	.000
Deviance	181.559	378	1.000

Link function: Logit.

With such mixed goodness of fit results, I investigated further using a Likelihood-ratio test. As discussed earlier, The Likelihood ratio test compares the difference in log likelihood between the full regression model and a reduced regression model. Model fitting information analyses using the Likelihood-ratio test showed that there was statistical significance for the final model prediction of the dependent variable compared to the intercept-only model, $\chi^2(3) = 196.814$, $p < .001$ (see Table 23). Overall, model 3 was a good fit as an ordinal logistic regression model for the dataset.

Table 23

Model 3 Model Fitting Information

Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	322.310			
Final	196.814	125.496	3	.000

Link function: Logit.

To find out whether the independent variables were able to predict the outcome variable with statistical significance, I ran the tests of model effects. The model effects for model 3 are shown in Table 24. The results indicated that in model 3, attitude towards compliance was a predictor of employees' intention to comply with password policies, Wald $\chi^2(1) = 39.685$, $p < .001$. The ability of information security awareness or password self-efficacy to predict employees' password policy compliance intentions was not statistically significant in model 3.

Table 24

Model 3 Tests of Model Effects

Tests of Model Effects

Source	Type III Wald Chi-Square	df	Sig.
ISA_SUM	1.918	1	.166
PSE_SUM	1.771	1	.183
ATC_SUM	39.685	1	.000

Dependent Variable: IC3
Model: (Threshold), ISA_SUM, PSE_SUM, ATC_SUM

Next, I examined the parameter estimates for model 3, specifically the odds ratios, to determine the extent to which a change in an employee's attitude towards compliance affected the odds that there would be a change in intentions to comply with password policies. Table 25 shows the parameter estimates for model 3. An increase in an employee's score for attitude towards compliance was associated with an increase in the odds that the employee had higher intentions to comply with password policies, with an odds ratio of 1.782 (95% CI, 1.489 to 2.132), Wald $\chi 2(1) = 39.685$, $p < .05$). In other words, a unit increase in an employee's score for attitude towards compliance resulted in an increase of 1.782 times in the odds of having a higher intention to comply with password policies.

Table 25

Model 3 Parameter Estimates

Parameter Estimates

				95% Wald Confidence Interval		Hypothesis Test				95% Wald Confidence Interval for Exp(B)	
Parameter		B	Std. Error	Lower	Upper	Wald Chi-Square	df	Sig.	Exp(B)	Lower	Upper
Threshold	[IC3=4]	13.962	1.9488	10.142	17.781	51.326	1	.000	1157567.1	25391.9	5.2E+7
	[IC3=5]	15.714	2.0420	11.711	19.716	59.217	1	.000	6672947.3	121947.5	3.6E+8
	[IC3=6]	19.080	2.2991	14.573	23.586	68.868	1	.000	193258507.3	2133678.1	1.750E+10
ISA_SUM		.076	.0545	-.031	.182	1.918	1	.166	1.078	.969	1.200
PSE_SUM		.123	.0921	-.058	.303	1.771	1	.183	1.130	.944	1.354
ATC_SUM		.578	.0917	.398	.757	39.685	1	.000	1.782	1.489	2.132
(Scale)		1[a]									

Dependent Variable: IC3

Model: (Threshold), ISA_SUM, PSE_SUM, ATC_SUM

a. Fixed at the displayed value.

Results from Model 3 showed that employees' information security awareness and password self-efficacy were not significant predictors of their intentions to comply with password policies by carrying out their responsibilities prescribed in the policy. However, attitude towards compliance was a significant predictor of intention to comply. Therefore, I rejected the null hypothesis $H_0$3.

Summary of Findings

The research question for this study was as follows: What is the relationship between employees' attitudes towards information system password policies, employees' security awareness, employees' password self-efficacy, and employees' intentions to comply with password policies? To address this research question, I performed regression analyses. First, I tested the assumptions of multiple linear regression on my dataset, and the dataset failed to satisfy the assumptions of normality, linearity, and lack of multicollinearity. Therefore, I analyzed the data using ordinal logistic regression, a technique akin to multiple linear regression but which does not require compliance with the assumption of normality. I ran three ordinal logistic regression models in SPSS and tested the following hypotheses:

$H_0$1: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' overall intentions to comply with password policies denoted by dependent variable IC1.

$H_0$2: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password

self-efficacy, and employees' intentions to comply by protecting information and technology resource according to the password policy denoted by dependent variable IC2.

$H_0$3: There is no statistically significant predictive relationship between employees' (a) attitudes towards password policies, (b) security awareness, (c) password self-efficacy, and employees' intentions to comply intention to comply by carrying out their responsibilities prescribed in the password policy denoted by dependent variable IC3.

For all three ordinal logistic regression models, the independent variables were the same (attitudes towards compliance, information security awareness, and password self-efficacy). For the dependent variable, three separate measures of employee intentions to comply with policies were used, namely IC1, IC2 and IC3, one in each regression model. Results from the regression analyses were as follows:

- Employees' attitude towards password policies had a significant positive effect on all three measures of intention to comply with policies (i.e., IC1, IC2, IC3).
- Employees' password self-efficacy had a significant positive effect on one measure of intention to comply with policies (IC1).
- Employee's information security awareness did not have a significant effect on any measure of intention to comply with policies.

In brief, employees' attitude towards policies and password self-efficacy affected their intention to comply with password policies, while information security awareness did not have a significant effect. Based on the results above, I rejected the null hypothesis

that there was no relationship between employees' attitudes towards information system password policies, employees' security awareness, employees' password self-efficacy, and employees' intentions to comply with password policies.

Interpretation of Results

The main findings from this study were that employees' attitudes towards password policies and password self-efficacy had significant effects on their intentions to comply with password policies, while information security awareness did not have a significant effect. Three ordinal logistic regression models were run to investigate whether the independent variables were able to significantly predict overall intentions to comply, intentions to comply by protecting information technology assets as prescribed by the policy, and intention to comply by carrying out their responsibilities as prescribed by the policy.

Employees' overall intentions to comply with password policies was significantly predicted by their attitudes towards compliance. That is, an increase in employees' score for attitude towards compliance was associated with statistically significant odds that scores for intentions to comply would increase. These findings were obtained in the context of employees who work for organizations in the United States, and participation was limited to employees who were aware of the password policies of their organizations. Therefore, these results may be generalized to a broader population meeting those criteria. These results are consistent with the assertion by Siponen et al. (2014) that there is a positive relationship between an employee's attitude towards information security policies and actual policy compliance. Menard et al. (2017) also reported that when

managers encouraged a favorable attitude towards information security policies by providing choices to users, there was a higher intention to comply with security requirements.

Contrary to the findings from my study and the studies mentioned above, Herath and Rao (2009) found that employees' attitude towards security policies did not affect their intentions to comply with the policies. Rather, they found self-efficacy, social influence, and perception of threat severity as significant contributors to employees' compliance intention (Herath & Rao, 2009). However, Herath and Rao (2009) focused their study on organizations which have high organizational commitment and monitoring of compliance, while my study included a broader range of organizations. In this study, attitude towards compliance was a significant predictor of employees' intentions to comply with policies in all three regression models. Attitude towards compliance significantly affected intentions to comply by safeguarding organizational information security assets as well as intentions to comply by carrying out responsibilities prescribed in the information security policy. Attitude towards compliance was a strong indicator of employees' compliance intentions: a unit increase in attitude towards compliance increased the odds that employees would have high compliance intentions by more than double.

Several factors may explain the influence of employees' attitudes towards policies on the intentions to comply with policies. For example, employees who have a positive attitude towards information security policies may have a greater sense of ownership in the information security endeavor and thus be more likely to comply with policy

requirements. Employees who have a positive attitude towards policies may also perceive that the benefits of compliance outweigh the costs (Kim et al., 2014), providing them a greater motivation to comply compared to employees with negative attitudes towards policies. Attitude towards compliance with password policies may also be affected by employees' perceptions of vulnerability to security threats. Belanger et al. (2017) suggested that users were more likely to comply with password policies when they felt vulnerable to security threats. In brief, employees may adopt a positive attitude towards password policies when they are more involved in the information security endeavor of an organization or when they perceive benefits associated to compliance, and such a positive attitude towards policies may lead to greater intentions to comply with security policies.

