Improving Employees’ Compliance with Password Policies

Enas Albataineh

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

Part of the Business Administration, Management, and Operations Commons, Computer Engineering Commons, Computer Sciences Commons, and the Library and Information Science Commons

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.
Improving Employees’ Compliance with Password Policies

by

Enas Saleh Albataineh

A dissertation submitted in partial fulfillment of the requirements for degree of Doctor of Philosophy in Information Systems

College of Computing and Engineering
Nova Southeastern University

2021
We hereby certify that this dissertation, submitted by Enas Albataineh conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Ling Wang, Ph.D.  
Chairperson of Dissertation Committee  
7/28/21  
Date

Mary Harward, Ph.D.  
Dissertation Committee Member  
7/28/21  
Date

Junping Sun, Ph.D.  
Dissertation Committee Member  
7/28/21  
Date

Approved:

Meline Keverykian, Ed.D.  
Dean, College of Computing and Engineering  
7/28/21  
Date

College of Computing and Engineering  
Nova Southeastern University  
2021
Employees’ lack of compliance with password policies increases password susceptibility, which leads to financial damages to the organizations as a result of information disclosure, fraud, and unauthorized transactions. However, few studies have examined what motivates employees to comply with password policies.

The purpose of this quantitative cross-sectional study was to examine what factors influence employees’ compliance with password policies. A theoretical model was developed based on Protection Motivation Theory (PMT), General Deterrence Theory (GDT), Theory of Reasoned Action (TRA), and Psychological Ownership Theory to explain employees’ compliance with password policies.

A non-probability convenience sample was employed. The sample consisted of employees who work at organizations that have password policies to comply with. Only employees who use passwords to log in to the organizational accounts can participate. A total of 151 responses were collected using an adapted survey instrument with a Likert scale. Data were analyzed using the Statistical Package for the Social Science (SPSS) software and the Smart Partial Least Square (SmartPLS) software.

The results of this study revealed that self-efficacy, response efficacy, and perceived certainty sanction have a positive influence on employees’ intention to comply with password policies. Employees’ intention to comply with password policies was also found to have a positive influence on employees’ actual compliance. Conversely, the study revealed that perceived vulnerability threat, perceived severity threat, perceived severity sanction, psychological ownership, and response cost have an insignificant influence on employees’ intention to comply with password policies.

This study has practical and theoretical contributions in Information Systems (IS) literature. It bridged the existing gap by developing a theoretical model and determining what factors influence employees’ compliance with password policies. Organizations can effectively tailor initiatives by focusing on the most impactful predictors to motivate employees’ compliance with password policies.
Acknowledgments

I would like to express my sincere appreciation and gratitude to my committee chair, Dr. Ling Wang whose vision, enthusiasm, and leadership truly exemplified a genuine scholar mentorship. Dr. Wang, I thank you for your support and for guiding me throughout my trajectory. I would also like to express my appreciation to my committee members, Dr. Mary Harward and Dr. Junping Sun who continuously guided this research, and their scientific stance paved the way for successfully executing this study. I would like also to thank Dr. John D’Arcy and Mr. Sebastian Kurowski who helped me with their professional knowledge. Finally, I would like to thank my peers Dr. Ayman Alfaid and Dr. Vasilka Chergarova for their continued support.

I would like to dedicate this work to my family, especially my parents who encouraged me and believed in me. I would like also to thank my brother Dr. Mohamed Bataineh who supported me and encouraged me throughout this journey. Finally, I would like to express my deepest love and gratitude to my husband, Dr. Nashat Abualhaija and my children Salah and Celine who never gave up on my dreams. I love you and I thank you for your support and encouragement; I will be forever grateful.
Table of Contents

Abstract iii
List of Table vii
List of Figures viii

Chapters
1. Introduction 1
   Background 1
   Problem statement 2
   Goal Statement 6
   Research Questions 8
   Relevance and significance 8
   Barriers and Issues 10
   Assumptions, Limitations, and Delimitations 11
   Definition of Items 11
   Summery 13

2. Review of the Literature 15
   Overview 15
   Theoretical Foundation 16
   Hypotheses 20
   Past Literature and Identification of Gaps 27
   Analysis of the Research Methods Used 32
   Synthesis of the Literature 33
   Summary 34

3. Methodology 36
   Overview of Research Design 36
   Specific Research Method 37
   Instrumentation 38
      Instrument Development 38
      Instrument Reliability 41
      Instrument Validity 44
   Population and Sample 46
   Pre-analysis Data Screening 47
   Data Analysis 47
   Ethical Consideration 49
   Format for presenting results 49
   Resource requirements 49
   Summary 50
4. Results 51
   Overview 51
   Phase One-Delphi Study 51
   Phase Two- Custom Qualification Technique 55
   Phase Three- Pilot Study 56
   Phase Four- Actual Data Collection Technique 61
     Pre-analysis Data Screening 61
     Test of Assumptions 62
     Demographics Analysis 64
     Reliability and Validity 65
   Research Hypotheses 69
   Summary 75

5. Conclusions, Implications, Recommendations, and Summary 77
   Conclusions 77
   Limitations 82
   Implications 83
   Recommendations 84
   Summary 85

Appendices 89
A. Survey Questionnaire 90
B. IRB Exempt Initial Approval Memo 97
C. IRB Amendment Approval Memo 99
D. Custom Qualification Questions 101
E. Pilot Study’s Factor Analysis 102
F. Test of Assumptions 104

References 107
List of Tables

Tables

1. Constructs, Adapted Items, and Sources 39
2. Reliability of the Original Items 43
3. Revised Adapted Survey Instrument 52
4. Reliability of Scale Based on a Pilot Study 57
5. Cronbach’s Alpha if an Item is Deleted 57
6. Last Version of the Revised Instrument 59
7. Demographic Description 64
8. Construct Reliability and Convergent Validity 67
9. Discriminant Validity 68
10. Summary of Hypotheses Testing for H1a-H2 75
List of Figures

Figures

1. Proposed Theoretical Model 19
2. Path Coefficients 70
3. PLS Analysis Results for Factors that Influence Employees’ Compliance with Password Policies 72
4. Bootstrapping Analysis Results for Factors that Influence Employees’ Compliance with Password Policies 74
5. Histogram 104
6. P-P Plot 104
7. Collinearity Statistics 105
8. Scatter plot 105
10. Cook’s Distance Statistics 106
Chapter 1

Introduction

Background

Password has been the most preferred authentication method for many users despite its shortcomings (Stewart et al., 2008). Furthermore, it has been a major strategy to protect information and to limit accessing sensitive data for many individuals and organizations (Furnell et al., 2004). Moreover, it is projected that using password will remain the most common authentication method in the future (Lo, 2016). Unfortunately, users have misunderstandings regarding the meaning of a strong password and password security models (Ur et al., 2016). Additionally, it has been suggested that users lack the motivation to comply with the challenges and requirements of password guidelines (Adams & Sasse, 1999). Consequently, users develop poor password practices, such as reusing the same password for different accounts (Abbott et al., 2018; Stobert & Biddle, 2014), resetting password that is related to the previous one (Habib et al., 2018), and writing password down (Lo, 2016; Stobert & Biddle, 2014).

According to Lo (2016), changing a password by revising the previously used one makes it guessable by brute-force and dictionary attacks, and writing the password down makes it accessible by unauthorized persons. Brute-force attacks try all different combinations of password's characters to crack it down, depending on raw computing
power (Bošnjak et al., 2018). On the other hand, the dictionary attack is described as a
type of brute-force technique that uses a database dictionary to guess all possible
passwords (Chakrabarti & Singha, 2007). Therefore, to enhance the strength of a selected
password, the user is required to abide by a given set of rules. These rules are commonly
referred to as password policies. These policies are considered as the essential foundation
to develop and implement efficient and effective passwords (Walters & Matulich, 2011).
Yildirim and Mackie (2019) defined password restriction policies as “a series of rules
which determine the content and format of the passwords accepted by an authentication
system. These policies are used by system administrators to enhance computer security
by guiding users to create more secure passwords” (p. 744).

**Problem Statement**

The main research problem that this study addressed was employees’ lack of
compliance with password policies. Lack of compliance with password policies increases
password vulnerability and causes numerous security issues (Choong et al., 2014; Habib
et al., 2018; Inglesant & Sassa, 2010; Shay et al., 2010). Compromised passwords may
eventually lead to substantial financial damages to individual users and organizations as a
result of information disclosure, fraud, and unauthorized transactions (Wakefield, 2004).
Similarly, insecure password practices can cause severe security breaches costing
companies millions of dollars (Ives et al., 2004). According to Choong et al. (2014),
employees cope with password policies’ requirements by making a minor modification to
the current password, choosing easy-to-remember passwords, and writing them down. In
2010, Shay et al. carried out qualitative research on university students, staff, and faculty
to understand users’ behaviors and perceptions towards password policies that required
them to revise their passwords frequently. The results of the study revealed that most users find password policies annoying although they believe that password policies provide sufficient security. It was also evident that most users had difficulties in complying with strict password requirements. Therefore, they share their passwords and modify old passwords by adding characters and letters. Habib et al. (2018) asserted that employees undermine the policy of password expiration by expanding and modifying their previous passwords, which hinder the security goal of resetting passwords. Moreover, Inglesant and Sassa (2010) examined password policies and practices among staff members and found that it is challenging to comply with the requirements of password policies when organizational password policies are firm. As a result of the difficulties in complying with firm password policies, employees have low security motivations to comply with the password policies (Adams & Sasse, 1999), whereas employees’ behavioral motivations have a significant role in performing secure behaviors (Blythe et al., 2015; Posey et al., 2015; Sommestad et al., 2015).

Previous studies have explored extensively employees’ security behaviors in different Information Systems (IS) contexts. For example, Sommestad et al. (2015) associated employees’ attitudes toward IS policies, perceived norm, and self-efficacy with their intention to comply with overall IS policies. Herath and Rao (2009) examined the influence of employees’ attitudes toward IS policies, perception of security threats, and perception of sanctions on their intention to comply with IS policies. Posey et al. (2015) assessed the effect of employees’ commitments on their motivations to engage in protection behaviors in order to protect organizational information assets. Johnston and Warkentin (2010) assessed the effect of fear appeal on complying with the recommended
security actions in order to mitigate threats. Additionally, Blythe et al. (2015) investigated the motivators and barriers of employees’ compliance with IS policies.

Although several studies have been conducted to predict employees’ behaviors in different IS contexts (Blythe et al., 2015; Herath & Rao, 2009; Johnston & Warkentin, 2010; Posey et al., 2015; Sommestad et al., 2015), few studies have been done specifically to better understand employees’ behaviors toward compliance with password policies (Anye, 2019; Choong & Theofanos, 2015). Anye (2019) as well as Choong and Theofanos (2015) effectively associated employees’ attitudes toward password policies with their intentions to comply with password policies. Anye (2019) recommended future research to expand the findings by examining how other factors, such as sanctions and threat appraisal, influence employees’ intention to comply with password policies based on General Deterrence Theory (GDT) and Protection Motivation Theory (PMT) respectively. Based on GDT, previous studies have associated employees’ perception of severity and certainty sanctions negatively with their intention to misuse IS resources (D’Arcy & Devaraj, 2012; D’Arcy et al., 2009), and positively with their intention to comply with IS policies (Chen et al., 2012). D’Arcy et al. (2009) defined sanction as a punishment for breaking rules.

On the other hand, PMT is based on both threat appraisal and coping appraisal, and their influence on individuals’ protection motivation (Rogers, 1975, 1983). Mwagwabi et al. (2014), as well as Mwagwabi (2015) utilized PMT to investigate how Internet users’ perceptions of password and security threats influence their intention to comply with password guidelines when they login to their email accounts. They found that (1) perceived threat, perceived password effectiveness (response efficacy), and
password self-efficacy positively influence Internet users’ intentions to comply with password guidelines, (2) response cost is negatively associated with the intention to comply with password guidelines, and (3) perceived vulnerability is not related to the intention to comply with password guidelines. Likewise, in 2017, Kusyanti and Sari examined students’ intention to change password after receiving a default password and found that response cost is negatively associated with the intention to change passwords. In addition, they found that perceived severity, response efficacy, and fear are positively associated with the intention to change passwords, but not perceived vulnerability.

Conversely, Ifinedo (2012) as well as Siponen et al. (2014) found that perceived vulnerability positively predicts intention to comply with IS policies in organizational settings. Therefore, Mwagwabi (2015) suggested utilizing PMT in organizational settings, where users would behave differently. Based on the previous literature, employees’ perceptions of threat vulnerability, threat severity, response efficacy, self-efficacy, response cost, severity of sanction, and certainty of sanction can be predictors to their intention to comply with password policies.

Menard et al. (2018) noted that previous studies have successfully explained IS behavioral intention by applying psychological ownership theory in IS domain. Psychological ownership is described as individuals’ developed feelings of ownership toward a target (Pierce et al., 2003). In 2018, Menard et al. assessed the effect of employees’ psychological ownership of the information on their protection motivations and intentions to not protect information, and they recommended examining the impact of psychological ownership on different types of security behaviors because increasing perceived psychological ownership of the information within an organization might be an
optimal practice to motivate secure behaviors. Accordingly, employees’ perception of psychological ownership to their organizational account can be a predictor to their intention to comply with password policies.

Besides the limited research that has examined specifically what factors influence employees’ intention to comply with password policies, there is a lack of password research that links the intention to comply with the actual password compliance behaviors, and there is a need for more studies to determine how intention predicts actual compliance, which is a new avenue for future research (Mwagwabi, 2015; Mwagwabi et al., 2018). Nevertheless, it has been found a positive relationship between intention and actual behaviors in different IS contexts (Boss et al., 2015; Liang & Xue, 2010; Siponen et al., 2014; Sommestad et al., 2015).

This study addressed the scarcity of research on employees’ lack of compliance with password policies by investigating the roles of employees’ perceptions of threat vulnerability, threat severity, response efficacy, self-efficacy, response cost, severity of sanction, certainty of sanction, and psychological ownership. Determining what factors influence employees’ compliance with password policies will help organizations to tailor initiatives, such as education and training, by focusing on the most impactful predictors, which will motivate employees to comply with password policies.

**Goal Statement**

The main goal of this quantitative cross-sectional study is to examine what factors influence employees’ compliance with password policies. Specifically, this study aimed to determine what influences employee’s compliance with password policies by examining the relationship between the independent variables (perceived vulnerability
threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, & perceived psychological ownership) and the mediating variable (intention to comply with password policies), as well as the relationship between the mediating variable (intention to comply with password policies) and the dependent variable (actual compliance with password policies).

This study was built based on previous studies that were conducted by Mwagwabi (2015), D'Arcy et al. (2009), Menard et al. (2018), and Siponen et al. (2014). Mwagwabi (2015) investigated how Internet user’s perceptions of passwords and security threats influence intention to comply with password guidelines based on PMT. D'Arcy et al. (2009) utilized GDT to examine the effect of perception of sanctions in deterring users’ misuse of IS resources. Menard et al. (2018) assessed the effect of employees’ perceptions of psychological ownership on their intentions to not protect information. Moreover, Siponen et al. (2014) examined the relationship between the intentions to comply with IS policies and the actual compliance behaviors, using Theory of Reasoned Action (TRA).

To accomplish this goal, this study adopted constructs and developed a theoretical model based on PMT, GDT, and the psychological ownership theory to examine employee’s intention to comply with password policies and to extend the model based on TRA to link the intention to comply with password policies with the actual compliance behaviors. Intention to comply with password policies, which is the mediating variable, will work as a function of independent variables to understand the dependent variable.

PMT theorizes that when threat evokes, individuals evaluate the situation of threat cognitively through threat appraisal and its coping mechanism (Rogers, 1975, 1983).
GDT posits that the more severity and certainty of sanctions, the more the individuals will be prevented from committing an illicit act (Gibbs, 1975). Moreover, psychological ownership theory postulates that when the perception of ownership increases, user’s motivation to perform behaviors increases to maintain the sense of self-identity, security, and control (Furby, 1978). Additionally, TRA posits that individuals’ intentions predict their actual behaviors (Fishbein & Ajzen, 1975).

**Research Questions**

RQ1: What is the relationship between (a) perceived vulnerability threat, (b) perceived severity threat, (c) response efficacy, (d) self-efficacy, (e) response cost, (f) perceived severity sanction of noncompliance, (g) perceived certainty sanction of noncompliance, (h) perceived psychological ownership of the organizational account, and employees’ intention to comply with password policies?

RQ2: What is the relationship between employees’ intention to comply with password policies and their actual compliance with password policies?

**Relevance and Significance**

Due to the difficulties in complying with the strict password policies, literature suggests that employees’ motivation to comply with password policies is low, which increases passwords’ susceptibility (Choong et al., 2014; Habib et al., 2018; Inglesant & Sassa, 2010; Shay et al., 2010). Compromising passwords causes financial damages to the organizations as a result of fraud, information disclosure, and unauthorized transactions (Wakefield, 2004).

Limited research has been conducted to examine specific factors that influence employees’ intention to comply with password policies (Anye, 2019; Choong &
Theofanos, 2015). In addition, there is a shortage in research that associates intention to comply with actual password compliance (Mwagwabi, 2015; Mwagwabi et al., 2018). This study addressed the scarcity of research by assessing the relationship between employees’ perceptions of threat vulnerability, threat severity, response efficacy, self-efficacy, response cost, severity of sanction, certainty of sanction, psychological ownership, and their intention to comply with password policies, as well as the relationship between intentions to comply with the actual password policies compliance in order to complete the understanding of employees’ compliance with password policies.

This study contributed to practitioners and information security literature in the area of IS policies by investigating factors that specifically influence employees’ compliance with password policies. This study filled the existing knowledge gap on the factors that motivate password policy compliance behaviors by adopting and developing a theoretical model based on four behavioral theories: PMT, GDT, TRA, and psychological ownership theory. In addition, the theoretical model constructs were examined to better understand employees’ compliance with password policies. This proposed theoretical model can be used in future research.

Determining the factors that influence password policy compliance will provide organizations with insights into how to motivate compliance with password policies and will enable organizations to effectively tailor initiatives, such as training and education, to promote employees’ password compliance in order to protect their passwords from being compromised. Consequently, organizational financial loss and information disclosure will be prohibited.
Weirich and Sasse (2001) asserted that forcing password policies is not sufficient to ensure compliance, but there is a need to design policies, trainings, and tutorials with persuasive power to persuade users to do so. Puhakainen and Siponen (2010) as well as Mwagwabi et al., (2014) noted that training techniques require utilizing methods that motivate and activate users to comply with policies. Puhakainen and Siponen (2010) asserted that the training approach should be based on theoretical evaluation. Therefore, this study will help in tailoring initiatives to enhance employees’ compliance with password policies based on the results of examining the constructs of PMT, GDT, TRA, and psychological ownership theory. In addition, the results of this study can be considered by password policies designers.

Moreover, associating employees’ perceptions with their password policies compliance would help organizations to inspire employees’ password policies compliance by focusing on the most impactful predictors. For example, inspiring a sense of psychological ownership would be an optimal practice to induce the employees to perform secure behaviors (Menard et al., 2018).

**Barriers and Issues**

This study used a survey instrument to collect data from employees who work at organizations and have organizational accounts to log in. The barriers in this study are in achieving a sufficient sample size, in using a convenience sample which negatively affects the generalizability of the study, and in collecting data about security behaviors. The participants would not be willing to share information about their compliance with password policies. To address this concern, the participants were told that the responses will be anonymous and used only for the study. Another issue is the need of an expert
panel to review the adapted instrument before collecting data. Lastly, the institutional review board (IRB) approval form Nova Southeastern University (NSU) must be received before collecting data.

Assumptions, Limitations, and Delimitations

The assumptions of this study include that the participants are honest in responding to the questionnaire, and all the hypotheses are significantly true. In addition, this study assumed that the quantitative cross-sectional design would address the research problem since the main goal is to examine the relationship between employees’ perceptions and compliance with password policies.

The limitations of this study may be the sample size and convenience sample method, which would affect the accuracy of results and the generalizability, respectively. Another limitation is that this study is based on self-reported data, which is considered a common bias technique. In addition, the survey instrument needs an expert panel to review it because its items are adapted.

The scope of this study is employees’ compliance with password polices which is under IS security behaviors context. The participants were encouraged to truthfully respond by ensuring their privacy and confidentiality. In addition, the survey instrument was simple and easy to understand in order to encourage participants to complete the survey.

Definition of Terms

The terms in this study are defined as follow:

Protection motivation- “an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity” (Rogers, 1975, p. 98).
**Thread appraisal**- “threat appraisal evaluates the maladaptive behavior. Factors comprising the threat-appraisal process are maladaptive response rewards (intrinsic and extrinsic) and the perception of threat (severity and vulnerability)” (Floyd et al., 2000, p. 410).

**Coping appraisal**- “the coping-appraisal process evaluates the ability to cope with and avert the threatened danger. Factors comprising the coping-appraisal process are efficacy variables (both response efficacy and self-efficacy) and response costs” (Floyd et al., 2000, p. 410-411).

**Perceived threat severity**- “degree of harm associated with the threat” (Herath & Rao, 2009, p.111).

**Perceived threat vulnerability**- “probability of the threat occurring” (Herath & Rao, 2009, p. 111).

**Response efficacy**- “the belief that the adaptive response will work, that taking the protective action will be effective in protecting the self or others” (Floyd et al., 2000, p. 411).

**Self-efficacy**- “the perceived ability of the person to actually carry out the adaptive response” (Floyd et al., 2000, p. 411).

**Response cost**- “any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response” (Floyd et al., 2000, p. 411).

**Sanction**- a punishment for breaking rules (D’Arcy et al., 2009).

**Severity sanction**- “degree of punishment” (D’Arcy et al., 2009, p. 83).

**Certainty sanction**- “the extent to which an individual believes that criminal behavior will be detected” (Siponen et al., 2010, p. 69).
Psychological ownership- “state where an individual feels as though the target of ownership or a piece of that target is ‘theirs’ (i.e., it is MINE!)” (Pierce et al., 2003, p. 5).

Intentions- “intentions are assumed to capture the motivational factors that influence a behavior; they are indications of how hard people are willing to try, of how much of an effort they are planning to exert, in order to perform the behavior” (Ajzen, 1991, p. 181).

Summary

This introductory chapter provided a research worthy problem in the field of IS, specifically focusing on employees’ compliance with password policies. Lack of compliance with password policies increases passwords vulnerability, which leads to financial losses to organizations. In this chapter, valid literature supported the problem and its need to be addressed.

This chapter also identified the main goal of this study. The main goal is to examine factors that influence employees’ compliance with password policies. Specifically, this study examines the relationship between perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, perceived psychological ownership, intention to comply with password policies, and actual compliance with password policies. A theoretical model is developed based on PMT, GDT, TRA, and psychological ownership theory to explain employees’ compliance with password policies.

The significance of this study was also addressed. By determining what factors influence employees’ compliance with password policies, organizations can tailor initiatives by focusing on the most impactful predictors to motivate employees’
compliance with password policies. In addition, this chapter addressed the assumptions, limitations, delimitations, barriers, and issues of the study.
Chapter 2

Review of the Literature

Overview

Passwords continue to be the most common authentication technique in most of organizations despite their vulnerability (Stewart et al., 2008). Therefore, many companies have turned to the trend of employing password policies to protect passwords. Despite these measures taken by many organizations, employees fail to abide by these policies (Choong et al., 2014; Habib et al., 2018). This chapter focuses on identifying the gaps and addressing the lack in the literature about factors that influence employees’ compliance with password policies by understanding employees’ compliance with password policies and what factors would influence their behaviors in complying with password policies. The key issue is to improve employees’ compliance with password policies to protect organizational passwords from being compromised.

Understanding employees’ IS behaviors and developing a theoretical model will help improving employees’ compliance with password policies. This study developed a theoretical model, grounded in four behavioral theories: PMT, GDT, TRA, and psychological ownership theory. This literature review helped in understanding the role of these theories’ constructs as factors that would be associated with employees’
password policies compliance. Additionally, based on the review of literature, most of the studies in IS context that applied PMT, GDT, TRA, and psychological ownership theory utilized surveys to examine the association between constructs.

To summarize, this literature review chapter discusses the theoretical foundation of the study, provides a review of previous literature to identify gaps, includes an analysis of the research methods used, and gives a synthesis of the literature.

**Theoretical Foundation**

The theoretical foundation of this study was based on PMT, GDT, TRA, and psychological ownership theory. GDT is rooted in classic criminology from the late 18th century (Mendes & McDonald, 2001) and started to be investigated by sociologists and psychologists in the early to mid-20th century (Mendes, 2004). GDT is a dependable theory from an economic view as it embraces that increasing certainty or severity of punishment will raise the cost expectation that would prevent criminals from committing illegal acts (Mendes & McDonald, 2001). If the individuals anticipate severe and certain penalties to offset the reward of an intentional act, then they will not commit the act (Paternoster, 2010).

PMT was developed in 1975 and revised in 1983 by Rogers. PMT was originally utilized in health field to explain how fear appeals affect health behaviors (Rogers, 1975). According to Rogers (1975), there are three cognitive appraisal processes: severity of threat, probability of threat occurrence, and belief of coping behavior efficacy in mitigating threat. In 1983, Rogers revised PMT by incorporating self-efficacy expectancy. The outcome of these cognitive appraisal processes is called protection motivation.
Psychological ownership, on the other hand, is formed by individuals’ developed feelings of ownership as a part of effective and cognitive thought processes, which makes strong emotional relations between the individual and object (Pierce et al., 2003). Pierce et al. (2001) proposed that psychological ownership emerged to satisfy human motives and suggested that psychological ownership is rooted in three main motives: self-identity, control, and having a place. When the individual feels a high level of psychological ownership towards people, assets, and organization, the individual acts as an extension of owner identity, experiences a high degree of control of the target, and has a high sense of place as his or hers.

PMT, GDT, and psychological ownership theory have been widely applied in IS studies. For example, GDT is a prominent theoretical foundation of employees’ misuse of IS resources (D’Arcy et al., 2009; D’Arcy & Devaraj, 2012; Willison et al., 2018) and employees’ security policy compliance and non-compliance (Chen et al., 2012; Kuo et al., 2017; Siponen & Vance, 2010). Additionally, PMT is a widely used motivation theory that explains and influences users’ protection motivation behaviors in different fields such as IS security. Boss et al. (2015) as well as Posey et al. (2015) utilized PMT based on threat appraisal (perceived severity threat, perceived vulnerability threat, & maladaptive rewards), and coping appraisal (self- efficacy, response efficacy, & response cost) to examine how they influence individuals’ security behaviors in order to mitigate threat. Moreover, psychological ownership theory has been employed for understanding employees’ behaviors by explaining employees’ perception of ownership of their organization (Menard et al., 2018). Therefore, it is a rationale for leveraging GDT, PMT, and psychological ownership theory’s constructs to predict and understand employees’
motivation in complying with password policies since they have explained IS security behaviors successfully. The integration of these grounded theories’ constructs also leads to develop more powerful and suitable model that explain employees’ intention to comply with password policies.

Based on the literature, factors that influence employees’ intention to comply with password policies and its relation to the actual compliance are not explained sufficiently. The researcher attempted to bridge the gap by proposing a theoretical model using PMT, GDT, and psychological ownership theory to examine employee’s intention to comply with password policies and to extend the model using TRA to associate employees’ intention to comply with password policies with the actual compliance behaviors. TRA was developed by Fishbein and Ajzen (1975), and it predicts how individuals behave based on their intentions, where intention is affected by individuals’ attitudes toward the behaviors and subjective norm. In 1991, TRA was extended by adding behavioral control to the model by Ajzen to develop TPB. According to Ajzen (991), intentions capture the influence of motivation and willingness to perform a specific behavior.

To accomplish, this study integrated the construct of (perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, perceived psychological ownership, intention to comply with password policies, & actual compliance) into one model to understand what motivates employees’ password policies compliance. The model represents the relationship between the independent variables (perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, & perceived psychological ownership)
and the mediating variable (intention to comply with password policies) as well as the relationship between the mediating variable and the dependent variable (the actual compliance with password policies). Figure 1 illustrates the proposed theoretical model.

**Figure 1**

*Proposed Theoretical Model*
Hypotheses

The constructs in this quantitative cross-sectional study were leveraged and identified based on the theoretical foundation. PMT constructs are perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, and response cost. The threat appraisal component of PMT is presented as perceived vulnerability threat and perceived severity threat, whereas coping appraisal component of PMT is presented as response efficacy, self-efficacy, and response cost. GDT constructs are perceived severity sanction and perceived certainty sanction. Perceived psychological ownership construct is also used, which is based on psychological ownership theory. Each construct is defined below, and all hypotheses were proposed based on previous studies’ findings.

Perceived Vulnerability Threat

Zhang and McDowell (2009) stated that “perceived vulnerability concerns the susceptibility a person has to a threat” (p. 185). Weak passwords can be compromised by dictionary attack techniques, which try all the possible password combinations (Chakrabarti & Singha, 2007). Written passwords can be accessible by unauthorized persons (Lo, 2016). In addition, passwords can be guessed by learning others’ personal information such as pets’ names and birthdays (Micallef & Arachchilage, 2017). Individuals who perceive a high degree of password vulnerability will be more concerned with protection motivation behavior to protect passwords (Zhang & McDowell, 2009).

Many studies have associated perceived vulnerability threat with protection motivation behaviors. For example, Ifinedo (2012) found that perceived vulnerability positively predicts the intention to comply with IS policies among business managers and IS professionals. Similarly, Siponen et al. (2014) utilized PMT to explain the adherence
of employees to IS policies and found that perceived vulnerability predicts employees’ intention to comply with IS policy. On the other hand, other researchers revealed that perceived vulnerability is not related to the intention to comply with password guidelines (Mwagwabi et al., 2014; Mwagwabi, 2015) or students’ intention to change passwords (Kusyanti & Sari, 2017). Mwagwabi et al. (2018) as well as Mwagwabi (2015) failed to explain why perceived vulnerability is not related to compliance with password guidelines among Internet users and suggested that perceived vulnerability differs in personal and organizational settings. Hence, the hypothesis is:

H1a: Perceived vulnerability threat is positively related to employees’ intention to comply with password policies.

Perceived Severity Threat

Zhang and McDowell (2009) stated that “perceived severity assesses how severe a person believes a threat will be to his or her life” (p. 184). Password breaches can lead to data exposure to hackers or public, and financial losses; therefore, when individuals perceived a high threat severity, they will be more motivated to perform protection motivation acts to protect their password from being compromised (Zhang & McDowell, 2009).

Previous studies have associated perceived severity threat with protection motivation behaviors. Ifinedo (2012) found that perceived severity did not predict intention to comply with IS policies among business managers and IS professionals. Likewise, in 2015, Posey et al. assessed the motivation of insiders’ security behaviors in organizational using PMT and found that threat severity was insignificantly related to protection motivation. On the other hand, in 2014, Siponen et al. utilized PMT to explain
the adherence of employees to IS policies and found that perceived severity positively affects employee’s intention to comply with IS policy. Additionally, Mwagwabi et al. (2014) as well as Mwagwabi (2015) found that perceived threat influences Internet users’ intentions to comply with password guidelines. Although there is a contradiction in findings among studies, Zhang and McDowell (2009) asserted that the more the individuals perceived severity of threat, the more they will perform the recommended action to mitigate the threat. Thus, the hypothesis is as follows:

H1b: Perceived severity threat is positively related to employees’ intention to comply with password policies.

**Response Efficacy**

Rogers (1983) defined response efficacy as the effectiveness of coping responses in preventing the threat. In addition, Herath and Rao (2009) defined response efficacy as “beliefs about whether the recommended coping response will be effective in reducing the threat” (p. 111). Similarly, Zhang and McDowell (2009) stated that “response efficacy evaluates how effective the recommended coping response is in reducing the threat” (p. 187). Floyd et al. (2000) asserted that response efficacy increases the possibility of performing an adaptive response.

Many studies have associated response efficacy with protection motivation behaviors. For example, Johnston and Warkentin (2010) examined the effect of fear appeals on university subject’s compliance with computer security actions that mitigate threats of spyware. They found that response efficacy positively impacts users’ intention to comply with the recommended security actions. Posey et al. (2015) examined the effect of employees’ commitments on their motivation to protect organizational
information assets, and they found that response efficacy was positively related to their protection motivation behaviors. Ifinedo (2012) asserted that response efficacy positively predicts the intention to comply with IS policies among business manages and IS professionals. Moreover, Mwagwabi (2015) as well as Mwagwabi et al. (2014) revealed that perceived password effectiveness influences the intentions to comply with password guidelines. Likewise, Kusyanti and Sari (2017) showed that response efficacy influences students’ intention to change passwords. Thus, the hypothesis is:

H1c: Response efficacy is positively related to employees’ intention to comply with password policies.

*Self-efficacy*

Rogers (1983) defined self-efficacy as “the ability to perform the coping response” (p. 170). Herath and Rao (2009) defined self-efficacy as “one’s ability to perform a task” (p. 111). Posey et al. (2015) defined self-efficacy as “the belief that an individual is personally capable of implementing the proposed coping strategy appropriately” (p. 15). In addition, Maddux and Rogers (1983) defined self-efficacy expectancy as “person’s belief that he or she is or is not capable of performing the requisite behavior” (p. 471). Additionally, Floyd et al. (2000) asserted that self-efficacy increases the possibility of performing the adaptive response.

Previous studies contended that self-efficacy predicts protection motivation behaviors. For example, Johnston and Warkentin (2010) found that self-efficacy positively impacts users’ intention to comply with the recommended security actions. Ifinedo (2012) revealed that self-efficacy positively influences intention to comply with IS policies. In addition, many researchers asserted that self-efficacy is positively related
to employees’ intentions to comply with password policies (Anye, 2019) and to Internet users’ intention to comply with password guidelines (Mwagwabi, 2015; Mwagwabi et al., 2014). Thus, the developed hypothesis is:

**H1d:** Self-efficacy is positively related to employee's intention to comply with password policies.

**Response Cost**

Herath and Rao (2009) defined response cost as “beliefs about how costly performing the recommended response will be” (p. 111). Zhang and McDowell (2009) defined response cost as “a factor in the coping-appraisal process, measures the perceived costs (e.g., time, money, effort) that a person has to pay in taking the protective behavior” (p. 186). For example, time and effort spent to create a strong password, update the previous passwords, and retrieve the forgotten password are barriers that prevent individuals from performing recommended actions (Zhang & McDowell, 2009). According to Kusyanti and Sari (2017), users minimize the cost of response by using the same password for different accounts. In addition, Floyd et al. (2000) asserted that response costs decrease the possibility of performing the adaptive response.