Employees' password self-efficacy was also a significant predictor of intentions to comply with password policies. Password self-efficacy was able to predict employees' overall intentions to comply with policies (IC1) but was not a significant predictor of intentions to comply in order to protect organizational information technology assets (IC2) or intentions to comply by carrying out responsibilities prescribed by the policy (IC3). Self-efficacy refers to an individual's perceptions of confidence in his or her ability to comply with information security policies (Johnston et al., 2016). Results from this study suggest that when employees perceive that they are able to meet the requirements of password policies such as length and complexity requirements, they have a greater intention to comply with such policies. These findings were aligned with results from several studies in the literature. Mwagwabi et al. (2014) found that password self-

efficacy has a strong influence on policy compliance. Similarly, Bulgurcu et al. (2010) and Siponen et al. (2014) reported that self-efficacy had a positive influence on employees' intention to comply with information security policies.

However, this view was not shared by Belanger et al. (2017), who found that self-efficacy does not affect employees' intentions to comply with security policies. According to Belanger et al. (2017), employees who had high self-efficacy were more likely to try to circumvent security policy requirements, resulting in less compliance. In my study which focused on password self-efficacy, the positive effect of self-efficacy may indicate that self-efficacy is beneficial for employees, enabling them to overcome challenges related to policy compliance rather than trying to circumvent the policy. Such challenges may include password complexity and password recall.

The influence of password self-efficacy on compliance intentions was not statistically significant in regression models 2 and 3. In regression model 2, employees' intentions to comply with policies was measured in terms of their intention to protect information technology resources. In model 3, intentions to comply was measured in terms of intention to carry out responsibilities prescribed in the policy. A higher score in password self-efficacy did not significantly increase the odds that employees would have higher intentions to comply by protecting technology resources or carrying out their responsibilities. However, an increase in password self-efficacy score was associated with higher odds of an increase in overall intentions to comply, as seen in model 1. One possible reason for this weak association between password self-efficacy and these measures of intentions to comply is that employees in this study may not have associated

protection of technology resources with policy compliance. For example, employees may be laying more emphasis on the benefits of compliance to them as individuals rather than the benefits to their organizations. Intrinsic benefits of compliance may include personal achievement, promotion, or reputation. Shibchurn and Yan (2015) suggest that users are more likely to engage in behavior if they expect some intrinsic benefit from the behavior. Therefore, if employees with high self-efficacy do not perceive an intrinsic benefit from protecting information technology resources, their level of self-efficacy may not affect their intention to comply by protecting resources. Future studies could investigate the relationship between employee's perceptions of benefits of compliance with password policies, and their intentions to comply with policies.

Information security awareness was not a significant predictor of employees' intentions to comply with password policies. In all three regression models, the effects of information security awareness on intentions to comply were not significant. This finding was not completely unexpected. Information security awareness has been shown to influence employees' information security behavior (Belanger et al., 2017; Bulgurcu et al., 2010). However, these studies indicated that information security awareness had a significant effect on employees' attitude towards policy compliance (Belanger et al., 2017; Bulgurcu et al., 2010), and attitude towards compliance affected intentions to comply (Bulgurcu et al., 2010). The role of information security awareness in employees' compliance intentions was therefore indirect. Bulgurcu et al. (2010) suggested that information security awareness may be indirectly affecting intentions to comply as a background factor. In this study, I tested the hypothesis that information security

awareness may have a direct effect on intentions to comply. Results of this study suggested that there was no significant predictive relationship between information security awareness and intentions to comply with policies.

Given the reports by Bulgurcu et al. (2010) and Belanger et al. (2017) indicating that information security awareness may be affecting employees' attitude towards compliance, I was interested in seeing whether there was a relationship between these two variables in my study. Therefore, I performed an exploratory correlational analysis to investigate the relationship between information security awareness and employees' attitudes towards compliance. There was a strong correlation between information security awareness (ISA_SUM) and attitude towards compliance (ATC_SUM), with a correlation coefficient of .599, $p < .001$. Although this correlation analysis does not demonstrate a predictive relationship between information security awareness and attitude towards compliance, this result was consistent with reports in the literature indicating that information security awareness has a significant effect on attitude towards compliance. In a nutshell, information security awareness was not a significant predictor of employees' intentions to comply with password policies within the context of employees in the United States, but information security awareness may be influencing compliance behavior indirectly by affecting attitudes towards policy compliance.

Alignment with Theory

As discussed under "Review of Underlying Theories," I based this study on the TPB and social cognitive theory. I adopted two constructs of the TPB: attitudes towards behavior and perceived behavioral control or self-efficacy to behave. In addition, I

examined information security awareness as a background factor that may influence password policy behavior. This approach was consistent with the view of Ajzen and Albarracin (2007) that background factors may play a role in predicting behavioral intention and behavior in the TPB. The construct of password self-efficacy was based on the social cognitive theory. Ajzen (1991) stated that in the TPB, perceived behavioral control is compatible with Bandura's (1989) self-efficacy variable, as both variables measure the same element of human behavior.

A central focus of the TPB is explaining people's intentions to perform certain behaviors. Intentions refer to motivations that influence behavior and indicate how much effort people are willing to put into performing a specific behavior (Ajzen, 1991). The TPB explains behavioral intentions in terms of attitudes towards the behavior and self-efficacy (or perceived behavioral control). In this study, employees' attitudes towards password policy compliance was a significant predictor of their intentions to comply with password policies. This result was in alignment with the TPB in which Ajzen (1991) identified attitude towards behavior as a factor that determines the intention to perform the behavior. The TPB also postulates that an individual's self-efficacy towards a behavior can be used to predict the actual performance of the behavior. Results from this study showed that employees' password self-efficacy was a significant predictor of intentions to comply with password policies. This outcome validates the positive relationship between self-efficacy and behavioral intentions as stipulated in the TPB, specifically in the context of password self-efficacy and intentions to comply with password policies among employees working for organizations in the United States. In

sum, the TPB proposes that an individual's attitude towards a behavior and self-efficacy can predict intentions to perform the behavior, and results from this study indicated that both of these constructs were significant predictors of employees' intentions to comply with password policies.

According to the TPB, the factors discussed above (attitude towards behavior and self-efficacy) may not be the only factors affecting behavior (Ajzen & Albarracin, 2007). In addition to these factors, other background factors may influence behavior indirectly. Background factors include factors which differ among individuals, such as experience, demographics, disposition, or knowledge (Ajzen & Albarracin, 2007). In the current study, I investigated the possible role of information security awareness as a background factor affecting employee intentions to comply with information security policies. The results indicated that there was no significant direct relationship between information security awareness and policy compliance intentions. However, it is possible that information security awareness was acting as a background factor affecting employees' attitudes towards compliance, which was the case in a similar study by Bulgurcu et al. (2010). The relationship between employees' level of information security awareness and their attitude towards compliance with security policies could be investigated in future studies.

In the social cognitive theory, Bandura (1989) asserts that an individual's self-efficacy affects his or her actions mediated by motivational, cognitive and affective processes. According to the social cognitive theory, people who have a high self-appraisal of their problem-solving skills visualize positive results of their actions, and

such a cognitive state enhances positive performance. Bandura (1989) suggests a positive relationship between self-efficacy towards some behavior and actual behavior. As discussed above, results from this study indicated that there was a positive relationship between employees' password self-efficacy and their policy compliance intentions, and these findings were consistent with the social cognitive theory. To summarize, results from this study suggest that in a sample of employees in the United States, employee attitudes towards policy compliance and password self-efficacy have positive effects on their intentions to comply with password policies, and these results support both the theory of planned behavior and the social cognitive theory.

Applications to Professional Practice

The purpose of this quantitative correlational design study was to quantify the relationship between employees' attitudes towards password policies, information security awareness, password self-efficacy, and employee intentions to comply with password policies. The independent variables were employees' attitudes towards password policies, information security awareness, and password self-efficacy. The dependent variables were three separate measures of intention to comply with password policies including employees' overall intentions to comply with password policies, intentions to comply by protecting information and technology resource according to the password policy, and intention to comply by carrying out their responsibilities prescribed in the password policy. Results from the study showed that in a sample of employees in the United States, employees' attitudes towards password policies and password self-efficacy had a significant effect on their intentions to comply with password policies,

while information security awareness did not have a significant effect. This study examined factors affecting information security policy compliance from the perspective of employees and may have several applications for information technology managers and policymakers.