In 2012, Ifinedo asserted that the proposition that response cost is negatively associated with the intention to comply with IS policies was not supported. However, Posey et al. (2015) negatively associated response costs with employees’ protection motivation behaviors that protect organizational information assets. Additionally, Kusyanti and Sari (2017) found that response cost negatively influences students’ intention to change passwords. Accordingly, the hypothesis is:
H1e: Response cost is negatively related to employees’ intention to comply with password policies.

*Perceived Severity Sanction and Perceived Certainty Sanction*

D’Arcy et al. (2009) defined severity sanction as a “degree of punishment” and certainty sanction as a “probability of being punished” (p. 83). However, Siponen et al. (2010) referred certainty to “the extent to which an individual believes that criminal behavior will be detected”, while severity referred to “how harshly it will be punished” (p. 69). D’Arcy and Herath (2011) asserted that certain, severe, and swift sanctions can control users’ illicit behaviors at the workplace. Grasmick and Bryjak (1980) found that perceived severity of punishment is negatively related to illicit behavior only when the perceived certainty is high. In 2009, D’Arcy et al. found that perceived severity of formal sanction is more effective than certainty sanction in deterring IS misuse. In addition, D’Arcy and Devaraj (2012) revealed that the threat of formal sanction has direct and indirect effects on IT resources misuse intention.

Previous studies asserted that sanctions also influence employees’ security policy compliance. For example, Herath and Rao (2009) examined the influence of perception of sanctions on employees’ intention to comply with IS policies and found that perceived certainty of sanction has a positive impact on intention to comply with policy, but not perceived severity sanction. Chen et al. (2012) conducted an experimental study to examine the combined effects of reward and punishment on enforcing security policy compliance. They found that the effects of reward, severity of punishment, and certainty of control are significant in enforcing security policies. In addition, in 2017, Kuo et al. conducted a correlational study to understand the effects of that deterrence on Electronic
Medical Record (EMR) privacy policy compliance among nurses. They showed that the formal sanctions and informal sanctions were effective in deterring nurses from violating EMR. Therefore, the hypotheses are:

H1f: Perceived severity sanction of noncompliance is positively related to employees’ intention to comply with password policies.

H1g: Perceived certainty sanction of noncompliance is positively related to employees’ intention to comply with password policies.

Perceived Psychological Ownership

Psychological ownership is formed when an individual develops feelings of ownership toward an object, which makes strong relations between the individual and that object (Pierce et al., 2003). Menard et al. (2018) extended previous studies based on PMT by showing the impact of psychological ownership and cultural difference. Menard et al. (2018) found that collectivism negatively affects psychological ownership and positively affects the intention not to protect information, whereas psychological ownership negatively affects the intention not to protect information. In 2018, Yoo et al. revealed that psychological ownership has a significant impact on security compliance intention and suggested utilizing psychological ownership to promote employees' security compliance intention. Van Dyne and Pierce (2004) found a positive association between psychological ownership, organizational behaviors, and employees’ attitudes. In addition, Kim and Beehr (2017) asserted that psychological ownership is negatively related to work-place deviant behaviors. Yoo et al. (2018) argued that having a feeling of ownership toward the organizational information assets makes employees identify
themselves in the organization, aware of protecting organizational information, and motivate toward security compliance. Thus, the hypothesis is as follows:

H1h: Perceived psychological ownership of the organizational account is positively related to employees’ intention to comply with password policies.

*Intention to Comply with Password Policies*

Intention is defined as the motivation that influences a specific behavior and the willingness to put effort in order to perform it (Ajzen, 1991). Ajzen asserted that the stronger the intention to perform a specific behavior, the more it is likely to perform that behavior. In 2015, Mwagwabi found that intention to comply and actual password compliance are positively associated but not strong. Mwagwabi believed that there was no strong relationship between intention to comply and the actual behaviors because the passwords were just for the survey, which did not reflect their actual behaviors. In addition, Thompson et al. (2017) as well as Giwah (2019) found a weak relationship between intention and actual mobile device usage. On the other hand, Lau (2020) found a significant positive effect of intention on actual mobile device usage. Siponen et al. (2014) also found that the intention to comply with IS policies is related to the actual compliance. In addition, Boss et al. (2015) implied that intention is related to the actual security behaviors. Thus, the hypothesis is:

H2: Employees’ intention to comply with password policies is positively related to their actual compliance with the password policies.

*Past Literature and Identification of Gaps*

Although most of the studies have focused on IS policy compliance and security behaviors in general (Blythe et al., 2015; Herath & Rao, 2009; Johnston & Warkentin,
few studies have examined specifically what factors influence password policies compliance in organizational settings (Anye, 2019; Choong & Theofanos, 2015). Therefore, these factors are still unknown and need further investigation. Based on reviewing past literature, perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, and perceived psychological ownership were considered to examine what factors influence employees’ compliance with password policies. In addition, this study addressed the scarcity of actual compliance usage as a dependent variable, which creates a gap in IS security literature.

In 2017, Kusyanti and Sari analyzed students’ intention toward changing passwords for Student Academic Information Systems (SAIS) application by adopting PMT constructs, which are perceived vulnerability, perceived severity, response efficacy, response cost, and fear. They found that the factors that influence students’ intention to change passwords are perceived severity, response efficacy, response cost, and fear but not perceived vulnerability. In addition, Mwagwabi et al. (2014) investigated how Internet users’ perceptions of password and security threats influence their intention to comply with password guidelines based on PMT and how these perceptions can be manipulated using fear appeals to improve password guidelines compliance. Mwagwabi et al. found that perceived threat, self-efficacy, and perceived password effectiveness influence the intentions to follow password guidelines but not perceived vulnerability, which support the findings of Kusyanti and Sari (2017) and contradict the findings of other studies (Ifinedo, 2012; Siponen et al., 2014).
Ifinedo (2012) found that perceived vulnerability, self-efficacy, response efficacy, objective norm, and attitude toward compliance positively predict the intention to comply with IS policies among business managers and IS professionals, but not perceived severity and response cost. Moreover, Siponen et al. (2014) utilized PMT, TRA, and Cognitive Evaluation Theory to explain the adherence of employees to IS policies and found that perceived vulnerability, perceived severity, attitude toward IS policy compliance, employees’ belief that they can adhere to IS policy, and social norm toward complying with IS policies positively affect employees’ intention to comply with IS policies. Mwagwabi et al. (2014) suggested that future research compare the intention to comply between users who have been impacted and have not been impacted by hacking to understand the link between perceived vulnerability and user’s intention to comply with password guidelines.

In 2015, Mwagwabi found that: (a) there is no association between perceived vulnerability threat and users’ intention to comply with password guidelines among users who have been impacted by hacking, (b) intention to comply and the actual password compliance are positively associated but not strong, and (c) fear appeals used in this study had no long-term effect on intention to comply with password guidelines. Mwagwabi recommended future research could examine the relationship between the intention to comply with password guidelines and the actual password guidelines compliance and what contributes to the weak prediction of actual behaviors. Mwagwabi’s 2015 study showed that there is no link between perceived vulnerability and intention to comply with password guidelines in the personal account setting, while Ifinedo (2012) as well as Siponen et al. (2014) found a link between perceived vulnerability threat and the
intention to comply with IS policies in the organizational setting. Therefore, the reason for the discrepancy in findings could be the differences in setting as well as the differences in IS context.

Compliance is different between Internet users and employees since users protect their personal information assets while employees protect the organizational assets (Mwagwabi et al., 2018). Perceived psychological ownership explains employees’ perception of ownership of their organizations (Menard et al., 2018). In 2018, Menard et al. extended previous studies that are based on PMT by showing the impact of psychological ownership and culture on intention not to protect information. Menard et al. found that collectivism negatively affects psychological ownership and positively affect the intention not to protect information; on the other hand, psychological ownership negatively affects intention not to protect information. Menard et al. (2018) recommended examining the impact of psychological ownership on different types of security behaviors because increasing perceived psychological ownership of the information within an organization might be an optimal practice to foster a secure environment. Therefore, considering users’ psychological ownership of the information in future research is needed because it would influence the intention to comply with password policies requirements.

Anye (2019) conducted a quantitative correlational study to examine the relationship between employees’ attitudes toward password policies, self-efficacy, information security awareness, and employee intentions to comply with password policies in different business sectors, based on TPB and Social Cognitive Theory. Anye found that both attitudes toward password policies and self-efficacy were significantly
related to employees’ intentions to comply with password policies. Anye recommended future research to examine other factors, such as threat appraisal, sanctions, and how these factors affect users’ intentions to comply with password policies. D’Arcy et al. (2009) as well as D’Arcy and Devaraj (2012) asserted that severity and certainty sanctions have significant effects on deterring employees’ misuse of IS resources. The limitation of Anye’s 2019 study was that all participants were highly aware of IS policies, which might affect their intentions to comply with password policies. In addition, Anye examined the intention to comply with password policies but not the actual compliance.

To conclude, many gaps in literature exist that need further research regarding factors that influence employees’ compliance with password policies. A few studies have specifically explored what factors influence employees’ password policies compliance. Mwagwabi et al. (2014) as well as Mwagwabi (2015) focused on Internet users, when they login to their e-mail accounts, to examine the effect of fear appeals in complying with password guidelines. Mwagwabi (2015) recommended future research to examine fear appeals in organizational settings, where users may behave differently. Mwagwabi (2015) as well as Mwagwabi et al. (2018) also confirmed that there is a lack of password research that links the intention to comply with the actual compliance behaviors, and there is a need for more studies to determine how intention predicts actual security behaviors. Additionally, Anye (2019) recommended future research to expand the findings by examining the influence of sanctions and threat appraisal on password policies compliance based on PMT and GDT. Furthermore, Menard et al. (2018) recommended examining the influence of psychological ownership on different types of
security behaviors because increasing perceived psychological ownership would foster secure behaviors.

**Analysis of the Research Methods Used**

Many studies in IS field that utilized PMT, GDT, TRA, and psychological ownership theory were reviewed in order to determine the research method of this study. Based on the methodologies of the reviewed studies, survey research was the most utilized research method. For example, Anye (2019) conducted a correlational study to examine the relationship between employees’ attitudes towards password policies and their intentions to comply with password policies using an Internet-based survey. In 2009, D’Arcy et al. conducted an empirical study on 269 computer users using a survey instrument to investigate the influence of perceived severity and certainty sanctions on reducing individuals’ intentions to misuse IS resources. Similarly, Hovav and D’Arcy (2012) conducted an empirical study to examine if increasing perceived severity and certainty sanctions would affect the security countermeasures effectiveness in deterring IS misuse behaviors based on national cultures. The sample consisted of 366 participants from the United States and 360 participants from Korea, and the data were collected using survey instrument. In addition, Menard et al. (2018) extended previous studied that are based on PMT by showing the impact of psychological ownership and cultures. The sample consisted of 439 participants, and the data were collected using survey instrument.

Almost all the reviewed studies assessed different types of validity, such as content, construct, and discriminant validity along with the reliability of constructs. Additionally, most of the reviewed studies used a cross-sectional method in collecting
data. Descriptive and inferential statistics were also used in most of the reviewed studies. Univariate descriptive statistics were used to calculate measures of central tendency and variability, whereas inferential statistics were used to infer the outcomes, test the hypotheses, and describe the relationships between variables.

**Synthesis of the Literature**

The developed theoretical foundation is based on PMT, GDT, TRA, and psychological ownership theory. PMT was developed by Rogers (1975, 1983) to explain fear appeals in health field. GDT was developed in 1975 by Gibbs to explain the effect of sanction on preventing criminal acts. In addition, psychological ownership theory was developed by Furby (1978) and posits that individuals’ feelings of ownership motivate them to perform behaviors to maintain the sense of self-identity, power, and security. Additionally, TRA was developed by Fishbein and Ajzen (1975), and it predicts how individuals behave based on their intentions.

Reviewing the literature revealed that many studies were conducted on individuals’ behaviors in different IS contexts (Blythe et al., 2015; Herath & Rao, 2009; Johnston & Warkentin, 2010; Posey et al., 2015; Sommestad et al., 2015). However, few studies have been done specifically to predict employees’ behaviors in complying with password policies (Anye, 2019; Choong & Theofanos, 2015). Anye (2019) as well as Choong and Theofanos (2015) examined the relationship between the attitudes toward password policies and employees’ intentions to comply with password policies. Anye (2019) recommended future research to examine other factors, such as threat appraisal and sanctions. In addition, Menard et al. (2018) suggested examining psychological
ownership construct on different security behaviors to promote practices that foster secure behaviors.

This study utilized existing constructs from PMT, GDT, and psychological ownership theory to determine other factors that influence employees’ intention to comply with password policies. The utilized constructs were perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, and perceived psychological ownership. In addition, although a few studies have been conducted to examine the relationship between intention and actual behaviors in different IS contexts (Boss et al., 2015; Giwah, 2019; Lau, 2020; Liang & Xue, 2010; Siponen et al., 2014), there is a lack of password research that addresses actual password compliance behaviors, which creates a gap in the literature (Mwagwabi, 2015; Mwagwabi et al., 2018). Therefore, this study also utilized TRA to link intention to comply with actual password compliance.

**Summary**

This chapter synthesized literature based on previous studies in IS security behaviors. The literature review explored different theories to develop the theoretical foundation of this study, which is based on PMT, GDT, TRA, and psychological ownership theory attempting to understand how to utilize their constructs in this study: perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, and perceived psychological ownership, which leads to intention to comply with password policies as well as the actual compliance. Not only theories in the previous studies were reviewed,
but also the findings, the gaps, and the methodologies in order to add to the knowledge by determining factors that influence employees’ compliance with password policies.
Chapter 3

Methodology

Overview of Research Design

A quantitative cross-sectional study was conducted using a survey strategy to examine what factors influence employees’ compliance with password policies. Furthermore, this method was used to collect and analyze the numerical data in order to test the hypotheses and answer the research questions. Quantitative research has its philosophical underpinnings in the positivist school of thoughts. Ontologically, positivism claims that there is only one reality in the universe, and it is the researcher’s duty to find the truth (Creswell, 2013). Additionally, the epistemology for this paradigm is based on objectivism where knowledge is generated objectively by the interaction with objects of the universe (Creswell, 2013). Nonetheless, this study aimed to reveal employees’ password policies compliance by examining the relationship as well as the predictions between the constructs using a quantitative cross-sectional approach. Incidentally, the relationship between variables is associative in nature and does not mean causality (Polit & Beck, 2008). This methodology chapter discusses the research method, instrumentation, population and sample, data analysis, format for presenting the results, and resource requirements.
**Specific Research Method**

To address the research problem, a theoretical model based on PMT (Rogers, 1975, 1983), GDT (Gibbs, 1975), and psychological ownership theory (Furby, 1978) was developed to explain employees’ compliance with password policies. A quantitative cross-sectional design was used to assess the relationship between the construct of perceived threat vulnerability, perceived threat severity, perceived response efficacy, self-efficacy, perceived response cost, perceived severity sanction, perceived certainty sanction, perceived psychological ownership, and intention to comply with password policies, as well as the relationship between the intention to comply with password policies and the actual compliance with password policies. The survey is an effective strategy to collect data for testing the aforementioned relationships.

This quantitative cross-sectional study was conducted in a non-contrived setting without interference. The unit of analysis is individuals since the data was collected from each employee. Data was collected using an adapted Likert rating scale survey instrument to determine factors that contribute to employees’ compliance with password policies. The adapted survey collected data for each construct as well as demographics data, such as gender, age, and educational level. The participation letter along with the survey instrument that addresses all variables and demographics questionnaire sent to the participants. Surveys are easy to administer, inexpensive, accessible, convenient, but have a low response rate (Sekaran & Bougie, 2012). Thus, to increase the response rate, a monetary incentive technique was used.

To ensure the validity and reliability of the survey instrument, the instrument was reviewed through a Delphi study and by an expert panel that is knowledgeable in IS
discipline. The reviewed instrument was then pilot tested using a small group of participants before starting actual data collection. Straub (1989) implied that the reliability and content validity of the instrument can be enhanced by a pilot test and expert panel review, respectively. Skulmoski et al. (2007) identified the Delphi method as “an iterative process used to collect and distill the judgments of experts using a series of questionnaires interspersed with feedback” (p. 2). Additionally, Hertzog (2008) suggested that when conducting a pilot study, a sample size of 10 to 40 participants would be sufficient. Based on the pilot and Delphi study’s feedback, the instrument was revised.

**Instrumentation**

*Instrument Development*

For developing a survey instrument in this study, only the items with composite reliability or Cronbach’s alpha values of 0.70 and above were adapted from previous validated studies. According to Straub (1989), adapting instrument by making a major change to the valid instrument without retesting it weakens the validity of the adapted instrument. Therefore, the adapted items were changed slightly. For example, “IS policies” was replaced by “password policies” as presented in Table 1.

For collecting data, a 7-point Likert scale survey instrument ranging from 1= *Strongly Disagree* to 7= *Strongly Agree* was developed (see Appendix A). The level of measurement used is an interval scale for measuring all survey items, which ensures distance equality. After developing the instrument, the instrument internal consistency was tested based on Cronbach’s alpha. Sekaran and Bougie (2012) implied that reliability less than 0.6 is considered poor, in the range of 0.7 is acceptable, and above 0.8 is good.
For this study, the acceptance coefficient of Cronbach’s alpha was 0.7 and above. In addition, the content validity of the instrument was tested by conducting Delphi study.

Table 1

*Constructs, Adapted Items, and Sources*

<table>
<thead>
<tr>
<th>Perceived Vulnerability Threat</th>
<th>PV1</th>
<th>PV2</th>
<th>PV3</th>
<th>PV4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I know my organizational password could be vulnerable to security breaches if I don’t adhere to password policies.</td>
<td>I could fall victim to password attacks if I fail to comply with my organizational password policies.</td>
<td>I believe that trying to protect my organizational password will reduce illegal access to it.</td>
<td>My organizational password may be compromised if I don’t pay adequate attention to policies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perceived Severity Threat</th>
<th>PS1</th>
<th>PS2</th>
<th>PS3</th>
<th>PS4</th>
<th>PS5</th>
<th>PS6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A security breach on my account would be a serious problem for me.</td>
<td>Loss of information resulting from compromising password would be a serious problem for me.</td>
<td>Having my account accessed by someone without my consent or knowledge would be a serious problem for me.</td>
<td>Having someone successfully attack my account would be very problematic for me.</td>
<td>I view password security attacks as harmful.</td>
<td>I believe that protecting my organizational password is important.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Self-Efficacy</th>
<th>SE1</th>
<th>SE2</th>
<th>SE3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I have the necessary skills to fulfill the requirements of password policies.</td>
<td>I have the necessary knowledge to fulfill the requirements of password policies.</td>
<td>I have the necessary competencies to fulfill the requirements of password policies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Efficacy</th>
<th>RE1</th>
<th>RE2</th>
<th>RE3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>My efforts to keep my organizational password safe from information security threats are effective.</td>
<td>Password policies that can be taken by employees to protect their organizational passwords are effective.</td>
<td>The preventive measures available to me are adequate to prevent others from accessing my organizational password.</td>
</tr>
</tbody>
</table>

Response Cost
| RC1 | Complying with the requirements of password policies is time consuming for me. | Bulgurcu et al. (2010) |
| RC2 | Complying with the requirements of password policies is burdensome for me. | |
| RC3 | Complying with the requirements of password policies is costly for me. | |

**Perceived Severity Sanction**

| PSS1 | The organization disciplines employees who break password policies. | Herath and Rao (2009) |
| PSS2 | My organization terminates employees who repeatedly break password policies. | |
| PSS3 | If I were caught violating my organization password policies, I would be severely punished. | |

**Perceived Certainty Sanction**

| PCS1 | If I don’t follow password policies, I will be punished. | Siponen et al. (2010). |
| PCS2 | If I violate password policies, the probability that I would be caught is: | Peace et al. (2003) |
| PCS3 | If I violate password policies, I would be probably caught. | |

**Perceived Psychological Ownership**

| PPO1 | This is my organizational account. | Yoo et al. (2018). |
| PPO2 | I feel a high degree of personal ownership of my organizational account. | |
| PPO3 | I sense that my organizational account is mine. | |

**Intention to Comply with Password Policies (Protection Motivation)**

| IC1 | I intend to comply with the requirements of my organization’s password policies. | Ajzen (1991) cited in Bulgurcu et al. (2010) |
| IC2 | I intend to protect my organizational password according to the requirements of my organization’s password policies. | |
| IC3 | I intend to carry out my responsibility prescribed in my organization’s password policies to protect my organizational password. | |

**Actual Compliance with Password Policies**

| AC1 | I adhere to the password policies that exist at my organization. | Sommestad et al. (2015) |
| AC2 | To the best of my knowledge, I do not violate password policies that exist at my organization. | |
| AC3 | I believe that I currently work entirely in accordance with the password policies that exist at my organization. | |
Instrument Reliability

The reliability of an instrument is defined as “an indication of the stability and consistency with which the instrument measures the concept and helps to assess the “goodness” of a measure” (Sekaran & Bougie, 2012, p. 223). The stability of measures refers to “the ability of a measure to remain the same over time”. In addition, consistency of measures refers to “the homogeneity of the items” (Sekaran & Bougie, 2012, p. 224). To increase the reliability of the instrument, the items for this study were adapted from previous studies that tested the reliability of the items, which should be above 0.07. According to McNeish (2017), the values of composite reliability and Cronbach’s alpha that are above 0.7 are considered acceptable. This study confirmed each reliability score is not less than 0.7.

This survey includes the following 10 major items: (a) perceived vulnerability threat, (b) perceived severity threat, (c) perceived response efficacy, (d) self-efficacy, (e) perceived response cost, (f) perceived severity sanction of noncompliance, (g) perceived certainty sanction of noncompliance, (h) perceived psychological ownership to the organizational account, (i) intention to comply with password policies, and (j) actual compliance with password policies.

As seen in Table 1 above and Table 2 below, to measure perceived psychological ownership, items were adapted from Yoo et al. (2018). These items were measured on a 5-point Likert scale. The reliability test of the perceived psychological ownership items was 0.93. Furthermore, items for actual compliance with password policies were measured using 7-point Likert scale ranging from 1 = Improbability to 7 = Probability,
and from 1 = \textit{False} to 7 = \textit{True}. The reliability measure of actual compliance items was a Cronbach’s alpha of 0.82 (Sommestad et al., 2015).

According to Ifinedo (2012), the composite reliability of perceived threat vulnerability items was 0.93. These items were measured on a 7-point Likert scale ranging from 1 = \textit{Strongly Disagree} to 7 = \textit{Strongly Agree}. Additionally, based on McGill and Thompson (2018), the Cronbach alpha value of perceived threat severity items was above 0.90. Perceived threat severity’s items were measured on a 7-point Likert scale from 1 = \textit{Strongly Disagree} to 7 = \textit{Strongly Agree}.

The items for intention to comply with password policies were measured on a 7-point Likert scale from 1 = \textit{Strongly Disagree} to 7 = \textit{Strongly Agree}. The items for response cost were measured on a 7-point Likert scale from 1 = \textit{Not at All} to 7 = \textit{Very Much}. In addition, the items for self-efficacy were measured on a 7-point Likert scale as 1 = \textit{Almost Never}; 2=\textit{Very Rarely}; 3=\textit{Rarely}; 4=\textit{Occasionally}; 5=\textit{Frequently}; 6=\textit{Very Frequently}; 7=\textit{Almost Always}. The reliability test for these items had a composite reliability of 0.982 for self-efficacy, 0.948 for response cost, and 0.984 for intention to comply with password policies (Bulgurcu et al., 2010). Moreover, the items for response efficacy were measured on a 7-point Likert scale from 1 = \textit{Strongly Disagree} to 7 = \textit{Strongly Agree}. The reliability of the response efficacy items was a Cronbach’s alpha of 0.85 (Posey et al., 2015).

The items for perceived severity sanction were measured using a 7-point Likert scale from 1 = \textit{Strongly Disagree} to 7 = \textit{Strongly Agree}. The reliability measure of perceived severity sanction items was a composite reliability of 0.88 (Herath & Rao, 2009). In addition, the items for perceived certainty sanction were measured using a 5-
point Likert scale from $1 = \text{Very Low}$ to $5 = \text{Very High}$, and from $1 = \text{Strongly Agree}$ to $5 = \text{Strongly Disagree}$. The reliability measure of perceived certainty sanction items was a composite reliability of 0.92 (Peace et al., 2003), and Cronbach’s alpha $> 0.6$ (Siponen et al., 2010).

Table 2

*Reliability of the Original Items*

<table>
<thead>
<tr>
<th>Constructs</th>
<th>Number of Items</th>
<th>Original reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived vulnerability threat</td>
<td>4</td>
<td>Composite reliability $= 0.93$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Ifinedo, 2012).</td>
</tr>
<tr>
<td>Perceived severity threat</td>
<td>6</td>
<td>Cronbach’s alpha was above $0.90$.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(McGrill &amp; Thompson, 2018).</td>
</tr>
<tr>
<td>Self- efficacy</td>
<td>3</td>
<td>Composite reliability $= 0.982$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Bulgurcu et al., 2010).</td>
</tr>
<tr>
<td>Response efficacy</td>
<td>3</td>
<td>Cronbach’s alpha $= 0.85$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Posey et al., 2015).</td>
</tr>
<tr>
<td>Response cost</td>
<td>3</td>
<td>Composite reliability $= 0.948$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Bulgurcu et al., 2010).</td>
</tr>
<tr>
<td>Perceived severity sanction</td>
<td>3</td>
<td>Composite reliability $= 0.88$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Herath &amp; Rao, 2009).</td>
</tr>
<tr>
<td>Perceived certainty sanction</td>
<td>3</td>
<td>Cronbach’s alpha $&gt; 0.6$ (Siponen et al., 2010).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Composite reliability $= 0.92$ (Peace et al., 2003).</td>
</tr>
<tr>
<td>Perceived psychological ownership</td>
<td>3</td>
<td>Composite reliability $= 0.93$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Yoo et al., 2018).</td>
</tr>
<tr>
<td>Intention to comply</td>
<td>3</td>
<td>Composite reliability $= 0.984$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Bulgurcu et al., 2010).</td>
</tr>
<tr>
<td>Actual compliance</td>
<td>3</td>
<td>Cronbach’s alpha $= 0.82$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Sommestad et al., 2015).</td>
</tr>
</tbody>
</table>
Instrument Validity

To ensure valid results, not only reliability but also the validity of the instrument was assessed. Sekaran and Bougie (2012) asserted that to ensure scientific research, a valid and reliable instrument is needed. Validity refers to “a test of how well an instrument that is developed measures the particular concept it is intended to measure” (Sekaran & Bougie, 2012, p. 220). There are different types of validity, such as content validity and construct validity. Content validity assesses whether the contents of the questionnaire reflect the content domain being measured. Construct validity, assessing through discriminant and convergent validity, refers to the degree to which a theoretical construct is measured by the instrument (Sekaran & Bougie, 2012). Hair, Hult, et al. (2014) defined convergent validity as “the extent to which a measure correlates positively with alternative measures of the same construct” (p. 102). According to Hair, Sarstedt, et al. (2014), convergent validity is supported when the outer loadings of each item is above 0.70, and the average variance extracted (AVE) value of each construct is 0.50 or higher. The AVE value of 0.50 means that the construct explains at least half of its indicators’ variance.

Additionally, Hair, Sarstedt, et al. (2014) defined discriminant validity as “the extent to which the construct is empirically distinct from other constructs” (p. 112). To measure the discriminant validity of the indicators, cross loadings method is used, which requires that the loadings of each construct’s indicator should be higher than all other constructs’ cross loadings (Henseler et al., 2009). Another method is Fornell- Larcker criterion, which notes that the construct shares with its indicators more variance than any other construct. To meet this criterion, every construct’s AVE should be higher than any
other construct’s highest squared correlation (Fornell & Larcker, 1981). In this study, Fornell- Larcker criterion was used to examine the discriminant validity.

To increase content validity, the questionnaire for the aforementioned dimensions (perceived vulnerability threat, perceived severity threat, perceived response efficacy, self-efficacy, perceived response cost, perceived severity sanction, perceived certainty sanction, perceived psychological ownership, intention to comply with password policies, & the actual compliance with password policies) was adapted and adopted. According to Straub et al. (2004), adopting questions from previous studies increases content validity. Moreover, to confirm the reliability and validity of the adapted instrument, a pilot and Delphi studies were conducted.

Threats to validity can be internal or external. Many factors affect the validity of studies, such as history, maturation, selection, morality, regression, instrumentation, and testing (Sekaran & Bougie, 2012). To address the history, morality, and maturation threats, the data was collected at one point in time to avoid changing over time. In addition, instrumentation threat was not an issue since the same instrument was used to collect data from all participants. According to Torre and Picho (2016), internal validity applies to experimental studies where the dependent variable is affected by the manipulated independent variables. In addition, Sekaran and Bougie (2012) stated that internal validity determines if there are other extraneous factors that cause the effects. This study is not experimental; therefore, there is no issue with internal validity threats, such as testing effect. Moreover, to mitigate the external validity threat, this study ensured a sufficient sample size using G* power analysis. Torre and Picho (2016) implied
that external validity affects the generalizability’s degree of results. However, the sample of this study is a convenience sample, which is not generalizable.

**Population and Sample**

Based on the objective of the study and the characteristics of the population, the sample is identified (Terrell, 2015). The target population is all employees who use a password to log in to the organizational accounts and have password policies to comply with. The sample, which is a subset of the population, was all participants who were willing to participate in this study by completing the survey.

There are two different types of sampling: probability and non-probability samplings. In probability sampling, each element has an equal probability to be selected as a subject in the study, which is expensive, generalizable, and less bias. For example, sample random sampling, cluster sampling, systematic sampling, area sampling, stratified sampling, and double sampling. On the other hand, in non-probability sampling, the element has an unequal probability to be selected, which means the findings cannot be generalized to the population. For example, purposive and convenience sampling (Sekaran & Bougie, 2012).

For this study, a non-probability convenience sample was used to gather data from employees who are conveniently accessible. The researcher utilized a market research company (MTurk) to recruit participants, send surveys, and gain access to the sample. According to Sekaran and Bougie (2012), convenience sample is a good choice to obtain information conveniently, quickly, efficiently, and inexpensively. Hence, a convenient choice of sampling was an instrumental choice in examining what factors influence employees’ compliance with password policies.
For this study, G*Power 3.1 analysis was used to obtain an adequate sample size. G*Power 3.1 is a software that can estimate the sample size based on alpha level (\(\alpha\)), power level (1-\(\beta\)), and effect size (Faul et al., 2007). For multiple regression analysis, an estimated sample size of 100 participants was determined using a significance level (\(\alpha = 0.05\)), power (1-\(\beta\)) of 0.80, a medium effect size (\(f^2\)) of 0.15, and eight predictor variables.

**Pre-Analysis Data Screening**

Before analyzing data, raw data were coded and edited. The outliers and inconsistent responses were reviewed and addressed to prepare for data analysis. Pre-analysis data screening is essential to confirm data accuracy and consequently to increase results validity (Sekaran & Bougie, 2012). In this study, to ensure coding accuracy, electronic survey was used, which directly enters the key of responses into the computer. In addition, before the analysis of data, all fundamental data were examined for normal distribution and homogeneity of variance to ensure the absence of any outliers. Outlier responses were investigated by the scatterplot method using the Statistical Package for the Social Science (SPSS) software. Based on Sekaran and Bougie (2012), the researcher can edit or omit the outlier and inconsistent responses, ignore the blank responses, and not include the questionnaire in data analysis if approximately 25% of the items are not answered.

**Data Analysis**

Data were analyzed using both descriptive and inferential statistics. Descriptive statistics involve central tendency and dispersion of demographics questionnaire. Central tendency is the mode, median, and mean, while dispersion is the range, variance, standard deviation, and interquartile range (Sekaran & Bougie, 2012). SPSS software was used for
data screening and descriptive analysis. In addition, the multiple regression method was used to infer the outcomes, test the hypotheses, and describe the relationship between the independent variables and the dependent variable. Constantin (2017) asserted that when the model involves more than two independent variables that predict one dependent variable, the multiple regression method is used. For conducting multiple regression analysis, SmartPLS 3.0 software was used.

To test the hypotheses of this study and to run a regression analysis, a partial least square structural equation modeling (PLS-SEM) approach was used. PLS-SEM can be used as a regression tool to examine the relationships between latent variables in the structural model as well as the relationship between the latent variable and its indicators in the measurement model (Chin et al., 2003).

There are two different approaches to structural equation modeling (SEM). One approach is covariance-based (CB-SEM) and another one is PLS-SEM. According to Hair et al. (2011) and Henseler et al. (2009), PLS is a regression-based approach that works with small samples, handles both reflective and formative measures, can measure non-normal data, and is less restrictive regarding data distribution. On the other hand, CB-SEM requires a large sample, can only measure the reflective measures, and requires fulfilling data normality (Hair et al., 2011).

PLS supports the prediction of structural models’ constructs. PLS-SEM is a good approach to use when the object of the research is theory development and prediction since PLS has a higher level of statistical power than CB-SEM. However, the CB-SEM approach disregards the prediction objective. CB-SEM is a suitable approach when the object of the research is confirmation and theory testing (Hair et al., 2011).
Ethical Consideration

The review and approval of this study were received from the IRB of NSU (see Appendix B). Thereafter, the participation letter, demographics questionnaire, and the adapted instrument questionnaire were sent to the participants in the survey. Participation letter was used to inform potential study participants about the purpose of this study, their rights to privacy, and contact information.

Format for Presenting Results

In this chapter, validity and reliability of the adapted items were presented in tables. According to the guidelines of NSU dissertation guide, IRB approval letters, participation letter, and the survey instrument are presented in the appendices. In addition, the findings of this study will be discussed in Chapter 4 along with screenshots of data analysis processes and results.

Resource Requirements

Few required resources were needed to conduct this research, such as: (1) devices with Internet access for the participants to participate, (2) a market research company to recruit the participants, (3) an adapted questionnaire as an instrument to collect data, (4) access to an expert panel to evaluate the survey instrument, (5) a pilot study to be conducted with a pilot sample group by the researcher, and data were analyzed before going on with the full study, (6) a secure laptop with sufficient computing resources to handle the collected data, (7) access to an expert in statistical analysis, and (8) SmartPLS and SPSS to analyze quantitative data.
Summary

In this chapter, the research design, instrument development and validation, sampling method, data analysis, presenting results formats, and resource requirements were discussed. This study used a quantitative cross-sectional design to examine the relationship between the independent variables and the dependent variable. A proposed sample was a convenience sample since it is conveniently accessible, inexpensive, and quick (Sekaran & Bougie, 2012). A survey questionnaire was developed by adapting items from valid previous studies. Descriptive and inferential statistics were determined to be used for data analysis. The results format of this study will be presented according to the requirements of the NSU dissertation guide. In addition, all required resources to conduct this study were determined and discussed.
Chapter 4

Results

Overview

A quantitative cross-sectional study was conducted using a survey strategy to examine factors that influence employees’ compliance with password policies. Furthermore, this method was used to collect and analyze the numerical data. This study involved the use of MTurk research company. MTurk was utilized to reach the participants anonymously, and the survey was hosted by google forms. MTurk was utilized to recruit participants because organizations are often unwilling to provide access to their employees. Based on Kotulic and Clark (2004), organizations are unwilling to allow outside researchers to access their employees, especially when the data is about organizational information security. In this chapter, the Delphi study, custom qualification technique, pilot study, and actual study were discussed along with their results.