In this study, employees' attitudes towards information security password policies was a significant predictor of their intentions to comply with policies. Employees play an important role in organizational information security. Without employee compliance, information security policies are less effective. The attitudes employees adopt towards the policies are vital in shaping their compliance intentions. Information technology leaders and policymakers should focus their efforts on ensuring that information security policies are viewed favorably by employees. Organizations can encourage positive attitudes towards policies by involving employees in the crafting and implementation of the policies. Organizational management should create a culture in which employees feel ownership and responsibility for securing information systems or other information technology assets. Employees have better attitudes towards information security policies when they perceive that compliance with such policies is useful and beneficial to them. Policymakers should, therefore, strive to create policies which do not obstruct the accomplishment of daily tasks. Information technology practitioners can also educate users about the benefits of safeguarding information technology assets. Also, organizations should enforce sanctions for policy violations. When sanctions are enforced, employees are less likely to have a nonchalant attitude towards complying with policies, and this may act as a deterrent to noncompliance.

Password self-efficacy was also a significant predictor of employee intentions to comply with password policies. Self-efficacy is an individual's perceptions of his or her capabilities or an individual's judgment of his or her ability to successfully perform a task (Hwang et al., 2016). Findings from this study indicate that employees are more likely to comply with password policies when they have positive perceptions of their ability to comply with the policies. Organizations should focus their efforts on promoting employee self-efficacy by providing information security education and training for employees. For example, information security programs should include practical training on how to create passwords which are strong and also easy to remember. Such training can empower employees and shape their perceptions of their ability to comply with password requirements. Mwagwabi et al. (2014) found that users' confidence in their ability to create strong passwords correlates with their likelihood to comply with password guidelines. Similarly, Bulgurcu et al. (2010) suggested that self-efficacy, along with information security awareness and normative belief positively affects employees' intentions to comply with information security policies. Information security managers should, therefore, leverage information security education, training, and awareness to positively influence employees' password policy compliance.

Implications for Social Change

Results from this study may have a significant impact on individuals and organizations. Information security passwords are an easy, inexpensive way of authenticating users in information systems. Employee compliance with password policies is vital for organizational information security, as failure to comply may result in

costly security breaches. Many security breaches have originated from employees through unintentional negligence or malicious intent to steal insider information for personal gain (Opderbeck, 2016). I identified employees' attitudes towards policies and password self-efficacy as factors that influence policy compliance intentions. Information security managers and security policy makers in the United States can use this knowledge in the crafting, implementation, and promotion of information security policies. Also, information security leaders can focus on these factors as they seek to improve security policy compliance. For example, discussions related to user attitudes towards policy compliance and self-efficacy can be included during employee security training. Results from this study can, therefore, be beneficial to organizations by fostering improved information security and better protection of organizational assets.

Improvements in employees' security policy compliance may have implications for communities. Better compliance with password policies could result in a reduction in the occurrence of employee-related security breaches. Such a reduction in security breaches may promote public confidence in organizational information systems. Also, improved information security may have a positive impact on the confidentiality, integrity, and availability of sensitive information. A reduction in security breaches caused by employee actions can also have a direct financial impact, as such breaches often involve financial loss through identity theft or legal costs. This study provided knowledge of some of the antecedents of employee intentions to comply with password policies, and this knowledge can be used by information security leaders to improve

employee compliance with policies, reduce the potential for security breaches, and reduce costs associated with security breaches.

Recommendations for Action

Information security policy compliance is an important part of an organization's security program. An information security policy is ineffective if users do not comply with the prescriptions of the policy. Knowledge from this study can be integrated into the implementation and promotion of information security policies. In this study, I examined factors affecting employees' compliance behavior from the perspective of employees themselves. Capturing employee perspectives was important because, as they seek ways to improve organizational information security, IT leaders can consider these factors related to the human aspects of security in addition to technical security controls, providing a more holistic view of information security. As discussed above, findings from this study suggest that employee self-efficacy and attitudes towards policies affect their policy compliance intentions. Information security leaders should focus on these predictors of employee policy compliance as they seek to enhance the security posture of their organizations.

Organizational information security practitioners should create a security culture that inspires positive attitudes towards security policies. Such a culture can be achieved by designing security-enhancing processes that involve employees and promote a sense of ownership in the information security endeavor. Furthermore, information security managers should design information security training and awareness programs in which positive attitudes towards security policies are reinforced. For example, management

should reward employees for pro-security behaviors. In addition to ensuring that employees know the requirements of the security policy, employees should also be made to understand why it is important to fulfill policy requirements. Also, security training should be used to lessen employee perceptions that compliance impedes their ability to accomplish daily tasks. At the same time, security training should emphasize the benefits of compliance. As a whole, these steps may boost employee attitudes towards security policies and ultimately affect compliance positively.

Results from this study echoed findings by others (Bulgurcu et al., 2010; Kim et al., 2014), who identified self-efficacy as having a significant positive effect on intentions to comply with security policies. Some of the challenges associated with password policy compliance include perceptions that password creation and management requirements are too complicated, employees are expected to manage multiple passwords, and passwords are hard to remember (Mwagwabi et al., 2014). Results from this study indicated that self-efficacy was a contributor to compliance intentions, so efforts to increase employees' self-efficacy may be beneficial in overcoming the challenges associated with compliance discussed above. A practical implication of this finding is that security practitioners should focus their efforts on training employees and creating awareness of the requirements of the security policy. For example, employees should be provided with practical, hands-on training on how to create passwords that are complex yet easy to remember. In addition, management should simplify compliance procedures, so employees do not feel that meeting security requirements is difficult or complicated. To summarize, information security leaders in the United States should leverage the results

of this study to improve password policy compliance by reinforcing positive attitudes towards policies, emphasizing the importance of compliance, and creating awareness of the requirements of the security policy.

Recommendations for Further Study

This study had some limitations. The first limitation was the likelihood of introducing selection bias due to the study design. I used an internet-based research firm to recruit participants by selecting an online sample. Sampling bias in such samples may occur due to the self-selection of participants or because the internet population may not be representative of the general population (Tsuboi et al., 2015). By using Qualtrics for data collection, the sample was limited to employees who were members of the Qualtrics pool of panel members. It can be argued that such an online sample is not very representative of the employee population in the United States. Therefore, the ability to generalize the results of this study may be limited. Future researchers should consider using a more diverse sample of employees so that results can be more generalizable.

Another limitation of the study had to do with the selection criteria. One of the selection criteria for the study was that participants had to be aware of the requirements of the information security policy of their organization. It is possible that I selected a pool of participants who had a high level of security awareness, and this may have affected the variability of the information security awareness variable. However, being aware of the security policy was a necessary selection criterion in order to measure intentions to comply with the policy. To circumvent this limitation, future studies could use an experimental design in which study variables such as information security

awareness and password self-efficacy are tested before and after employees receive a training intervention. Such an approach would be adequate to investigate a cause-effect relationship between the variables.

The third limitation was possible response bias. The survey used for data collection in this study required self-reporting by participants on their information security behavior. It is possible that the participants were not completely truthful in their responses, especially on questions related to security policy compliance, which is a sensitive topic. Employees may tend to provide positive responses to policy compliance questions because it is more socially acceptable (Fomby & Sastry, 2018). Future studies could use other data collection approaches such as participant observation or archival data to measure employee compliance with information security policies.

Further research on factors affecting employee intentions to comply with password policies could also include additional factors. In this study, I examined factors such as employees' information security awareness, attitudes towards policy compliance, and password self-efficacy. Other factors that may be considered include threat appraisal, sanctions and rewards, social influence, employee involvement, and normative beliefs. Future researchers can investigate how these factors affect employees' intentions to comply with password policies. In addition, future studies can focus on studying policy compliance behavior in employees from specific economic sectors, such as sectors which are highly targeted by cybercriminals.

Reflections

The doctoral study process was challenging and very enlightening. Beginning from the process of identifying a focus area for my research, I learned to identify an area of inquiry in a manner driven not only by gaps in the literature but also by the social impact of the research. Through excellent mentoring and very relevant coursework on research and methodology, I got to understand the intricate interplay of factors that need to be considered during the planning phases of a doctoral study. Early cognizance of the role of factors such as study scope, availability of resources and ability to collect data, was very useful throughout the research process.

The prospectus and proposal approval processes were rigorous. I had to complete several iterations at each stage. Although this was not an exciting process while it was being completed, I gained an appreciation of the need to follow the scientific process throughout the development of a study. Each doctoral committee member brought insights from a different perspective, resulting in a much stronger doctoral study. The IRB review process was equally demanding, requiring very thoughtful consideration of the ethical implications of research. Completing the doctoral study has been a rewarding experience, one that has prepared me with competencies that I can apply to perform ethically sound scientific inquiry, including data collection, analyses, and proper communicating of findings.

Summary and Study Conclusions

The use of passwords is a simple, inexpensive method of user authentication and many organizations rely on passwords for employee authentication. For passwords to be

effective in protecting information systems, employees must comply with password policies. The goal of this study was to quantify the relationship between employees' attitudes towards password policies, information security awareness, password self-efficacy, and employee intentions to comply with password policies. Findings from this study indicated that in a sample of U.S. employees, employees' attitudes towards password policies and password self-efficacy were significant predictors of intentions to comply with password policies, while information security awareness did not have a significant effect on compliance intentions. Information security managers in the United States can leverage these findings by providing employee education and training that focuses on promoting positive attitudes towards password policies and increasing password self-efficacy. This study may contribute to positive social change, as findings from the study could lead to a reduction in the likelihood of security breaches, and an increase in the integrity of customers' personally identifiable information. A potential reduction in security breaches could be beneficial by promoting customers' confidence in enterprise information systems, and reducing security breach-related revenue loss, for both organizations and individuals.

References

Ahuja, S. (2015). System-level benchmarks for the cloud. *Computer and Information Science, 8*(2), 58-63. doi:10.5539/cis.v8n2p58

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

Ajzen, I., & Albarracin, D. (2007). Predicting and changing behavior: A reasoned action approach. In I. Ajzen, D. Albarrazin, & R. Hornik (Eds.), *Prediction and change of health behaviour: Applying the reasoned action approach* (pp. 3-18). Mahwah, NJ: Erlbaum.

Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., ... & Khan, M. K. (2015). Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation, and future directions. *Journal of Network and Computer Applications*, *48*, 44-57. doi:10.1016/j.jnca.2014.10.009

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

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet & Information Systems*, *12*(2), 747-763 doi:10.3837/tiis.2018.02.012

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management*, *36*(6), 907-916. doi:10.1016/j.ijinfomgt.2016.05.017

Anestis, M. D., Anestis, J. C., Zawilinski, L. L., Hopkins, T. A., & Lilienfeld, S. O. (2014). Equine□related treatments for mental disorders lack empirical support: A systematic review of empirical investigations. *Journal of Clinical Psychology*, *70*(12), 1115-1132. doi:10.1002/jclp.22113

Annansingh, F., & Howell, K. (2016). Using phenomenological constructivism (PC) to discuss a mixed method approach in information systems research. *Electronic Journal of Business Research Methods*, *14*(1), 39-49. Retrieved from http://www.ejbrm.com

Antonacopoulos, N. D., & Serin, R. C. (2016). Comprehension of online informed consents: Can it be improved? *Ethics & Behavior*, *26(3)*, 177-193. doi:10.1080/10508422.2014.1000458

Auxilia, M., & Raja, K. (2016). Ontology centric access control mechanism for enabling data protection in the cloud. *Indian Journal of Science and Technology*, *9*(23), 1-7. doi:10.17485/ijst/2016/v9i23/95148

Ayyagari, R., & Figueroa, N. (2017). Is seeing believing? Training users on information security: Evidence from Java Applets. *Journal of Information Systems Education*, *28*(2), 115-122. Retrieved from www.jise.org

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

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist*, *44*(9), 1175-1184. doi:10.1037//0003-066X.44.9.1175

Barczak, G. (2015). Publishing qualitative versus quantitative research. *Journal of Product Innovation Management,32*(5), 658. doi:10.1111/jpim.12277

Barnham, C. (2015). Quantitative and qualitative research: Perceptual foundations. *International Journal of Market Research, 57*(6), 837-854. doi:10.2501/ijmr-2015-070

Barnighausen, T., Tugwell, P., Røttingen, J. A., Shemilt, I., Rockers, P., Geldsetzer, P., ... & Bor, J. (2017). Quasi-experimental study designs series—paper 4: uses and value. *Journal of clinical epidemiology*, *89*, 21-29. doi:10.1016/j.jclinepi.2017.03.012

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods*, *27*(1), 3-21. doi:10.1177/1525822X14526838

Bartolucci, F., Bacci, S., & Mira, A. (2018). On the role of latent variable models in the era of big data. *Statistics & Probability Letters*. doi:10.1016/j.spl.2018.02.023

Bauer, D. J., & Sterba, S. K. (2011). Fitting multilevel models with ordinal outcomes: performance of alternative specifications and methods of estimation. *Psychol Methods, 16(4*), 373-90.

Bauer, S., Bernroider, W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & security*, *68*, 145-159. doi:10.1016/j.cose.2017.04.009

Bedeian, A. G. (2014). “More than meets the eye”: A guide to interpreting the descriptive statistics and correlation matrices reported in management research. *Academy of Management Learning & Education*, *13*(1), 121-135. doi:10.5585/ijsm.v14i2.2244

Belanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887-901. doi:10.1016/j.im.2017.01.003

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. doi:10.1080/07448481.2013.872648

Boulesteix, A., Stierl, V., & Hapfelmeier, A. (2015). Publication bias in methodological computational research. *Cancer Informatics*, *(14)*, 11-19. doi:10.4137/CIN.S30747

Bracken-Roche, D., Bell, E., Racine, E., & Macdonald, M. E. (2017). The concept of ' vulnerability ' in research ethics: an in-depth analysis of policies and guidelines. *Health Research Policy and Systems*, *15.* doi:10.1186/s12961-016-0164-6

Bromwich, D., & Rid, A. (2015). Can informed consent to research be adapted to risk? *Journal of Medical Ethics*, *41*(7), 521-528. doi:10.1136/medethics-2013-101912

Brown, J. L., MacDonald, R., & Mitchell, R. (2015). Are people who participate in cultural activities more satisfied with life? *Social Indicators Research*, *122*(1), 135-146.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548. doi:10.2307/25750690

Bun, M. J., & Harrison, T. D. (2018). OLS and IV estimation of regression models including endogenous interaction terms. *Econometric Reviews*, 1-14. doi:10.1080/07474938.2018.1427486

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209. doi:10.1016/j.chb.2016.11.018

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

Catania, J. A., Dolcini, M. M., Orellana, R., & Narayanan, V. (2015). Nonprobability and probability-based sampling strategies in sexual science. *Journal of Sex Research*, *52*(4), 396-411. doi:10.1080/00224499.2015.1016476

Chan, K., Ng, Y., & Prendergast, G. (2014). Should different marketing communication strategies be used to promote healthy eating among male and female

adolescents? *Health Marketing Quarterly*, *31*(4), 339-352. doi:10.1080/07359683.2014.966005

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal 0f Management Information Systems*, *31*(4), 49-87. doi:10.1080/07421222.2014.1001257

Chen, L., Pourahmadi, M., & Maadooliat, M. (2014). Regularized multivariate regression models with skew-t error distributions. *Journal of Statistical Planning and Inference*, *149*, 125-139. doi:10.1016/j.jspi.2014.02.001

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*, 447-459. doi:10.1016/j.cose.2013.09.009

Chiou, J. M., Yang, Y. F., & Chen, Y. T. (2016). Multivariate functional linear regression and prediction. *Journal of Multivariate Analysis*, *146*, 301-312. doi:10.1016/j.jmva.2015.10.003

Cho, H., Mountain, P., Porto, N., Kiss, E., Gutter, S., & Griesdorn, T. (2016). Experimental design to understand the student loan decision: A methodological note. *Family and Consumer Sciences Research Journal, 45*(1), 65-76. doi:10.1111/fcsr.12186

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability*, *8*(7), 638. doi:10.3390/su8070638

Chul Ho, L., Xianjun, G., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research, 27*(1), 70-86. doi:10.1287/isre.2015.0607

Clarke, C. (2016). Preferences and positivist methodology in economics. *Philosophy of Science*, *83*(2), 192-212. doi:10.1086/684958

Claydon, L. S. (2015). Rigour in quantitative research. *Nursing Standard, 29*(47), 43. doi:10.7748/ns.29.47.43.e8820

Connelly, L. M. (2016). Cross-Sectional Survey Research. *MEDSURG Nursing*, *25*(5), 369-370. Retrieved from www.medsurgnursing.net

Conner, M., McEachan, R., Taylor, N., O'Hara, J., & Lawton, R. (2015). Role of affective attitudes and anticipated affective reactions in predicting health behaviors. *Health Psychology*, *34*(6), 642. doi:10.1037/hea0000143

Constantin, C. (2017). Using the Regression Model in multivariate data analysis. *Bulletin of the Transilvania University of Brasov. Series V: Economic Sciences*, *10*(1), 27-34. Retrieved from http://webbut.unitbv.ro

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

Cowls, J., & Schroeder, R. (2015). Causation, correlation, and big data in social science research. *Policy & Internet*, *7*(4), 447-472. doi:10.1002/poi3.100

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605-641. doi:10.1057/s41303-017-0059-9

Curtis, E. A., Comiskey, C., & Dempsey, O. (2016). Importance and use of correlational research. *Nurse Researcher (2014+),23*(6), 20. doi:10.7748/nr.2016.e1382

Dahlke, S., Hall, W., & Phinney, A. (2015). Maximizing theoretical contributions of participant observation while managing challenges. *Qualitative Health Research*, *25*(8), 1117-1122. doi:10.1177/1049732315578636

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Investigation into the formation of information security influence: Network analysis of an emerging organization. *Computers & Security*. doi:10.1016/j.cose.2017.05.010

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

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

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319-340. doi:10.2307/249008

Dijkstra, T. K., & Henseler, J. (2015). Consistent Partial Least Squares Path Modeling. *MIS Quarterly*, *39*(2). Retrieved from http://www.misq.org.