Phase One - Delphi Study

A Delphi study was conducted to ensure the content validity of the adapted instrument. An expert panel consisting of those who are knowledgeable in the IS field was invited by the researcher to conduct the Delphi study, and the instrument was revised based on expert panel feedback. The expert panel was asked to evaluate the cognition,
content, usability, and clarity of the instrument. Groves et al. (2011) stated that expert panel’s reviews are based on content, usability, and cognition of the questionnaire. To conduct a Delphi study, direct invitations were sent to 11 experts by emails. Of the 11 invited experts, only four experts accepted the invitation. According to Skulmoski et al. (2007), the sample size for conducting a Delphi study varies from 4 to 171 experts. The adapted survey instrument was sent to the expert panel for feedback. The recommendations include minor changes for a few items to improve clarity, remove items that are not related to the constructs, add more items for specific constructs, and changing all self-efficacy items since some experts commented that the items are not related to the self-efficacy construct. Therefore, based on the experts’ feedback, the instrument was revised, and a consensus was reached among experts in the second round (see Table 3). Based on Delbecq et al. (1975), mostly two to three Delphi rounds are sufficient to reach consensus. After that, the researcher submitted an amendment to the IRB and got approval for using the modified instrument (see Appendix C).

Table 3

Revised Adapted Survey Instrument

<table>
<thead>
<tr>
<th>Perceived Vulnerability Threat</th>
<th>Ifinedo (2012)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV1 I know that my organizational password could be vulnerable to security breaches if I don’t follow my organization’s password policies.</td>
<td></td>
</tr>
<tr>
<td>PV2 I could fall victim to password attacks if I fail to comply with my organizational password policies.</td>
<td></td>
</tr>
<tr>
<td>PV3 I believe that trying to protect my organizational password will reduce illegal access to it.</td>
<td></td>
</tr>
<tr>
<td>PV4 My organizational password may be compromised if I don’t pay adequate attention to password policies.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3 (continued)

**Revised Adapted Survey Instrument**

<table>
<thead>
<tr>
<th><strong>Perceived Severity Threat</strong></th>
<th><strong>Self-Efficacy</strong></th>
<th><strong>Response Efficacy</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>PS1 Threats on my organizational account would be a serious problem.</td>
<td>SE1 I feel comfortable following password policies to protect my organizational password.</td>
<td>RE1 If I were to engage in efforts to protect my organizational password, those efforts would be effective.</td>
</tr>
<tr>
<td>PS2 Loss of data resulting from compromising my organizational password would be a serious problem.</td>
<td>SE2 Following password policies is entirely under my control.</td>
<td>RE2 Password policies that protect organizational passwords are effective.</td>
</tr>
<tr>
<td>PS3 Having my organizational account accessed by someone else without my permission or knowledge would be a serious problem.</td>
<td>SE3 I have the necessary skills to implement the requirements of password policies in order to protect my organizational password.</td>
<td>RE3 Preventive password policies available to me are adequate to prevent unauthorized persons from accessing my organizational password.</td>
</tr>
<tr>
<td>PS4 Having security breaches successfully attack my organizational account would be very problematic.</td>
<td>SE4 I have the knowledge and resources to fulfill the requirements of password policies.</td>
<td>RE4 Preventive password policies available to me are adequate to prevent password security attacks from guessing my organizational password.</td>
</tr>
<tr>
<td>PS5 I view password security attacks on my organizational password as harmful.</td>
<td>SE5 Following password policies is easy.</td>
<td></td>
</tr>
<tr>
<td>PS6 I believe that threat to my organizational password is severe.</td>
<td>SE6 I’m able to follow password policies by myself.</td>
<td></td>
</tr>
<tr>
<td>PS7 I believe that threat to my organizational password is significant.</td>
<td>SE7 I can enable password policies on my organizational password.</td>
<td></td>
</tr>
</tbody>
</table>


Witte (1996)

Workman et al. (2008)
Table 3 (continued)

Revised Adapted Survey Instrument

<table>
<thead>
<tr>
<th><strong>Response Cost</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RC1</td>
<td>Complying with password policies’ requirements is time consuming for me.</td>
</tr>
<tr>
<td>RC2</td>
<td>Complying with password policies’ requirements is burdensome for me.</td>
</tr>
<tr>
<td>RC3</td>
<td>Complying with password policies’ requirements is costly for me.</td>
</tr>
<tr>
<td>RC4</td>
<td>Complying with the requirements of password policies is inconvenience for me.</td>
</tr>
<tr>
<td>RC5</td>
<td>The cost of comply with the requirements of password policies exceeds the benefits.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Perceived Severity Sanction</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PSS1</td>
<td>My organization punishes employees who break password policies.</td>
</tr>
<tr>
<td>PSS2</td>
<td>My organization terminates employees who violate password policies repeatedly.</td>
</tr>
<tr>
<td>PSS3</td>
<td>If I were caught violating my organization’s password policies, I would be punished severely.</td>
</tr>
<tr>
<td>PSS4</td>
<td>I would receive reprimand in oral if I were caught violating my organization’s password policies.</td>
</tr>
<tr>
<td>PSS5</td>
<td>I would receive reprimand in written report if I were caught violating my organization’s password policies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Perceived Certainty Sanction</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PCS1</td>
<td>If I don’t follow password policies, I will be punished.</td>
</tr>
<tr>
<td>PCS2</td>
<td>If I violate password policies, I would probably get caught.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Perceived Psychological Ownership</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PPO1</td>
<td>I feel like my work account is mine.</td>
</tr>
<tr>
<td>PPO2</td>
<td>I feel a high degree of personal ownership of my organizational account.</td>
</tr>
<tr>
<td>PPO3</td>
<td>I sense that I own my work account.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Intention to Comply with Password Policies (Protection Motivation)</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IC1</td>
<td>I intend to comply with the requirements of my organization’s password policies.</td>
</tr>
<tr>
<td>IC2</td>
<td>I intend to protect my work account according to the requirements of my organization’s password policies.</td>
</tr>
<tr>
<td>IC3</td>
<td>I intend to carry out my responsibility prescribed in my organization’s password policies whenever possible.</td>
</tr>
</tbody>
</table>
Table 3 (continued)

Revised Adapted Survey Instrument

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IC4</td>
<td>My intention is to continue complying with my organization’s password policies.</td>
</tr>
<tr>
<td>AC1</td>
<td>I adhere to the password policies that exist at my organization.</td>
</tr>
<tr>
<td>AC2</td>
<td>To the best of my knowledge, I do not violate password policies that exist at my organization.</td>
</tr>
<tr>
<td>AC3</td>
<td>I currently work entirely in accordance with the password policies that exist at my organization.</td>
</tr>
</tbody>
</table>

**Actual Compliance with Password Policies**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IC4</td>
<td><em>Ifinedo (2012)</em></td>
</tr>
<tr>
<td>AC1</td>
<td><em>Sommestad et al. (2015)</em></td>
</tr>
</tbody>
</table>

Phase Two - Custom Qualification Technique

To identify qualified participants for this study, it was important to prepare targeted participants with specific criteria. Therefore, a few questions were published via a human intelligence task (HIT) to assign the custom qualification (see Appendix D). Each response included the worker ID of the participant, which was used to assign the worker who meets the criteria to custom qualification. Only qualified participants were invited later for the pilot study as well as the actual study. The qualified participant should be an adult employee who works at an organization with password policies and use a password to log in to his or her work account. Via HIT, the researcher requested 500 responses from employees at organizations in the United States to screen for qualified participants. Among the 500 employees surveyed, 425 met the criteria, which is almost 85% of the employees surveyed. Workers’ ID was very important, so the researcher could identify (a) who was qualified to participate and (b) who participated in the pilot study so they would not be invited to participate in the actual study.
**Phase Three - Pilot Study**

After evaluating the instrument content and before conducting the actual study, a pilot study was done for instrument reliability using a small group from the actual sample. The survey was piloted with 39 employees from the qualified participants. The participants were asked to complete the survey and offer suggestions to improve the clarity of the instrument. Most of the participants had no comments regarding improving the instruments, but two participants mentioned that password policies are enforced by the system. In addition, 65% of the participants responded with “Strongly Agree” for the actual compliance construct. Therefore, the researcher added a section about what is considered a violation of password policies that cannot be enforced by the system, which would affect their answers in the actual study. In addition, the researcher changed the instrument scale from a 5-point scale to a 7-point scale to provide the participants with more options to choose from.

**Instrument Reliability**

All the subscales were found reliable because Cronbach’s alpha values were above 0.7. According to Fornell and Larcker (1981), Cronbach’s alpha should be at least 0.7 to ensure reliability. However, there may be redundancy in the items of the Intention to Comply construct. Furthermore, for Threat Severity and Actual Compliance, the vast majority of the responses were either “Strongly Agree” or “Agree” (See Table 4).

Notice that the Table 5 below shows what Cronbach’s alpha would be if a question were deleted. Cronbach’s alpha remains at 0.98 regardless of which question is deleted. Consequently, a slight change in wording is a better strategy for reducing redundancy. Therefore, IC4 was reworded to avoid redundancy.
### Table 4

**Reliability of Scale Based on a Pilot Study**

<table>
<thead>
<tr>
<th>Scale</th>
<th>Cronbach’s alpha</th>
<th>Mean</th>
<th>Variance</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intention to Comply</td>
<td>.990</td>
<td>4.494</td>
<td>.703</td>
<td>likely redundancy IC2</td>
</tr>
<tr>
<td>Threat Severity</td>
<td>.952</td>
<td>4.403</td>
<td>.531</td>
<td>68% Strongly Agree</td>
</tr>
<tr>
<td>Psychological Ownership</td>
<td>.946</td>
<td>3.880</td>
<td>1.150</td>
<td></td>
</tr>
<tr>
<td>Severity of Sanction</td>
<td>.940</td>
<td>3.082</td>
<td>1.392</td>
<td></td>
</tr>
<tr>
<td>Actual Compliance</td>
<td>.940</td>
<td>4.564</td>
<td>.531</td>
<td>63% Strongly Agree</td>
</tr>
<tr>
<td>Response Efficacy</td>
<td>.932</td>
<td>4.000</td>
<td>1.013</td>
<td></td>
</tr>
<tr>
<td>Certainty of Sanction</td>
<td>.918</td>
<td>3.397</td>
<td>1.469</td>
<td></td>
</tr>
<tr>
<td>Threat Vulnerability</td>
<td>.912</td>
<td>4.436</td>
<td>.692</td>
<td></td>
</tr>
<tr>
<td>Response Cost</td>
<td>.910</td>
<td>2.144</td>
<td>1.591</td>
<td></td>
</tr>
<tr>
<td>Self-Efficacy</td>
<td>.895</td>
<td>4.289</td>
<td>.761</td>
<td></td>
</tr>
</tbody>
</table>

### Table 5

**Cronbach’s Alpha if an Item is Deleted**

<table>
<thead>
<tr>
<th>Intention to Comply with Password Policies (Protection Motivation)</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>[IC1: I intend to comply with the requirements of my organization’s password policies.]</td>
<td>13.49</td>
<td>6.414</td>
<td>.969</td>
<td>.988</td>
</tr>
<tr>
<td>[IC2: I intend to protect my work account according to the requirements of my organization’s password policies.]</td>
<td>13.51</td>
<td>6.046</td>
<td>.988</td>
<td>.983</td>
</tr>
</tbody>
</table>
Table 5 (continued)

Cronbach’s Alpha if an Item is Deleted

<table>
<thead>
<tr>
<th>Intention to Comply with Password Policies (Protection Motivation)</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>[IC3: I intend to carry out my responsibility prescribed in my organization’s password policies whenever possible.]</td>
<td>13.46</td>
<td>6.097</td>
<td>.970</td>
<td>.987</td>
</tr>
<tr>
<td>[IC4: My intention is to continue complying with my organization’s password policies.]</td>
<td>13.46</td>
<td>6.097</td>
<td>.970</td>
<td>.987</td>
</tr>
</tbody>
</table>

Factor Analysis

Factor analysis groups together items that “vary together” by explaining the variance in responses among participants in the sample. Changes were done and reflected on the instrument based on the factor analysis results (see Appendix E). First, two items were not grouped with any factor, indicating that these questions did not work and needed to be removed: (a) Self-Efficacy [SE2: Following password policies is entirely under my control.] and (b) Perceived Severity Threat [PS7: I believe that threat to my organizational password is significant.]. Second, PSS1 item was removed from perceived severity sanction construct since it is not related to the construct. For the last version of the revised instrument (see Table 6 below).
### Table 6

*Last Version of the Revised Instrument*

<table>
<thead>
<tr>
<th>Perceived Vulnerability Threat</th>
<th>PV1</th>
<th>PV2</th>
<th>PV3</th>
<th>PV4</th>
</tr>
</thead>
<tbody>
<tr>
<td>I know that my organizational password could be vulnerable to security breaches if I don’t follow my organization’s password policies.</td>
<td>Ifinedo (2012).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I could fall victim to password attacks if I fail to comply with my organizational password policies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I believe that trying to protect my organizational password will reduce illegal access to it.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>My organizational password may be compromised if I don’t pay adequate attention to password policies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perceived Severity Threat</th>
<th>PS1</th>
<th>PS2</th>
<th>PS3</th>
<th>PS4</th>
<th>PS5</th>
<th>PS6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of data resulting from compromising my organizational password would be a serious problem.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Having my organizational account accessed by someone else without my permission or knowledge would be a serious problem.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Having security breaches successfully attack my organizational account would be very problematic.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I believe that threat to my organizational password is severe.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Self-Efficacy**

<table>
<thead>
<tr>
<th>SE1</th>
<th>SE2</th>
<th>SE3</th>
<th>SE4</th>
<th>SE5</th>
<th>SE6</th>
</tr>
</thead>
<tbody>
<tr>
<td>I feel comfortable following password policies to protect my organizational password.</td>
<td>McGill and Thompson (2018).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I have the necessary skills to implement the requirements of password policies in order to protect my organizational password.</td>
<td>Workman et al. (2008).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I have the knowledge and resources to fulfill the requirements of password policies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Following password policies is easy.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I’m able to follow password policies by myself.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I can enable password policies on my organizational password.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Response Efficacy**

<table>
<thead>
<tr>
<th>RE1</th>
</tr>
</thead>
<tbody>
<tr>
<td>If I were to engage in efforts to protect my organizational password, those efforts would be effective.</td>
</tr>
</tbody>
</table>
### Last Version of the Revised Instrument

| RE2 | Password policies that protect organizational passwords are effective. |
| RE3 | Preventive password policies available to me are adequate to prevent unauthorized persons from accessing my organizational password. |
| RE4 | Preventive password policies available to me are adequate to prevent password security attacks from guessing my organizational password. |

**Response Cost**

| RC1 | Complying with password policies’ requirements is time consuming for me. |
| RC2 | Complying with password policies’ requirements is burdensome for me. |
| RC3 | Complying with password policies’ requirements is costly for me. |
| RC4 | Complying with the requirements of password policies is inconvenience for me. |
| RC5 | The cost of complying with the requirements of password policies exceeds the benefits. |

**Perceived Severity Sanction**

| PSS1 | My organization terminates employees who violate password policies repeatedly. |
| PSS2 | If I were caught violating my organization’s password policies, I would be punished severely. |
| PSS3 | I would receive reprimand in oral if I were caught violating my organization’s password policies. |
| PSS4 | I would receive reprimand in written report if I were caught violating my organization’s password policies. |

**Perceived Certainty Sanction**

| PCS1 | If I don’t follow password policies, I will be punished. |
| PCS2 | If I violate password policies, I would probably get caught. |

**Perceived Psychological Ownership**

| PPO1 | I feel like my work account is mine. |
| PPO2 | I feel a high degree of personal ownership of my organizational account. |
| PPO3 | I sense that I own my work account. |

**Intention to Comply with Password Policies (Protection Motivation)**
Table 6 (continued)

Last Version of the Revised Instrument

| IC1 | I intend to comply with the requirements of my organization’s password policies. |
| IC2 | I intend to protect my work account according to the requirements of my organization’s password policies. |
| IC3 | I intend to carry out my responsibility prescribed in my organization’s password policies whenever possible. |
| IC4 | My intention is to continue complying with my organization’s password policies in the future. |

Bulgurcu et al. (2010).

Actual Compliance with Password Policies

| AC1 | I adhere to the password policies that exist at my organization. |
| AC2 | To the best of my knowledge, I do not violate password policies that exist at my organization. |
| AC3 | I currently work entirely in accordance with the password policies that exist at my organization. |

Sommestad et al. (2015).

Phase Four - Actual Data Collection Technique

Data were collected by sending an anonymous survey. Based on the G* power, 100 participants are needed; therefore, the researcher collected 151 responses considering the data cleaning. Fortunately, there were no missing data since each question was marked as required.