Drazen, J. M., Harrington, D. P., McMurray, J. J. V., Ware, J. H., Woodcock, J., Grady, C., . . . Kang, G. (2017). The changing face of clinical trials: Informed consent. *The New England Journal of Medicine, 376*(9), 856-867. Retrieved from www.nejm.org

Dusick, D. (2015). Writing the assumptions and limitations. Retrieved from http://bold-ed.com/barrc/assumptions.htm

Elifoglu, H., Abel, I., & Tasseven, O. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business*, *38*(2), 61-73. Retrieved from http://www.stjohns.edu

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science & Information Technology*, *6*, 323-337. doi:10.28945/1062

El-Masri, M. (2017). Probability sampling. *Canadian Nurse*, *113*(2), 26. Retrieved from https://www.canadian-nurse.com

Estevez, E., Janowski, T., & Lopes, N. V. (2016). Policy monitoring on accessible technology for inclusive education - Research findings and requirements for a software tool. *Journal of Computer Science & Technology*, *16*(1), 29-37. Retrieved from http://jcst.ict.ac.cn

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. doi:10.3758/BRM.41.4.1149

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Reading, MA: Addison-Wesley.

Florêncio, D., Herley, C., & Van Oorschot, P. C. (2016). Pushing on String: The 'Don't Care' Region of Password Strength. *Communications of the ACM, 59*(11), 66-74. doi:10.1145/2934663

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. doi: 10.1016/j.cose.2014.03.004

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*, 169-183. doi:10.1016/j.cose.2016.06.002

Fomby, P., & Sastry, N. (2018). Data Collection on Sensitive Topics with Adolescents Using Interactive Voice Response Technology. *Methods, data, analyses*, 20. doi: 0.12758/mda.2018.05

Foresman, A. R. (2015). Once more unto the [corporate data] breach, dear friends. *Journal of Corporation Law*, *41*(1), 343-358. Retrieved from https://jcl.law.uiowa.edu/

Fortin, M., Haggerty, J., Almirall, J., Bouhali, T., Sasseville, M., & Lemieux, M. (2014). Lifestyle factors and multimorbidity: a cross sectional study. *BMC Public Health, 14*(1), 686. doi:10.1186/1471-2458-14-686

Fritz, J., & Kaefer, F. (2017). The rise of the mega breach and what can be done about it. *Journal of Applied Security Research*, *12*(3), 392-406. doi:10.1080/19361610.2017.1315700

Fugard, A. J., & Potts, H. W. (2015). Supporting thinking on sample sizes for thematic analyses: a quantitative tool. *International Journal of Social Research Methodology*, *18*(6), 669-684. doi:10.1080/13645579.2015.1005453

Gallagher, C., McMenemy, D., & Poulter, A. (2015). Management of acceptable use of computing facilities in the public library: avoiding a panoptic gaze? *Journal of Documentation, 71*(3), 572-590. doi:10.1108/jd-04-2014-0061

Gaudioso, F., Turel, O., & Galimberti, C. (2015). Explaining work exhaustion from a coping theory perspective: Roles of techno-stressors and technology-specific coping strategies. *Studies in Health Technology and Informatics, 219,* 14-20. doi:10.3233/978-1-61499-595-1-14

Gheyas, A., & Abdallah, E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics, 1*(1), 6. doi:10.1186/s41044-016-0006-0

Gibbs, B. G., Shafer, K., & Dufur, M. J. (2015). Why infer? The use and misuse of population data in sports research. *International Review for the Sociology of Sport*, *50*(1), 115-121. doi:10.1177/1012690212469019

Gibson, C. B. (2017). Elaboration, generalization, triangulation, and interpretation: On enhancing the value of mixed method research. *Organizational Research Methods*, *20*(2), 193-223. doi:10.1177/1094428116639133

Goel, D., & Jain, A. K. (2017). Mobile phishing attacks and defense mechanisms: state of the art and open research challenges. *Computers & Security, 73*, 519-544. doi:10.1016/j.cose.2017.12.006

Gotterbarn, D., Bruckman, A., Flick, C., Miller, K., & Wolf, M. J. (2018). ACM code of ethics: A guide for positive action. *Communications of the ACM*, *61*(1), 121-128. doi:10.1145/3173016

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

Green, J. (2015). Somatic sensitivity and reflexivity as validity tools in qualitative research. Research in Dance Education, *16*(1), 67-79. doi:10.1080/14647893.2014.971234

Grzyb, T. (2017). Obtaining informed consent from study participants and results of field studies. Methodological problems caused by the literal treatment of codes of ethics. *Polish Psychological Bulletin, 48*(2), 288-292. doi:10.1515/ppb-2017-0032

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

Guo, Y., & Zhang, Z. (2017). LPSE: lightweight password-strength estimation for password meters. *Computers & Security*, *73*, 507-518. doi:10.1016/j.cose.2017.07.012

Haegele, J. A., & Hodge, S. R. (2015). Quantitative methodology: a guide for emerging physical education and adapted physical education researchers. *The Physical Educator*, (SI), 59. doi:10.18666/tpe-2015-v72-i5-6133

Hall, C. F. (2016). Using Regression Analysis in the Market Approach. *Value Examiner*, 16-24. Retrieved from www.nacva.com/valueexaminer.

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52-65. doi:10.1016/j.cose.2016.12.016

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

Hauer, B. (2015). Data and information leakage prevention within the scope of information security. *IEEE Access*, *3*, 2554-2565. doi:10.1109/ACCESS.2015.2506185

Hays, R. D., Liu, H., & Kapteyn, A. (2015). Use of internet panels to conduct surveys. *Behavior Research Methods*, *47*(3), 685-690. doi:10.3758/s13428-015-0617-9

Hazra, A., & Gogtay, N. (2016). Biostatistics Series Module 6: Correlation and Linear Regression. *Indian Journal of Dermatology*, *61*(6), 593-601. doi:10.4103/0019-5154.193662

He, D., Kuhn, D., & Parida, L. (2016). Novel applications of multitask learning and multiple output regression to multiple genetic trait prediction. *Bioinformatics*, *32*(12), i37-i43. doi:10.1093/bioinformatics/btw249

Hedeker, D. (2015). Methods for multilevel ordinal data in prevention research. *Prevention Science*, *16*(7), 997-1006. doi: 10.1007/s11121-014-0495-x

Heickero, R. (2016). Cyber espionage and illegitimate information retrieval. *International Journal of Cyber Warfare and Terrorism*, *6*(1), 13-23. doi: 10.4018/ijcwt.2016010102

Helil, N., & Rahman, K. (2017). CP-ABE access control scheme for sensitive data set constraint with hidden access policy and constraint policy. *Security and Communication Networks*, *2017*. doi:10.1155/2017/2713595

Helkala, K., & Hoddø Bakås, T. (2014). Extended results of Norwegian password security survey. *Information Management & Computer Security*, *22*(4), 346-357. doi: 10.1108/IMCS-10-2013-0079

Helmich, E., Boerebach, B. C., Arah, O. A., & Lingard, L. (2015). Beyond limitations: Improving how we handle uncertainty in health professions education research. *Medical Teacher, 37*(11), 1043-1050. doi:10.3109/0142159x.2015.1073239

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6

Hills, M., & Anjali, A. (2017). A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. *Security Journal, 30*(1), 142-152. doi:10.1057/sj.2015.36

Hilvert-Bruce, Z., Neill, J. T., Sjoblom, M., & Hamari, J. (2018). Social motivations of live-streaming viewer engagement on Twitch. *Computers in Human Behavior*, *84*, 58-67. doi: 10.1016/j.chb.2018.02.013

Hopkins, L., & Ferguson, K. E. (2014). Looking forward: The role of multiple regression in family business research. *Journal of Family Business Strategy, 5*(1), 52-62. doi: 1016/j.jfbs.2014.01.008

Hull, B. (2015). PWC global state of information security survey 2016. Retrieved from http://www.acunetix.com/blog/articles/pwc-global-state-of-information-security-survey-2016/

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282-293. doi:10.1016/j.chb.2017.12.022

Hwang, I., Hwang, I., Kim, D., Kim, D., Kim, T., Kim, T., ... & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2-18. doi:10.1108/oir-11-2015-0358

Hwang, Y., Lee, Y., & Shin, D. (2016). The role of goal awareness and information technology self-efficacy on job satisfaction of healthcare system users. *Behaviour & Information Technology*, *35*(7), 548-558. doi:10.1080/0144929X.2016.1171396

IBM Corp. Released 2017. IBM SPSS Statistics for Windows, Version 25.0. [Computer software]. Armonk, NY: IBM Corp.

Ifinedo, P. (2016). Critical times for organizations: What should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, *33*(1), 30-41. doi:10.1080/10580530.2015.1117868

Ingham-Broomfield, R. (2014). A nurses' guide to quantitative research. *The Australian Journal of Advanced Nursing, 32*(2), 32. Retrieved from http://www.ajan.com.au

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626. doi:10.1080/07421222.2017.1334499

Jervis, G., & Drake, A. (2014). The use of qualitative research methods in quantitative science: A review. *Journal of Sensory Studies*, *29*(4), 234-247. doi:10.1111/joss.12101

Johnston, A. C., Warkentin, M., Mcbride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231-251. doi:10.1057/ejis.2015.15

Jouini, M., Rabai, A., & Aissa, B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496. doi: 10.1016/j.jprocs.2014.05.452

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, *67*, 267-279. doi:10.1016/j.cose.2016.12.012

Khan, W. Z., & Al Zubaidy, S. (2017). Prediction of student performance in academic and military learning environment: Use of multiple linear regression predictive

model and hypothesis testing. *International Journal of Higher Education, 6*(4), 152. doi:10.5430/ijhe.v6n4p152

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*, *12,* 1-12. doi:10.1155/2014/463870

Klein, A. G., Gerhard, C., Buchner, R. D., Diestel, S., & Schermelleh-Engel, K. (2016). The detection of heteroscedasticity in regression models for psychological data. *Psychological Test and Assessment Modeling*, *58*(4), 567.

Koch, L. C., Niesz, T., & McCarthy, H. (2014). Understanding and reporting qualitative research: An analytical review and recommendations for submitting authors. *Rehabilitation Counseling Bulletin*, *57*(3), 131-143.

Kock, N., Avison, D., & Malaurent, J. (2017). Positivist information systems action research: Methodological issues. *Journal of Management Information Systems*, *34*(3), 754-767. doi:10.1080/07421222.2017.1373007

Korkmaz, O., Çakir, R., & Ozden, Y. (2017). A validity and reliability study of the Computational Thinking Scales (CTS). *Computers in Human Behavior, 72*, 558-569. doi:10.1016/j.chb.2017.01.005

Koymen, B., & Tomasello, M. (2018). Children's meta-talk in their collaborative decision making with peers. *Journal of experimental child psychology*, *166*, 549-566. doi:10.1016/j.jecp.2017.09.018

Kuru, O., & Pasek, J. (2016). Improving social media measurement in surveys: Avoiding acquiescence bias in Facebook research. *Computers in Human Behavior, 57*, 82-92. doi:10.1016/j.chb.2015.12.008

Kyonne, J. (2015). Is the scientific method adaptable to the study of social work? A focus on the comparative study of cultural differences. *International Journal of Science in Society*, *7*(4). doi:10.18848/1836-6236/cgp/v07i04/51459

Larinkari, S., Liisanantti, J. H., Ala-Lääkkölä, T., Meriläinen, M., Kyngäs, H., & Ala-Kokko, T. (2016). Identification of tele-ICU system requirements using a content validity assessment. *International Journal of Medical Informatics, 86*, 30-36. doi:10.1016/j.ijmedinf.2015.11.012

Laszka, A., Johnson, B., Schöttle, P., Grossklags, J., & Böhme, R. (2014). Secure team composition to thwart insider threats and cyber-espionage. *ACM Transactions on Internet Technology, 14*(2/3), 19:1-19:22. doi:10.1145/2663499

Laube, S., & Bohme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, *2*(1), 29-41. doi:10.1093/cybsec/tyw002

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. doi:10.1108/MRR-04-2013-0085

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. doi:10.1016/j.cose.2016.02.004

Lee, C. M. (2015). Criminal profiling and industrial security. *Multimedia Tools and Applications*, *74*(5), 1689-1696. doi:10.1007/s11042-014-2014-2

Lewis, C. (2016). Understanding research methods to study African American males in college. *Journal of Negro Education*, *85*(1), 3-15. doi:10.7709/jnegroeducation.85.1.0003

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics, and sanction on internet use policy compliance. *Information Systems Journal*, *24*(6), 479-502. doi:10.1111/isj.12037

Liu, M., Ko, Y., Willmann, A., & Fickert, C. (2018). Examining the role of professional development in a large school district's iPad initiative. *Journal of Research on Technology in Education*, *50*(1), 48-69. doi:10.1080/15391523.2017.1387743

Lobo, R., Hildebrand, J., Burns, S., Lobo, R., Howat, P., Zhao, Y., & ... Allsop, S. (2015). Potential and challenges in collecting social and behavioral data on adolescent alcohol norms: Comparing respondent-driven sampling and web-based respondent-driven sampling. *Journal of Medical Internet Research*, *17*(12), e285. doi:10.2196/jmir.4762

Lowry, B., & Moody, D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, *25*(5), 433-463. doi:10.1111/isj.12043

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83*, 32-44. doi:10.1016/j.chb.2018.01.028

Mangili, M., Martignon, F., & Paraboschi, S. (2015). A cache-aware mechanism to enforce confidentiality, trackability, and access policy evolution in Content-Centric Networks. *Computer Networks, 76*, 126-145. doi:10.1016/j.comnet.2014.11.010

Manterola, C., & Otzen, T. (2017). Checklist for reporting results using observational descriptive studies as research designs. The MInCir Initiative. *International Journal of Morphology*, *35*(1), 72-76. doi:10.4067/s0717-95022017000100013

Martinez-Mesa, J., González-Chica, D. A., Duquia, R. P., Bonamigo, R. R., & Bastos, J. L. (2016). Sampling: how to select participants in my research study? *Anais Brasileiros de Dermatologia*, *91*(3), 326–330. doi:10.1590/abd1806-4841.20165254

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

McKim, C. A. (2017). The value of mixed methods research: A mixed methods study. *Journal of Mixed Methods Research*, *11*(2), 202-222. doi:10.1177/1558689815607096

McNeish, D. (2017). Thanks coefficient alpha, we'll take it from here. *Psychological Methods*. doi:10.1037/met0000144

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230. doi:10.1080/07421222.2017.1394083

Montesdioca, Z., & Maçada, G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48*, 267-280. doi:10.1016/j.cose.2014.10.015

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-A22. doi:10.25300/misq/2018/13853

Morin, D., Thomas, E., & Saadé, G. (2015). Fostering problem-solving in a virtual environment. *Journal of Information Technology Education: Research*, *14*339-362. doi:10.28945/2273

Mueller, K., Straatmann, T., Hattrup, K., & Jochum, M. (2014). Effects of personalized versus generic implementation of an intra-organizational online survey on psychological anonymity and response behavior: A field experiment. *Journal of Business & Psychology, 29*(2), 169-181. doi:10.1007/s10869-012-9262-9

Murshed, F., & Zhang, Y. (2016). Thinking orientation and preference for research methodology. *Journal of Consumer Marketing*, *33*(6), 437-446. doi:10.1108/jcm-01-2016-1694

Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect

compliance with guidelines. In 2014 47th Hawaii International Conference on System Sciences (pp. 3188-3197). IEEE. doi:10.1109/hicss.2014.396

Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, *39*(4), 865-892. doi:10.1111/j.1745-9125.2001.tb00943.x

Narain Singh, A., Gupta, P., & Ojha, A. (2014). Identifying factors of "organizational information security management." *Journal of Enterprise Information Management*, *27*(5), 644-667. doi:10.1108/jeim-07-2013-0052

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. doi:10.1177/1523422314559810

Niblett, G. (2016). Insider Threats. *ITNow*, *58*(2), 23. doi:10.1093/itnow/bww039

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1-20. doi:10.1057/s41303-016-0025-y

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

Opderbeck, D. W. (2016). Cybersecurity, data breaches, and the economic loss doctrine in the payment card industry. *Maryland Law Review*, *75*(4), 935. doi:10.2139/ssrn.2636944

Owen, A., Smith, A. C., Osei-Owusu, P., Harland, A., & Roberts, J. R. (2017). Elite players' perceptions of football playing surfaces: a mixed effects ordinal logistic regression model of players' perceptions. *Journal of Applied Statistics*, *44*(3), 554-570. doi:10.1080/02664763.2016.1177500

Padilla, M. A., & Divers, J. (2016). A comparison of composite reliability estimators: coefficient omega confidence intervals in the current literature. *Educational and Psychological Measurement, 76*(3), 436-453. doi:10.1177/0013164415593776

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. doi:10.1016/j.cose.2013.12.003.