Pre-Analysis Data Screening

Data screening involves examining the research data for missing data, outliers, and normality assumption responses to determine the readiness of the data for further statistical analysis (Sekaran & Bougie, 2012). To ensure that the data used was accurate before the actual data analysis, a pre-data analysis screening was done. Responses collected from the online survey were downloaded from google forms into Microsoft Excel for the pre-data analysis screening. At the initial stage, the data were subjected to visual inspection by the researcher to identify response-set biases. However, no
substantial response-set biases were found. Subsequently, missing values were examined using descriptive statistics, such as means, standard deviations, minimum as well as maximum values. Missing data refers to an unanswered item on a survey instrument by a respondent either intentionally or unintentionally (Hair, Hult, et al., 2014). Missing values were not present as all the questions listed on the google forms were indicated as required for respondents to select from a proposed option before they can move to the next stage of the questionnaire. Frequencies of the descriptive statistics were valid for all the responses. Also, there were no missing values as indicated by the descriptive statistics. Therefore, prior to the analysis, the answers or responses gathered were examined using SPSS for missing values, accuracy of data entry, and outliers. Mahalanobis distance statistic was used to test the multivariate outliers in this study. To sum up, there were no eliminated values, leaving 151 responses for data analysis.

Test of Assumptions

Various assumptions were tested to perform regression analyses. Assumptions were examined with regards to linearity, independence of variables, multicollinearity, homoscedasticity, outliers as well as normality distribution. The results are presented as follows:

1. According to Tabachnick and Fidell (2019), a histogram made up of regression standardized residuals along with the normal probability plot that plots the observations against the predicted cumulative probability values were used to determine the normality of distribution. The results revealed that the data spread out normally in a bell-shaped curve (Appendix F, Figure 5), while normal P-P plot residuals resemble a straight line (Appendix F, Figure 6). Based on Mertler and Vanatta (2017), the assumption was met.
2. Multicollinearity occurs when at least two independent variables are strongly related in the regression model (Mertler & Vanatta, 2017). To assess the existence or absence of multicollinearity, the variance inflation factor (VIF) values were examined. According to Hair et al. (2011), VIF values should be less than 5 and tolerance values should be more than 0.20. Otherwise, a collinearity problem can occur. The results indicate no collinearity problem (Appendix F, Figure 7).

3. To determine linearity, a scatterplot of the standardized residuals against the expected values is used (Tabachnick & Fidell, 2019). The residuals were distributed predictably and related linearly along the regression line, satisfying the linearity combinations of variables, according to the scatterplot (Appendix F, Figure 8).

4. Homoscedasticity is “the assumption that the variability in scores for one continuous variable is roughly the same at all values of another continuous variable” (Mertler & Vanatta, 2017, p. 35). Scatterplot was examined to also assess homoscedasticity (Appendix F, Figure 8). According to Tabachnick and Fidell (2007), the homoscedasticity assumption is related to the normality assumption. If the multivariate normality assumption is met, then the two variables must have a homoscedastic relationship.

5. The Durbin-Watson (DW) statistics test was used to determine the case/error independence. A Durbin-Watson value of 2 or closer to 2 means that the residuals or errors are independent (Mertler & Vanatta, 2017). The D-W number was 1.956, revealing that the assumption was met (Appendix F, Figure 9).

6. Cook’s distance statistics describes the findings that adversely affect the overall regression model and revealed no major outliers or influential points (Tabachnick &
Fidell, 2019). All Cook’s distance values were less than 0.358 (Appendix F, Figure 10). A meaning greater than 1.0 should be taken seriously (Cook, 1977). Based on the results of Mahalanobis distance outlier detection test, there was no need to delete any values. This assumption was met.

**Demographic Analysis**

Five demographic indicators were collected, which are age, gender, computer skill level, highest degree, and ethnicity. Among 151 participants, 78 (51.7%) were females and 73 (48.3%) were males. Moreover, 7 (4.6%) were between 18–25 age group, 38 (25.2%) were between 26–35 age group, 45 (29.8%) were between 36–45 age group, 37 (24.5%) were between 46–55 age group, and 24 (15.9%) were between 56–65 age group. A greater number of respondents fall between the 36–45 age groups. Also, more than half of the respondents had a high level of computer skills. Among the responses, 81 (53.6%) reported having high computer skills and 70 (46.4%) reported having medium computer skills. Furthermore, most of the participants (129, 85.4%) were white, while Hispanic were four. Furthermore, the majority have undergraduate or graduate degrees at 66 (43.7%) and 40 (26.5%), respectively (see Table 7).

**Table 7**

**Demographic Description**

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-25 years</td>
<td>7</td>
<td>4.6</td>
</tr>
<tr>
<td>26-35 years</td>
<td>38</td>
<td>25.2</td>
</tr>
<tr>
<td>36-45 years</td>
<td>45</td>
<td>29.8</td>
</tr>
<tr>
<td>46-55 years</td>
<td>37</td>
<td>24.5</td>
</tr>
<tr>
<td>56-65 years</td>
<td>24</td>
<td>15.9</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Women</td>
<td>78</td>
<td>51.7</td>
</tr>
</tbody>
</table>
Table 7 (continued)

Demographic Description

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Men</td>
<td>73</td>
<td>48.3</td>
</tr>
<tr>
<td>Computer Skill</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>81</td>
<td>53.6</td>
</tr>
<tr>
<td>Medium</td>
<td>70</td>
<td>46.4</td>
</tr>
<tr>
<td>Highest Degree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High school diploma</td>
<td>24</td>
<td>15.9</td>
</tr>
<tr>
<td>Associate degree</td>
<td>21</td>
<td>13.9</td>
</tr>
<tr>
<td>Undergraduate degree</td>
<td>66</td>
<td>43.7</td>
</tr>
<tr>
<td>Graduate degree</td>
<td>40</td>
<td>26.5</td>
</tr>
<tr>
<td>Ethnicity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>African-American</td>
<td>7</td>
<td>4.6</td>
</tr>
<tr>
<td>Asian</td>
<td>10</td>
<td>6.6</td>
</tr>
<tr>
<td>Hispanic</td>
<td>4</td>
<td>2.6</td>
</tr>
<tr>
<td>White</td>
<td>129</td>
<td>85.4</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td>0.7</td>
</tr>
</tbody>
</table>

Reliability and Validity

Testing the reliability and validity of the instrument is important to ensure the accuracy of the results. Straub (1989) defined reliability as “the stability of individual measures across replications from the same source of information” (p. 160). To ensure the reliability of the instrument, all items were adapted from previous reliable and valid studies. Internal consistency of the adapted instrument was measured using Cronbach’s alpha. Cronbach’s alpha measures how closely items are related in the same group (Hair, Hult, et al., 2014). The values of Cronbach’s alpha were measured twice after conducting both pilot study and actual study.

Construct validity is assessed through convergent and discriminant validity (Straub, 1989). Convergent validity is measured by the outer loadings technique or AVE value (Hair, Sarstedt, et al., 2014). In this study, convergent validity was measured using
AVE in SmartPLS 3.0. AVE examines how each construct explains its indicators’ variance (Hair, Hult, et al., 2014). Convergent validity is supported when the AVE value is 0.50 or higher (Hair, Sarstedt, et al., 2014). In addition, discriminant validity can be measured by cross loadings method (Henseler et al., 2009) as well as Fornell-Larcker criterion (Fornell & Larcker, 1981). This study used Fornell-Larcker criterion to examine discriminant validity. Discriminant validity is supported when the square root of every construct’s AVE is higher than any other construct’s highest correlation (Fornell & Larcker, 1981). Additionally, content validity was assessed by the expert panel review through a Delphi study.

Cronbach’s alpha values along with composite reliability values were used to examine the constructs’ reliability. The construct reliability was supposed to be determined by these two criteria. Internal reliability was suggested by Cronbach’s alphas and composite reliability values of 0.7 or greater. According to Fornell and Larcker (1981), Cronbach’s alpha values of 0.7 and above are accepted. Both Cronbach’s alpha and composite reliability values were above 0.7, as indicated in Table 8, which means that the adapted instrument is reliable. As a result, all the latent variables have high levels of internal consistency reliability. Moreover, AVE was used to investigate the construct's convergent validity, and it was found that AVE values for all the latent variables (AC, IC, PCS, PPO, PRC, PS, PSS, PV, PE, and SE) were equal or above the minimum accepted value of 0.5. In addition, according to Hair and Sarstedt, et al. (2014), AVE values of at least 0.5 represent acceptable validity.
### Table 8

**Construct Reliability and Convergent Validity**

<table>
<thead>
<tr>
<th>Constructs</th>
<th>Cronbach’s Alpha</th>
<th>Rho A</th>
<th>Composite Reliability</th>
<th>AVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived vulnerability threat (PV)</td>
<td>0.917</td>
<td>0.931</td>
<td>0.943</td>
<td>0.806</td>
</tr>
<tr>
<td>Perceived severity threat (PS)</td>
<td>0.923</td>
<td>0.931</td>
<td>0.940</td>
<td>0.724</td>
</tr>
<tr>
<td>Self-efficacy (SE)</td>
<td>0.850</td>
<td>0.906</td>
<td>0.888</td>
<td>0.615</td>
</tr>
<tr>
<td>Response efficacy (RE)</td>
<td>0.896</td>
<td>0.899</td>
<td>0.928</td>
<td>0.762</td>
</tr>
<tr>
<td>Response cost (RC)</td>
<td>0.941</td>
<td>0.951</td>
<td>0.962</td>
<td>0.894</td>
</tr>
<tr>
<td>Perceived severity sanction (PSS)</td>
<td>0.876</td>
<td>0.893</td>
<td>0.915</td>
<td>0.729</td>
</tr>
<tr>
<td>Perceived certainly sanction (PCS)</td>
<td>0.835</td>
<td>0.936</td>
<td>0.924</td>
<td>0.859</td>
</tr>
<tr>
<td>Perceived psychological ownership (PPO)</td>
<td>0.970</td>
<td>1.297</td>
<td>0.978</td>
<td>0.936</td>
</tr>
<tr>
<td>Intention to comply with password (protection motivation) (IC)</td>
<td>0.953</td>
<td>0.954</td>
<td>0.966</td>
<td>0.878</td>
</tr>
<tr>
<td>Actual compliance with password policies (AC)</td>
<td>0.950</td>
<td>0.953</td>
<td>0.968</td>
<td>0.909</td>
</tr>
</tbody>
</table>

In this study, the discriminant validity of the constructs was examined using the criterion proposed by Fornell and Larcker (1981). SmartPLS 3.0 was used to calculate the square root of the AVE values for all latent variables (see Table 9). According to Fornell and Larcker, to demonstrate discriminant validity, the square root of the AVE value for
each construct should be greater than any correlation values among all other latent variables.

**Table 9**

*Discriminant Validity*

*Square Root of AVE and the Correlation Values.*

<table>
<thead>
<tr>
<th></th>
<th>AC</th>
<th>IC</th>
<th>PCS</th>
<th>PPO</th>
<th>RC</th>
<th>PS</th>
<th>PSS</th>
<th>PV</th>
<th>RE</th>
<th>SE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>0.953</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IC</td>
<td>0.810</td>
<td>0.937</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCS</td>
<td>0.384</td>
<td>0.370</td>
<td>0.927</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPO</td>
<td>0.050</td>
<td>0.102</td>
<td>0.052</td>
<td>0.968</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td>0.335</td>
<td>0.312</td>
<td>0.176</td>
<td>0.060</td>
<td>0.820</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PS</td>
<td>0.533</td>
<td>0.508</td>
<td>0.283</td>
<td>0.063</td>
<td>0.145</td>
<td>0.851</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSS</td>
<td>0.292</td>
<td>0.265</td>
<td>0.862</td>
<td>0.090</td>
<td>0.144</td>
<td>0.281</td>
<td>0.854</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PV</td>
<td>0.476</td>
<td>0.503</td>
<td>0.161</td>
<td>0.168</td>
<td>0.211</td>
<td>0.544</td>
<td>0.102</td>
<td>0.898</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RE</td>
<td>0.421</td>
<td>0.598</td>
<td>0.253</td>
<td>0.134</td>
<td>0.253</td>
<td>0.464</td>
<td>0.229</td>
<td>0.478</td>
<td>0.873</td>
<td></td>
</tr>
<tr>
<td>SE</td>
<td>0.468</td>
<td>0.568</td>
<td>0.192</td>
<td>0.122</td>
<td>0.458</td>
<td>0.375</td>
<td>0.139</td>
<td>0.493</td>
<td>0.635</td>
<td>0.754</td>
</tr>
</tbody>
</table>

The square root of the AVE values reported for AC (0.953), IC (0.937), PCS (0.927), PPO (0.968), RC (0.820), PS (0.851), PSS (0.851), PV (0.898), RE (0.873), and SE (0.754) is shown in Table 9. It shows that the calculated square root of each AVE value is greater than all other latent variables’ correlations. As a result, the criterion of the discriminant validity was met.
**Research Hypotheses**

The study examined factors that influence employees’ compliance with password policies. Specifically, it examined the relationship between perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, perceived psychological ownership, intention to comply with password policies, and the actual compliance with password policies. The following hypotheses were tested:

H1a: Perceived vulnerability threat is positively related to employees’ intention to comply with password policies.

H1b: Perceived severity threat is positively related to employees’ intention to comply with password policies.

H1c: Response efficacy is positively related to employees’ intention to comply with password policies.

H1d: Self-efficacy is positively related to employees’ intention to comply with password policies.

H1e: Response cost is negatively related to employees’ intention to comply with password policies.

H1f: Perceived severity sanction of noncompliance is positively related to employees’ intention to comply with password policies.

H1g: Perceived certainty sanction of noncompliance is positively related to employees’ intention to comply with password policies.

H1h: Perceived psychological ownership of the organizational account is positively related to employees’ intention to comply with password policies.
H2: Employees’ intention to comply with password policies is positively related to their actual compliance with the password policies.

The study tested nine hypotheses by estimating path coefficients and using Smart PLS 3.0 software. The relationship among the independent variables and the dependent variables (hypotheses: H1a-H2) were tested and the results are presented in Figure 2 and Figure 3. They depict the standardized path coefficients ($\beta$) as well as the R-square ($R^2$) values for the hypothesized model. Path coefficients represent “the hypothesized relationships among the constructs” (Hair, Hult, et al., 2014, p. 171). Path coefficient values range from -1 to +1. Path coefficient values that are close to +1 represent strong positive relationships, and path coefficient values that are close to -1 represent strong negative relationships. On the other hand, path coefficient values that are close to 0 represent weak and nonsignificant relationships (Hair, Hult, et al., 2014).

In Figure 2, it can be deduced from path coefficients values that IC ($\beta=0.810$) has the strongest influence on AC. PCS ($\beta=0.361$) has the strongest influence on IC, followed by RE ($\beta = 0.265$), PSS ($\beta = -0.211$), SE ($\beta = 0.195$), PS ($\beta = 0.192$), and PV ($\beta = 0.124$).

**Figure 2**

*Path Coefficients*
Coefficient of determination ($R^2$ value) was used to evaluate the structural model and is defined as “a measure of the model’s predictive accuracy and is calculated as the squared correlation between a specific endogenous construct’s actual and predicted values” (Hair, Hult, et al., 2014, p. 174). $R^2$ explains the combined variance of the independent latent variables on the dependent latent variable (Hair, Hult, et al., 2014). Chin (1998) stated that $R^2$ value of 0.19 is considered weak, $R^2$ value of 0.33 is considered moderate, and $R^2$ value of 0.67 is considered significant. Figure 3 shows the coefficient of the determination for latent variables, $R^2$ for IC is 0.528 and $R^2$ for AC is 0.656. Thus, factors such as PV, PS, RE, SE, PRC, PSS, PCS and PPO predict about 52.8% of the variance in IC, whereas IC explains 65.6% of the variance in AC. The $R^2$ values are shown inside the circle or inside the construct (IC and AC).
Figure 3

PLS Analysis Results for $R^2$ values to explain the variance of independent variables on the dependent variable.
The bootstrapping technique was used to examine the significance of the structural model. Since the sample is small, the researcher preferred using the bootstrapping technique rather than the traditional method for better inferences about the population. According to Hair, Hult, et al. (2014), using 5000 subsamples, which are drawn with replacement from the original sample, is recommended to avoid bias.

Figure 4 and Table 10 illustrate the results of the bootstrapping analysis with 5000 bootstrap samples along with the path coefficients to assess the significance of the hypotheses using Smart PLS 3.0. The results show that RE ($\beta = 0.265$, $t = 2.371$, $p <0.05$), SE ($\beta = 0.195$, $t = 2.056$, $p <0.05$) and PCS ($\beta = 0.361$, $t = 2.562$, $p <0.05$) have a significant positive effect on intention to comply with password policies (protection motivation) (IC). This means that hypotheses H1c, H1d and H1g were fully supported. On the other hand, PSS ($\beta = -0.211$, $t =1.627$, $p >0.05$) has a negative insignificant effect on IC. However, this hypothesis (H1f) was not supported. Moreover, PV ($\beta = 0.124$, $t = 0.937$, $p >0.05$), PS ($\beta = 0.192$, $t = 1.693$, $p >0.05$), PRC ($\beta = 0.068$, $t = 1.056$, $p >0.05$), and PPO ($\beta = 0.006$, $t = 0.102$, $p >0.05$) have no significant positive effect on IC. Thus, hypotheses H1a, H1b, H1e, H1f and H1h were not supported.