Peduzzi, P., Concato, J., Kemper, E., Holford, T., & Feinstein, R. (1996) A simulation study of the number of events per variable in logistic regression analysis. *Journal of Clinical Epidemiology, 49*, 1373-1379. doi:10.1016/S0895-4356(96)00236-3

Perrault, E. K. (2018). Using an interactive online quiz to recalibrate college students' attitudes and behavioral intentions about phishing. *Journal of Educational Computing Research*, *55*(8), 1154-1167. doi:10.1177/0735633117699232

Peng, C. J., Lee, K. L., & Ingersoll, G. M. (2002). An introduction to logistic regression analysis and reporting. *The journal of educational research*, *96*(1), 3-14.

Peterson, R. A., & Merunka, D. R. (2014). Convenience samples of college students and research reproducibility. *Journal of Business Research*, *67*(5), 1035-1041. doi:10.1016/j.jbusres.2013.08.010

Qualtrics. (2018). Research Core. Retrieved from https://www.qualtrics.com/research-core/

Ranjan, P., & Om, H. (2016). An efficient remote user password authentication scheme based on Rabin's Cryptosystem. *Wireless Personal Communications*, *90*(1), 217-244. doi:10.1007/s11277-016-3342-5

Rice, S., Winter, S. R., Doherty, S., & Milner, M. (2017). Advantages and disadvantages of using internet-based survey methods in aviation-related research. *Journal of Aviation Technology and Engineering*, *7*(1), 5. doi:10.7771/2159-6670.1160

Ritzman, M. E., & Kahle-Piasecki, L. (2016). What works: A systems approach to employee performance in strengthening information security. *Performance Improvement*, *55*(8), 17-22. doi:10.1002/pfi.21614

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114. doi:10.1080/00223980.1975.9915803

Rosopa, P. J., Schaffer, M. M., & Schroeder, A. N. (2013). Managing heteroscedasticity in general linear models. Psychological Methods, 18(3), 335–351. doi: 10.1037/a0032553

Roster, C. A., Albaum, G., & Smith, S. M. (2014). Topic sensitivity and internet survey design: A cross-cultural/national study. *Journal of Marketing Theory & Practice*, *22*(1), 91-102. doi:10.2753/mtp1069-6679220106

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

Sampson, J. P., Hou, P. C., Kronholz, J. F., Dozier, V. C., McClain, M. C., Buzzetta, M., ... & Reardon, R. C. (2014). A content analysis of career development theory, research, and practice—2013. *The career development quarterly*, *62*(4), 290-326. doi:10.1002/j.2161-0045.2014.00085.x

Scherdin, M., & Zander, I. (2014). On the role and importance of core assumptions in the field of entrepreneurship research: A neurophilosophical perspective. *International Journal of Entrepreneurial Behavior & Research, 20*(3), 216-236. doi: 10.1108/ijebr-01-2012-0015

Schoenherr, T., Ellram, L. M., & Tate, W. L. (2015). A note on the use of survey research firms to enable empirical data collection. *Journal of Business Logistics*, *36*(3), 288-300. doi:10.1111/jbl.12092

Sedgwick, P. (2014). Cross sectional studies: Advantages and disadvantages. *British Medical Journal, 348*, 1-2. doi:10.1136/bmj.g2276

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341. doi:10.1080/07421222.2015.1063315

Shibchurn, J., & Yan, X. (2015). Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective. *Computers in Human Behavior*, *44*, 103-117. doi:10.1016/j.chb.2014.10.059

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

Slade, E., Williams, M., Dwivedi, Y., & Piercy, N. (2015). Exploring consumer adoption of proximity mobile payments. *Journal of Strategic Marketing, 23*(3), 209-223. doi:10.1080/0965254X.2014.914075

Soilen, K. S. (2016). Economic and industrial espionage at the start of the 21st century–Status quaestionis. *Journal of Intelligence Studies in Business*, *6*(3), 51-64. Retrieved from http://www.ojs.hh.se

Soilkki, K. K., Cassim, N., & Anis, M. K. (2014). An evaluation of the factors influencing the performance of registered nurses at the national referral hospital in Namibia. Australian Journal of Business and Management Research, *4*(2), 47-60. Retrieved from http://www.ajbmr.com

Solic, K., Ocevcic, H., & Blazevic, D. (2015). Survey on Password Quality and Confidentiality. *Automatika*, *56*(1), 69-75. doi:10.7305/automatika.2015.04.587

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

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. doi:10.1016/j.ijinfomgt.2015.11.009

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. doi:10.1177/1747016115626198

Steinbart, J., Raschke, L., Gal, G., & Dilla, N. (2016). SECURQUAL: an instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems, 30*(1), 71. doi:10.2308/isys-51257

Steinbart, J., Raschke, L., Gal, G., & Dilla, W. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems*, *2*, 65. doi:10.2308/isys-50510

Taki, M., Ajabshirchi, Y., Ranjbar, S. F., & Matloobi, M. (2016). Application of neural networks and multiple regression models in greenhouse climate estimation. *Agricultural Engineering International: CIGR Journal*, *18*(3), 29-43. Retrieved from http://www.cigrjournal.org

Tamjidyamcholo, A., Baba, B., Shuib, M., & Rohani, A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, *43*, 19-34. doi:10.1016/j.cose.2014.02.010

Tarafdar, M., Bolman Pullins, E., & Ragu-Nathan, T. S. (2014). Examining impacts of technostress on the professional salesperson's behavioural performance. *Journal of Personal Selling & Sales Management*, *34*(1), 51-69. doi:10.1080/08853134.2013.870184

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

Teh, P. L., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory. *Journal of Global Information Management*, *23*(1), 44-64. doi:10.4018/jgim.2015010103

Thaler, K. M. (2017). Mixed methods research in the study of political and social violence and conflict. *Journal of Mixed Methods Research*, *11*(1), 59-76. doi:10.1177/1558689815585196

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. doi:10.1016/j.pedn.2014.07.006

Torre, D. M., & Picho, K. (2016). Threats to internal and external validity in health professions education research. *Academic Medicine*, *91*(12), e21. doi:10.1097/acm.0000000000001446

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

Tsuboi, S., Yoshida, H., Ae, R., Kojo, T., Nakamura, Y., & Kitamura, K. (2015). Selection bias of internet panel surveys: a comparison with a paper-based survey

and national governmental statistics in Japan. *Asia Pacific Journal of Public Health*, *27*(2), NP2390-NP2399. doi:10.1177/1010539512450610

Udo, G., Bagchi, K., & Kirs, P. (2018). Analysis of the growth of security breaches: A multi-growth model approach. *Issues in Information Systems*, *19*(4), 176-186. Retrieved from https://www.iacis.org/iis/iis.php

U.S. Government Accountability Office. (2016). Federal high-impact system security (Publication No. GAO-16-501). Retrieved from www.gao.gov/products/GAO-16-501.