Regarding the influence of IC on AC, it was found that there was a strong positive influence of IC ($\beta = 0.810$, $t = 20.712$, $p <0.05$) on AC. Therefore, this hypothesis (H2) was supported. This means that intention to comply (IC) with password policy is positively related to the actual compliance with the password policies (AC). For the summary of the results (see Table 10).
Figure 4

Bootstrapping Analysis Results for Factors That Influence Employees’ Compliance with Password Policies
Table 10

Summary of Hypotheses Testing for H1a-H2

<table>
<thead>
<tr>
<th>H</th>
<th>Path</th>
<th>Path Coefficients</th>
<th>t-value</th>
<th>p-value</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1a</td>
<td>PV → IC</td>
<td>0.124</td>
<td>0.937</td>
<td>0.371</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H1b</td>
<td>PS → IC</td>
<td>0.192</td>
<td>1.693</td>
<td>0.078</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H1c</td>
<td>RE → IC</td>
<td>0.265</td>
<td>2.371</td>
<td>0.020</td>
<td>Supported</td>
</tr>
<tr>
<td>H1d</td>
<td>SE → IC</td>
<td>0.195</td>
<td>2.056</td>
<td>0.040</td>
<td>Supported</td>
</tr>
<tr>
<td>H1e</td>
<td>PRC → IC</td>
<td>0.068</td>
<td>1.056</td>
<td>0.303</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H1f</td>
<td>PSS → IC</td>
<td>-0.211</td>
<td>1.627</td>
<td>0.123</td>
<td>Supported</td>
</tr>
<tr>
<td>H1g</td>
<td>PCS → IC</td>
<td>0.361</td>
<td>2.562</td>
<td>0.015</td>
<td>Supported</td>
</tr>
<tr>
<td>H1h</td>
<td>PPO → IC</td>
<td>0.006</td>
<td>0.102</td>
<td>0.922</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H2</td>
<td>IC → AC</td>
<td>0.810</td>
<td>20.712</td>
<td>0.000</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Summary

This chapter revealed the study findings. First, the expert panel’s review results were outlined, and slight changes were made to the instrument based on the expert panel’s feedback. Second, the custom qualification technique was described along with its results and ended with 425 qualified employees. Third, the pilot study was conducted with 39 participants. Based on the results, a few adjustments to the instrument were made. Finally, the actual study was conducted to examine the proposed hypotheses along with pre-analysis data screening, the reliability and the validity of the instrument, and descriptive and inferential statistics using SPSS and SmartPLS 3.0. Among the nine proposed hypotheses, the results revealed that H1c, H1d, and H1g had a major effect on the intention to comply (IC) with passwords and were thus fully supported. In addition, H2 had a significant effect on the actual compliance with the password policies and were therefore fully supported.
Nevertheless, the rest of the hypotheses (H1a, H1b, H1e, H1f, and H1h) were not supported. These results are explained further in Chapter 5.
Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Employees’ low motivation to comply with password policies increases passwords susceptibility (Choong et al., 2014; Habib et al., 2018; Inglesant & Sassa, 2010; Shay et al., 2010), and consequently leads to financial damages to organizations (Wakefield, 2004). A few studies have examined the influence of employees’ intention to comply with password policies (Anye, 2019; Choong & Theofanos, 2015). Mwagwabi (2015) as well as Mwagwabi et al. (2018) also asserted that there is a lack of password research that links the intention to comply with the actual compliance behaviors.

This study aimed to address the scarcity of research by examining what factors influence employees’ compliance with password policies. The research goal was achieved by applying the theoretical model to assess the relationship between employees’ perceptions of threat vulnerability, threat severity, response efficacy, self-efficacy, response cost, severity of sanction, certainty of sanction, psychological ownership, and their intention to comply with password policies, as well as the relationship between the intentions to comply with the actual password policies compliance.

The hypotheses (H1a-H1e) integrated PMT constructs of perceived vulnerability threat, perceived severity threat, response cost, response efficacy, and self-efficacy, and
how they predict employees’ intention to comply with password policies. As shown in the results, this study found that response efficacy influenced employees’ intention to comply with password policies, which is supported by previous studies. For example, Johnston and Warkentin (2010) noticed that response efficacy positively influenced users’ intention to fulfill the suggested security measures. Posey et al. (2015) revealed that response efficacy had the most significant effect on employees’ protection motivation behaviors among other constructs. Ifinedo (2012) showed that response efficacy positively influenced intention to comply with IS policies in an organizational setting. Moreover, Mwagwabi (2015) as well as Mwagwabi et al. (2014) found that perceived password response efficacy influences user’s intention to comply with password guidelines. Similarly, Kusyanti and Sari (2017) contended that response efficacy influences the intention to change passwords among university students.

This study also found that self-efficacy positively influences employee’s intention to comply with password policies, which is supported by previous studies. For example, Johnston and Warkentin (2010) found that self-efficacy has a positive impact on users’ intention to comply with security measures. Anye (2019) revealed that self-efficacy is positively related to employees’ intentions to comply with password policies. Mwagwabi (2015) as well as Mwagwabi et al. (2014) contended that self-efficacy significantly influences Internet users’ intention to comply with password guidelines. Additionally, Ifinedo (2012) uncovered that self-efficacy significantly influences employees’ intention to comply with IS policies.

Perceived severity threat, on the other hand, has no influence on employees’ intention to comply with password policies as hypothesized, which is supported by Ifinedo (2012) and Posey et al. (2015). Ifinedo (2012) as well as Posey et al. (2015) found that perceived severity was insignificantly related to intention to comply with IS policies and
protection motivation of insiders’ security behaviors, respectively. However, Siponen et al. (2014) as well as Mwagwabi et al. (2014) found that perceived severity positively associated with employees’ intention to comply with IS policy and Internet users’ intention to comply with password guidelines, respectively. Giwah (2019) inferred that response efficacy and self-efficacy dismiss the effect of perceived severity threat. In this study, both response efficacy and self-efficacy have significant influences on intention to comply with password policies, which would dismiss the effect of perceived severity threat on the intention to comply with password policies.

Perceived vulnerability threat, another threat appraisal, has no influence on employees’ intention to comply with password policies, which is contradicted by previous literature findings. For example, Zhang and McDowell (2009) asserted that perceiving a high degree of password vulnerability threat motivates individuals to behave securely to protect password from being compromised. Similarly, previous studies have found that perceived vulnerability threat positively predicts employees’ intention to comply with IS policies (Ifinedo, 2012; Siponen et al., 2014). Posey et al. (2015) also considered perceived vulnerability threat as a major component in forming protection motivation behaviors. In contrast, Kusyanti and Sari (2017) found that perceived vulnerability threat has no influence on students’ intention to reset passwords. Additionally, Mwagwabi et al. (2014), Mwagwabi (2015), as well as Mwagwabi et al. (2018) found that perceived vulnerability has no effect on Internet users’ intention to comply with password guidelines. Mwagwabi et al. (2014) suggested comparing the intention to comply between users who have been impacted by hacking and who have not in order to understand why perceived vulnerability did not influence Internet users’ intention to comply with password guidelines. Consequently, in 2015, Mwagwabi found that there is a relationship between exposure to hacking and perceived vulnerability, but still there is no relationship between perceived vulnerability
and users’ intention to comply with password guidelines. Mwagwabi (2015) suggested that users behave differently when safeguarding personal accounts versus organizational accounts. Ifinedo (2012) as well as Siponen et al. (2014) showed that there is an association between perceived vulnerability and the intention to comply with IS policies in organizational settings, while Mwagwabi (2015) showed that there is no association between perceived vulnerability and intention to comply with password guidelines in personal settings, which differs from this study setting. Therefore, the reason why perceived vulnerability had no influence on employees’ intention to comply with password policies is still unknown, which is recommended to be investigated in future research.

This study also revealed that response cost has no influence on employees’ intention to comply with password policies, which is contrary to previous studies’ findings. According to Kusyanti and Sari (2017), response cost had a negative influence on students’ intention to reset passwords. Additionally, Posey et al. (2015) found that response cost is negatively associated with employees’ protection motivation toward information assets. According to Herath and Rao (2009), response cost did not have a significant influence on compliance intentions, while response efficacy and self-efficacy had significant influences on compliance intentions. Posey et al. (2015) as well as Boss et al. (2015) also asserted that among coping appraisal constructs, self-efficacy and response efficacy have more effects than response cost on individual’s protection motivation. Boss et al. explained that response efficacy and self-efficacy outweigh the effect of response cost on individual’s protection motivation.

The hypotheses (H1f & H1g) integrated GDT constructs of perceived severity sanction and perceived certainty sanction, and how they predict employees’ intention to comply with password policies. This study revealed that only perceived certainty sanction influences employees’ intention to comply with password policies but not perceived
severity sanction. Herath and Rao (2009) also found that perceived certainty sanction has a positive effect on intention to comply with IS policies but not perceived severity sanction. Chen et al. (2012) showed that certainty of control and severity of sanction are significant in coercing complying with security policies. In addition, D’Arcy et al. (2009) implied that perceived severity of formal sanction has more influence than perceived certainty sanction; however, perceived certainty sanction has more influence than perceived severity sanction in deterring IS misuse only when the level of morality is high. D’Arcy et al. explained that people with high morality are more sensitive to certainty of sanction more than the severity of sanction because it is unpleasant to them to be accused of an undesirable act. Conversely, people with low morality are more concerned about penalties rather than being accused of an undesirable act. Therefore, the explanation of this study’s findings that only perceived certainty sanction affects the intention to comply with password policies, but not perceived severity sanction would refer to participants’ high morality.

Hypothesis (H1h) examined perceived psychological ownership as a predictor of employees’ intention to comply with password policies. The results revealed that perceived psychological ownership has no influence on employees’ intention to comply with password policies, which contradicts previous studies’ findings. According to Menard et al. (2018), psychological ownership negatively influenced intention not to protect information. Kim and Beehr (2017) also found that psychological ownership is negatively associated with work deviant behaviors. Additionally, Yoo et al. (2018) showed that psychological ownership significantly impacts the intention toward security compliance. Moreover, Van Dyne and Pierce (2004) found a positive relationship between psychological ownership and organizational behaviors. Therefore, the reason for the discrepancy in this study’s findings and previous studies’ findings is unknown. This can be explained by uncovering the
possible moderators’ effects or other organizational constructs that might offset the influence of psychological ownership.

The second hypothesis (H2) examined intention to comply with password policies as a predictor of the actual compliance with password policies. The results revealed that actual compliance with password policies is significantly influenced by the intention to comply with password policies. This finding is supported by the existing literature. Lau (2020) found that intention has a substantial influence on actual mobile device usage. Additionally, Siponen et al. (2014) implied that the intention to comply is positively related to the actual compliance with IS policies. Moreover, Boss et al. (2015) indicated that intention is related to the actual secure behaviors. However, Mwagwabi (2015) found no strong association between intention to comply and actual password compliance. Mwagwabi explained that the passwords created were only for the survey and do not reflect the actual behaviors.

**Limitations**

A few limitations were found in this study. The sample size and technique affected the accuracy as well as the generalizability of the results, respectively. The sample size was limited to the participants who are members of the MTurk pool. This study was based on self-reported data. In addition, this study was conducted with employees in general in the U.S. without specifying sectors, such as education and commerce. Moreover, this study collected information about employees’ security behaviors, which could depend on participants’ honesty in answering questions. Based on research by Knapp and Kirk (2003), study participants may be concerned about confidentiality when they disclose personal security behaviors. Therefore, participants may not be truthful in their responses when completing surveys related to password policies due to personal confidentiality concerns.
Implications

This study has practical and theoretical contributions in IS literature by investigating factors that may influence employees’ compliance with password policies. This study helped to bridge the existing gap by developing a theoretical model based on four behavioral theories: PMT, GDT, TRA, and psychological ownership theory. The theoretical model proposed in this study may be explored and expanded upon in future research studies to examine other security-related behaviors in various disciplines.

By determining the factors that influence employees’ password policy compliance, organizations will better understand their employees’ behaviors toward complying with password policies. Organizations can inspire employees’ password policies compliance by focusing on the most impactful predictors. Moreover, organizations can tailor training and education, and password policies designers can design new policies, while considering these factors to promote and motivate compliance with password policies among employees to prohibit financial losses.

The findings of this research study revealed several practical contributions to organizations. For instance, self-efficacy and response efficacy are predictors of intention to comply with password policies and consequently to the actual password policies’ compliance. Organizations should promote their employees’ beliefs and confidence regarding their ability to protect organizational passwords from being compromised by following policies, which consequently prevents information disclosure as well as financial losses. Herath and Rao (2009) asserted that individuals who have confidence and belief in their ability to undertake the activity will be more motivated to perform the action. Therefore, training and educating employees on new skills, that make it easy for them to follow the policies, are practical strategies. For example, organizations can train the employee on how to create strong and memorable passwords at the same time. In addition,
organizations need to inspire awareness among employees toward the password policies’ effectiveness in protecting organizational passwords. According to Zhang and McDowell (2009), individuals who believe that protection behaviors, such as creating a strong password and changing an old password, are effective in preventing threats will be more motivated to perform protection behaviors.

Organizations should also increase the certainty of sanction of noncompliance with password policies to deter employees from violating password policies. Organizations should monitor policies violation to confirm the certainty of being caught and consequently the certainty of being punished. According to Herath and Rao (2009), employees who are aware of being monitored and perceive a high chance of being detected are more likely to comply with policies.

**Recommendations**

This study recommends future studies continue examining other factors that may influence employees’ compliance with password policies. For example, this study suggests adding other PMT constructs to the model, such as maladaptive rewards (extrinsic and intrinsic), to examine their influences on employees’ intention to comply with password policies. Additionally, utilizing other behavioral theories is highly recommended to examine other factors that influence employees’ compliance with password policies.

Moreover, cultural differences may be added to the proposed model as moderator variables to examine their impact on other constructs. Dinev et al. (2009) recommended examining how cultural factors not only affect the behavioral intention but also the actual behaviors. Based on Hofstede (1983), the terminology of national cultures consists of four dimensions: (a) Individualism vs. Collectivism, (b) Masculinity vs. Femininity, (c) Large or Small Power Distance, and (d) Strong or Weak Uncertainty Avoidance. In 2012, Hovav and
D’Arcy found differences in cultures affect the impact of perceived severity and certainty sanctions on security countermeasure.

This study examined employees’ compliance with password policies in general. Therefore, the researcher suggests examining specific compliance behaviors, such as sharing passwords, writing passwords down, and creating weak passwords. Blythe et al. (2015) recommended reducing compliance to single security behavior to better understand what influence specific security behavior. Additionally, since this study was limited to MTurk employees, future research may be conducted to recruit a more diverse sample population to ensure the generalizability of results. Moreover, a quasi-experimental research design is recommended to compare trained or educated employees with those who are not.

Using the proposed model is highly recommended to examine other security behaviors. The researcher also recommended enhancing the instrument which could be applied in different IS contexts. This study could also be repeated in different sectors, such as education, commerce, and financial services. Abbott et al. (2018) stated that complying with a password policy among users in different organizations, such as banks, medical portals, and email providers, might differ.

Summary

This study addressed employees’ lack of compliance with password policies, which leads to security issues (Choong et al., 2014; Habib et al., 2018; Inglesant & Sassa, 2010; Shay et al., 2010). Several studies have examined employees’ behaviors in IS field (Blythe et al., 2015; Herath & Rao, 2009; Johnston & Warkentin, 2010; Posey et al., 2015; Sommestad et al., 2015). However, few studies were conducted specifically to understand employees’ password policies compliance (Anye, 2019; Choong & Theofanos, 2015). Additionally, there is a lack of research that associates the intention to comply with the
actual compliance (Mwagwabi, 2015; Mwagwabi et al., 2018). The main goal of this study was to examine factors that influence employees’ compliance with password policies. This study determined what influences employees’ compliance with password policies by examining the relationship between (perceived vulnerability threat, perceived severity threat, response efficacy, self-efficacy, response cost, perceived severity sanction, perceived certainty sanction, & perceived psychological ownership) and intention to comply with password policies, as well as the relationship between the intention to comply with password policies and the actual compliance with password policies.

The main research questions were:

RQ1: What is the relationship between (a) perceived vulnerability threat, (b) perceived severity threat, (c) response efficacy, (d) self-efficacy, (e) response cost, (f) perceived severity sanction of noncompliance, (g) perceived certainty sanction of noncompliance, (h) perceived psychological ownership to the organizational account, and employee’s intention to comply with password policies?

RQ2: What is the relationship between employees’ intention to comply with password policies and their actual compliance with password policies?

To answer these research questions, a quantitative cross-sectional study was conducted utilizing an adapted survey instrument that employed four behavioral theories. A non-probability convenience sample was utilized. The study was conducted in a non-contrived setting and without interference to examine what factors influence employees’ compliance with password policies. The adapted survey was reviewed by the expert panel using the Delphi technique and slight changes were made based on expert panel feedback. A custom qualification technique was used resulting in 425 qualified employees. A qualified participant is an adult employee who uses a password to log in to the organizational account and works at organizations in U. S. that have password policies to
comply with. Then, a pilot study was done with 39 participants out of the pool of 425 qualified participants. Afterwards, adjustments were made based on the pilot study results. The researcher invited all the 425 qualified participants to participate in the pilot study. The pilot study sample consisted of participants who were motivated to participate and completed the survey.