Van der Stede, W. A. (2014). A manipulationist view of causality in cross-sectional survey research. *Accounting, Organizations and Society, 39*(7), 567-574. doi:10.1016/j.aos.2013.12.001

Vargas, T., Duff, L., & Faber, J. (2017). A Practical Guide to Experimental Advertising Research. *Journal of Advertising, 46*(1), 101-114. doi:10.1080/00913367.2017.1281779

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication, 20*(5), 570-584. doi:10.1111/jcc4.12126

Wagner, S., Goodin, N., & Hammond, C. (2017). A Brief Primer on Quantitative Measurement for the OD Professional. *OD Practitioner, 49*(2), 55-58. Retrieved from http://www.odnetwork.org

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91–112. doi:10.25300/misq/2015/39.1.05

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management*, *11*(Fall), 1h. Retrieved from http://www.perspectives.ahima.org

Wilkin, C. L., Couchman, P. K., Sohal, A., & Zutshi, A. (2016). Exploring differences between smaller and large organizations' corporate governance of information technology. *International Journal of Accounting Information Systems*, *22*, 6-25. doi:10.1016/j.accinf.2016.07.002

Willaby, H. W., Costa, D. S., Burns, B. D., MacCann, C., & Roberts, R. D. (2015). Testing complex models with small sample sizes: A historical overview and empirical demonstration of what partial least squares (PLS) can offer differential psychology. *Personality and Individual Differences*, *84*, 73-78. doi:10.1016/j.paid.2014.09.008

Williams, R. (2016). Understanding and interpreting generalized ordered logit models. *The Journal of Mathematical Sociology*, *40*(1), 7-20. doi: 10.1080/0022250X.2015.1112384

Williams, M. M., Gomez Grajales, C. A., & Kurkiewicz, D. (2013). Assumptions of multiple regression: Correcting two misconceptions. *Practical Assessment, Research & Evaluation, 18*(11), 1-14. Retrieved from http://www.pareonline.net

Woodside, A. G. (2013). Moving beyond multiple regression analysis to algorithms: Calling for adoption of a paradigm shift from symmetric to asymmetric thinking in data analysis and crafting theory. *Journal of Business Research*, *66*(4), 463-472. doi: 10.1016/j.jbusres.2012.12.021

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note - influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research*, *25*(2), 385-400. doi:10.1287/isre.2014.0522

Wu, H., & Leung, S. O. (2017). Can Likert scales be treated as interval scales? A simulation study. *Journal of Social Service Research*, *43*(4), 527-532. doi:10.1080/01488376.2017.1329775

Yang, C., Liang, P., & Avgeriou, P. (2017). Assumptions and their management in software development: A systematic mapping study. *Information and Software Technology, 94*, 82-110. doi:10.1016/j.infsof.2017.10.003

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology*, *88*(2), 225-231. Retrieved from http://www.radiologictechnology.org

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36-46. doi:10.1016/j.dss.2016.09.009

Zafar, H., Ko, M. S., & Osei-Bryson, K. (2016). The value of the CIO in the top management team on performance in the case of information security

breaches. *Information Systems Frontiers, 18*(6), 1205-1215. doi:10.1007/s10796-015-9562-5

Zellmer-Bruhn, M., Caligiuri, P., & Thomas, C. (2016). From the Editors: Experimental designs in international business research. *Journal of International Business Studies, 47*, 399–407. doi:10.1057/jibs.2016.12

Zhao, D., & Luo, W. (2017). One-time password authentication scheme based on the negative database. *Engineering Applications of Artificial Intelligence*, *62*, 396-404. doi:10.1016/j.engappai.2016.11.009

Zheng, Z., Cheng, H., Zhang, Z., Zhao, Y., & Wang, P. (2018). An alternative method for understanding user-chosen passwords. *Security & Communication Networks*, 1-12. doi:10.1155/2018/6160125

Appendix A: Survey Instrument

1. Overall, I am aware of potential security threats and their negative consequences.
2. I have sufficient knowledge about the cost of potential security problems.
3. I understand the concerns regarding information security and the risks they pose in general.
4. I know the rules and regulations prescribed by the IS Password Policy of my organization.
5. I understand the rules and regulations prescribed by the IS Password Policy of my organization.
6. I know my responsibilities as prescribed in the IS Password Policy to enhance the IS security of my organization.
7. I have the necessary skills to fulfill the requirements of the IS Password Policy.
8. I have the necessary knowledge to fulfill the requirements of the IS Password Policy
9. I have the necessary competencies to fulfill the requirements of the IS Password Policy
10. To me, complying with the requirements of the IS Password Policy is __ unnecessary…necessary
11. To me, complying with the requirements of the IS Password Policy is _____ unbeneficial…beneficial
12. To me, complying with the requirements of the IS Password Policy is ___unimportant…important

13. To me, complying with the requirements of the IS Password Policy is _____

    useless…useful

14. I intend to comply with the requirements of the IS Password Policy of my organization in the future.

15. I intend to protect information and technology resources according to the requirements of the IS Password Policy of my organization in the future.

16. I intend to carry out my responsibilities prescribed in the IS Password Policy of my organization when I use information and technology in the future.

Appendix B: Screening Survey Questions

Do you work for an organization in the United States?

Yes

No

Has your employer established an information security policy including a password policy?

Yes

No

To what extent are you aware of the regulations prescribed by the information security policy (ISP) of your organization?

1 Completely Unaware

2 Very Unaware

3 Somewhat Unaware

4 Aware

5 Somewhat Aware

6 Very Aware

7 Completely Aware

To what extent are you aware of the regulations prescribed by the password policy of your organization?

1 Completely Unaware

2 Very Unaware

3 Somewhat Unaware

4 Aware

5 Somewhat Aware

6 Very Aware

7 Completely Aware

Hours of computer usage per day for work

Appendix C: Survey Questions and Instructions

For questions 1-7, please provide a response on a scale of one to seven (where 1 = Not at All — 7 = Very Much).

1. Overall, I am aware of the potential security threats and their negative consequences.
2. I have sufficient knowledge about the cost of potential security problems.
3. I understand the concerns regarding information security and the risks they pose in general.
4. I know the rules and regulations prescribed by the IS Password Policy of my organization.
5. I understand the rules and regulations prescribed by the IS Password Policy of my organization.
6. I know my responsibilities as prescribed in the IS Password Policy to enhance the IS security of my organization.

For questions 7 through 9, please provide a response on a scale of 1 to 7 where 1 = Almost Never; 2 = Very Rarely; 3 = Rarely; 4 = Occasionally; 5 = Frequently; 6 = Very Frequently; 7 = Almost Always.

7. I have the necessary skills to fulfill the requirements of the IS Password Policy.
8. I have the necessary knowledge to fulfill the requirements of the IS Password Policy
9. I have the necessary competencies to fulfill the requirements of the IS Password Policy

For questions 10 through 13, please select a response on a scale of 1-7 where 1 = Extremely; 2 = Quite; 3 = Slightly; 4 = Neither; 5 = Slightly; 6 = Quite; 7 = Extremely.

10. To me, complying with the requirements of the IS Password Policy is _____
    unnecessary…necessary
11. To me, complying with the requirements of the IS Password Policy is _____
    unbeneficial…beneficial
12. To me, complying with the requirements of the IS Password Policy is _____
    unimportant…important
13. To me, complying with the requirements of the IS Password Policy is _____
    useless…useful

For questions 14 through 16, please provide a response on a scale of 1-7 (where 1 = Strongly Disagree — 7 = Strongly Agree).

14. I intend to comply with the requirements of the IS Password Policy of my organization in the future.
15. I intend to protect information and technology resources according to the requirements of the IS Password Policy of my organization in the future.
16. I intend to carry out my responsibilities prescribed in the IS Password Policy of my organization when I use information and technology in the future.

Appendix D: Permission to Use Survey Instrument

EA

Ernest Anye
Fri 9/1/2017, 8:22 PM
burcu.bulgurcu@bc.edu; izak.benbasat@sauder.ubc.ca; hasan.cavusoglu@sauder.ubc.ca

Reply all

Dr. Bulgurcu,

I am a doctoral student in the Doctor of Information Technology (DIT) program at Walden University. I am currently working on my doctoral study. I am writing to seek your permission to use your survey instrument published in the article "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness."

The focus of my study is to explore the factors that affect employee compliance with information system password policies. Specifically, I will be investigating the relationship between employees' perceptions towards password policy, information security awareness, password self-efficacy, and employees' intentions to comply with password policies (dependent variable). If you grant me permission to use your instrument, I would also like to modify some of the items to reflect an examination of compliance with password policies rather than information security policies in general.

I would greatly appreciate your kind permission to use your survey, and also to modify some items. I am looking forward to your response.

Sincerely,

Ernest Anye
Doctor of Information Technology Program
Walden University
U.S.A.

BB

Burcu Bulgurcu <burcu.bulgurcu@bc.edu>
Mon 9/4/2017, 3:07 PM

Dear Ernest,

Thank you for your interest in our study. You're welcome to use our survey instrument. Please let me know if you have any questions.

All the best,

Burcu

Burcu Bulgurcu, Assist. Professor of Information Systems
Boston College, Carroll School of Management
Tel: 617-552-1256; Office: 454B Fulton Hall