Finally, the actual study employed 151 participants. Pre-analysis data screening, and descriptive and inferential statistics were conducted using SPSS. In addition, SmartPLS 3.0 was used to examine instrument validity and the proposed hypotheses. The results revealed that (H1c, H1d, & H1g) have significant effects on intention to comply with password policies. To specify, self-efficacy, response efficacy, and perceived certainty sanction had significant influences on intention to comply with password policies. Additionally, intention to comply had a significant influence on employee actual compliance with password policies, which supports H2. On the other hand, (H1a, H1b, H1e, H1f, & H1h) had no significant effects on intention to comply with password policies. To specify, perceived vulnerability threat, perceived severity threat, perceived severity sanction, psychological ownership, and response cost had insignificant influences on employee’s intention to comply with password policies.

The limitations of this research study included factors, such as sample size and sample technique. The sample size was small, which affects the accuracy of the results, and the sample technique was convenient, which is not generalizable. Additionally, this study collected information about employees’ security behaviors and was based on self-reported data, which would affect participants’ truth on answering the survey questions and consequently the accuracy of the study results.

The findings of this study provided valuable insight into factors that may influence employee compliance with password policies by developing a theoretical model based on
four behavioral theories: PMT, GDT, TRA, and psychological ownership theory.

Determining the factors that influence employees’ password policy compliance may help organizations better understand their employees’ behaviors. Consequently, organizations can motivate employees’ password policies compliance by tailoring initiatives such as training, education, and password policies design, while considering the impactful factors.

This study recommended opportunities for future research to examine other security behaviors in different disciplines, while applying the developed theoretical model. Utilizing other behavioral theories is also highly recommended to examine other factors that would influence employees’ compliance with password policies. Future research is also needed on security behaviors to explore additional PMT constructs that may enhance the proposed model in this study, such as extrinsic and intrinsic maladaptive rewards. Moreover, national cultural dimensions could be added to the model for further investigation. Another recommendation is to recruit a large and diverse sample using experimental research design to ensure the generalizability of results.
Appendices
Appendix A: Survey Questionnaire

INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

Participant Letter for Anonymous Surveys
NSU Consent to be in a Research Study Entitled
Improving Employees’ Compliance with Password Policies

This is Enas Albataineh, a doctoral student with the College of Computing and Engineering at Nova Southeastern University in Florida. I’m working under the supervision of Dr. Ling Wang. The purpose of my dissertation is understanding the factors that contribute to employees’ compliance with password policies. You are being asked to take part in this research study because you are an adult employee who works at an organization which has password policies to obey, and you use a password to log in to your organizational account. If you agree to participate in this study, you will be taking a one-time, anonymous survey. The survey will take about 15 minutes to complete.

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life. You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time. Additionally, there is no cost for participation in this study. Participation is voluntary and a $1.5 payment will be provided upon completion of the survey.

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Your personal identifiable information will not be collected or stored. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution.

If you have questions, you can contact Enas Albataineh at ea642@mynsu.nova.edu or Dr. Wang at lingwang@nova.edu. If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-6389 or toll free at 1-866-499-0790 or email at IRB@nova.edu

If you have read the above information and voluntarily wish to participate in this research study, please click “Start” button.

Sincerely,
Enas Albataineh
Survey Questionnaire

General Information

Age:
- 18-25 years
- 26-35 years
- 36-45 years
- 46-55 years
- 56-65 years
- Older than 65

Gender:
- Male
- Female

Computer Skills:
- Low
- Medium
- High

Highest level of education completed:
- Less than a high school diploma
- High school diploma
- Associate degree
- Undergraduate degree
- Graduate degree

Ethnicity:
- African-American
- American Indian or Alaska Native
- Asian
- Native Hawaiian or other Pacific Islander
- White
- Hispanic
- Other

When you provide responses to the following survey items, please keep in mind password policies can be violated by writing password down, sharing password with anyone, creating same password for different accounts, creating password that has a proper name or
Feeling confident to answer
Your responses are anonymous, and your personal identifiable information will not be collected.

Please indicate your perception level with the following statements.

**Perceived Vulnerability Threat**

| PV1: I know that my organizational password could be vulnerable to security breaches if I don’t follow my organization’s password policies. |
|---|---|---|---|---|---|---|
| Strongly disagree | Disagree | Somewhat disagree | Neither agree or disagree | Somewhat agree | Agree | Strongly agree |
| ○ | ○ | ○ | ○ | ○ | ○ | ○ |

| PV2: I could fall victim to password attacks if I fail to comply with my organizational password policies. |
| PV3: I believe that trying to protect my organizational password will reduce illegal access to it. |
| PV4: My organizational password may be compromised if I don’t pay adequate attention to password policies. |

| Perceived Severity Threat |
|---|---|---|---|---|---|---|
| PS1: Threats on my organizational account would be a serious problem. |
| PS2: Loss of data resulting from compromising my organizational password would be a serious problem. |
| PS3: Having my organizational account accessed by someone else without my permission or knowledge would be a serious problem. |
| PS4: Having security breaches successfully attack my organizational account would be very problematic. |
| PS5: I view password security attacks on my organizational password as harmful. |
| PS6: I believe that threat to my organizational password is severe. |

| PS1: Threats on my organizational account would be a serious problem. |
| PS2: Loss of data resulting from compromising my organizational password would be a serious problem. |
| PS3: Having my organizational account accessed by someone else without my permission or knowledge would be a serious problem. |
PS4: Having security breaches successfully attack my organizational account would be very problematic.

PS5: I view password security attacks on my organizational password as harmful.

PS6: I believe that threat to my organizational password is severe.

Self-Efficacy

SE1: I feel comfortable following password policies to protect my organizational password.

SE2: I have the necessary skills to implement the requirements of password policies in order to protect my organizational password.

SE3: I have the knowledge and resources to fulfill the requirements of password policies.

SE4: Following password policies is easy.

SE5: I’m able to follow password policies by myself.

SE6: I can enable password policies on my organizational password.

Response Efficacy

RE1: If I were to engage in efforts to protect my organizational password, those efforts would be effective.

RE2: Password policies that protect organizational passwords are effective.

RE3: Preventive password policies available to me are adequate to prevent unauthorized persons from accessing my organizational password.

RE4: Preventive password policies available to me are adequate to prevent password security attacks from guessing my organizational password.
RE1: If I were to engage in efforts to protect my organizational password, those efforts would be effective.

RE2: Password policies that protect organizational passwords are effective.

RE3: Preventive password policies available to me are adequate to prevent unauthorized persons from accessing my organizational password.

RE4: Preventive password policies available to me are adequate to prevent password security attacks from guessing my organizational password.

### Response Cost *

<table>
<thead>
<tr>
<th>Response Cost</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Somewhat disagree</th>
<th>Neither agree or disagree</th>
<th>Somewhat agree</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC1: Complying with password policies' requirements is time consuming for me.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>RC2: Complying with password policies' requirements is burdensome for me.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>RC3: Complying with password policies' requirements is costly for me.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>RC4: Complying with the requirements of password policies is inconvenience for me.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>RC5: The cost of complying with the requirements of password policies exceeds the benefits.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

### Perceived Severity Sanction *

<table>
<thead>
<tr>
<th>Perceived Severity Sanction</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Somewhat disagree</th>
<th>Neither agree or disagree</th>
<th>Somewhat agree</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSS1: My organization terminates employees who violate password policies repeatedly.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>PSS2: If I were caught violating my organization's password policies, I would be punished severely.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>PSS3: I would receive reprimand in oral if I were caught violating my organization's password policies.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>PSS4: I would receive reprimand in written report if I were caught violating my organization's password policies.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
PSS1: My organization terminates employees who violate password policies repeatedly.

PSS2: If I were caught violating my organization's password policies, I would be punished severely.

PSS3: I would receive reprimand in oral if I were caught violating my organization's password policies.

PSS4: I would receive reprimand in written report if I were caught violating my organization's password policies.

Perceived Certainty Sanction *

<table>
<thead>
<tr>
<th>PCS1: If I don't follow password policies, I will be punished.</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Somewhat disagree</th>
<th>Neither agree or disagree</th>
<th>Somewhat agree</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCS2: If I violate password policies, I would probably get caught.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCS1: If I don't follow password policies, I will be punished.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCS2: If I violate password policies, I would probably get caught.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Perceived Psychological Ownership *

<table>
<thead>
<tr>
<th>PPO1: I feel like my work account is mine.</th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Somewhat disagree</th>
<th>Neither agree or disagree</th>
<th>Somewhat agree</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPO2: I feel a high degree of personal ownership of my work account.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPO3: I sense that I own my work account.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPO1: I feel like my work account is mine.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPO2: I feel a high degree of personal ownership of my work account.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPO3: I sense that I own my work account.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Intention to Comply with Password Policies (Protection Motivation) *

| IC1: I intend to comply with the requirements of my organization's password policies. | Strongly disagree | Disagree | Somewhat disagree | Neither agree or disagree | Somewhat agree | Agree | Strongly agree |
| IC2: I intend to protect my work account according to the requirements of my organization's password policies. | 
| IC3: I intend to carry out my responsibility prescribed in my organization's password policies whenever possible. | 
| IC1: I intend to comply with the requirements of my organization's password policies. | 
| IC2: I intend to protect my work account according to the requirements of my organization's password policies. | 
| IC3: I intend to carry out my responsibility prescribed in my organization's password policies whenever possible. |
IC4: My intention is to continue complying with my organization's password policies in the future.
IC1: I intend to comply with the requirements of my organization's password policies.
IC2: I intend to protect my work account according to the requirements of my organization's password policies.
IC3: I intend to carry out my responsibility prescribed in my organization's password policies whenever possible.
IC4: My intention is to continue complying with my organization's password policies in the future.

**Actual Compliance with Password Policies**

<table>
<thead>
<tr>
<th></th>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Somewhat disagree</th>
<th>Neither agree or disagree</th>
<th>Somewhat agree</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC1: I adhere to the password policies that exist at my organization.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>AC2: To the best of my knowledge, I do not violate password policies that exist at my organization.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>AC3: I currently work entirely in accordance with the password policies that exist at my organization.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>AC1: I adhere to the password policies that exist at my organization.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>AC2: To the best of my knowledge, I do not violate password policies that exist at my organization.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>AC3: I currently work entirely in accordance with the password policies that exist at my organization.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
Appendix B: IRB Exempt Initial Approval Memo

MEMORANDUM

To: Enas Albataineh
   College of Engineering and Computing

From: Ling Wang, Ph.D.
      College Representative, College of Engineering and Computing

Date: December 4, 2020

Subject: IRB Exempt Initial Approval Memo

TITLE: Improving Employees' Compliance with Password Policies—NSU IRB Protocol Number 2020-623

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on December 4, 2020. You may proceed with your study.

Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Annual Status of Research Update: You are required to notify the IRB Office annually if your research project is still active.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-5369 • 866-499-0790 • Fax: (954) 262-3977 • Email: irb@nova.edu • Web site: www.nova.edu/irb

Page 1 of 2
research study is still ongoing via the *Exempt Research Status Update xForm*.

**Final Report:** You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm*.

**Translated Documents:** No

*Please retain this document in your IRB correspondence file.*

CC: Ling Wang, Ph.D.
    Ling Wang, Ph.D.
Appendix C: IRB Amendment Approval Memo

MEMORANDUM

To: Enas Albataineh
    College of Engineering and Computing

From: Office of the Institutional Review Board

Date: January 21, 2021

Subject: IRB Exempt Amendment Approval Memo

TITLE: Improving Employees' Compliance with Password Policies—NSU IRB Protocol Number 2020-623

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on December 4, 2020. You may proceed with your study.

Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

Type of Approval: Amendment
**Exempt Review Category:** Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

**Post-Approval Monitoring:** The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

**Annual Status of Research Update:** You are required to notify the IRB Office annually if your research study is still ongoing via the *Exempt Research Status Update xForm.*

**Final Report:** You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm.*

The following modifications were approved:

- Addition of/change to study population
- Addition of/change to survey(s), questionnaire(s), or other research instruments

Translated Documents: No

*Please retain this document in your IRB correspondence file.*

**CC:** Ling Wang, Ph.D.

Ling Wang, Ph.D.
Appendix D: Custom Qualification Questions

1. Are you 18 years old or above?
   - Yes
   - No

2. Do you work at an organization that has password policies for the employees to obey?
   - Yes
   - No

3. Do you use password to log in to your organizational account?
   - Yes
   - No
### Appendix E: Pilot Study’s Factor Analysis

<table>
<thead>
<tr>
<th>Variable</th>
<th>Factor 1</th>
<th>Factor 2</th>
<th>Factor 3</th>
<th>Factor 4</th>
<th>Factor 5</th>
<th>Factor 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Vulnerability Threat [PV4: My organizational password may be compromised if I don't pay adequate attention to password policies.]</td>
<td>.224</td>
<td>.331</td>
<td>.089</td>
<td>.272</td>
<td>.788</td>
<td>.250</td>
</tr>
<tr>
<td>Perceived Vulnerability Threat [PV2: I could fall victim to password attacks if I fail to comply with my organizational password policies.]</td>
<td>.093</td>
<td>.173</td>
<td>.270</td>
<td>.285</td>
<td>.719</td>
<td>.031</td>
</tr>
<tr>
<td>Perceived Vulnerability Threat [PV1: I know that my organizational password could be vulnerable to security breaches if I don't follow my organization's password policies.]</td>
<td>.399</td>
<td>.233</td>
<td>.171</td>
<td>.134</td>
<td>.714</td>
<td>.138</td>
</tr>
<tr>
<td>Perceived Vulnerability Threat [PV3: I believe that trying to protect my organizational password will reduce illegal access to it.]</td>
<td>.315</td>
<td>.346</td>
<td>.152</td>
<td>.139</td>
<td>.594</td>
<td>.260</td>
</tr>
<tr>
<td>Intention to Comply with Password Policies (Protection Motivation) [IC2: I intend to protect my work account according to the requirements of my organization's password policies.]</td>
<td>.944</td>
<td>.159</td>
<td>.153</td>
<td>-.052</td>
<td>.038</td>
<td>.188</td>
</tr>
<tr>
<td>Intention to Comply with Password Policies (Protection Motivation) [IC1: I intend to comply with the requirements of my organization's password policies.]</td>
<td>.935</td>
<td>.125</td>
<td>.179</td>
<td>-.058</td>
<td>.005</td>
<td>.191</td>
</tr>
<tr>
<td>Intention to Comply with Password Policies (Protection Motivation) [IC4: My intention is to continue complying with my organization's password policies.]</td>
<td>.905</td>
<td>.121</td>
<td>.157</td>
<td>-.024</td>
<td>.051</td>
<td>.211</td>
</tr>
<tr>
<td>Intention to Comply with Password Policies (Protection Motivation) [IC3: I intend to carry out my responsibility prescribed in my organization's password policies whenever possible.]</td>
<td>.904</td>
<td>.186</td>
<td>.168</td>
<td>.017</td>
<td>.071</td>
<td>.213</td>
</tr>
<tr>
<td>Perceived Severity Threat [PS5: I view password security attacks on my organizational password as harmful.]</td>
<td>.823</td>
<td>.204</td>
<td>.143</td>
<td>.108</td>
<td>.353</td>
<td>.057</td>
</tr>
<tr>
<td>Perceived Severity Threat [PS1: Threats on my organizational account would be a serious problem.]</td>
<td>.738</td>
<td>.184</td>
<td>.135</td>
<td>.375</td>
<td>.302</td>
<td>.069</td>
</tr>
<tr>
<td>Perceived Severity Threat [PS6: I believe that threat to my organizational password is severe.]</td>
<td>.631</td>
<td>.078</td>
<td>.277</td>
<td>.287</td>
<td>.350</td>
<td>-.089</td>
</tr>
<tr>
<td>Perceived Severity Threat [PS3: Having my organizational account accessed by someone else without my permission or knowledge would be a serious problem.]</td>
<td>.629</td>
<td>.164</td>
<td>.250</td>
<td>.435</td>
<td>.327</td>
<td>-.160</td>
</tr>
<tr>
<td>Perceived Severity Threat [PS4: Having security breaches successfully attack my organizational account would be very problematic.]</td>
<td>.604</td>
<td>.104</td>
<td>.226</td>
<td>.352</td>
<td>.439</td>
<td>-.294</td>
</tr>
<tr>
<td>Perceived Severity Threat [PS2: Loss of data resulting from compromising my organizational password would be a serious problem.]</td>
<td>.560</td>
<td>.123</td>
<td>.281</td>
<td>.584</td>
<td>.272</td>
<td>-.134</td>
</tr>
<tr>
<td>Perceived Psychological Ownership [PPO3: I sense that I own my work account.]</td>
<td>.026</td>
<td>.150</td>
<td>.155</td>
<td>.883</td>
<td>.100</td>
<td>.201</td>
</tr>
<tr>
<td>Perceived Psychological Ownership [PPO2: I feel a high degree of personal ownership of my work account.]</td>
<td>.144</td>
<td>.112</td>
<td>.135</td>
<td>.854</td>
<td>.175</td>
<td>.021</td>
</tr>
</tbody>
</table>
Appendix E: Pilot Study’s Factor Analysis (continued)

| Perceived Psychological Ownership [PPO1: I feel like my work account is mine.] | .007 | .178 | .106 | .761 | .369 | .307 |
| Self-Efficacy [SE4: I have the knowledge and resources to fulfill the requirements of password policies.] | .052 | .786 | .140 | .052 | .110 | .173 |
| Self-Efficacy [SE3: I have the necessary skills to implement the requirements of password policies in order to protect my organizational password.] | .071 | .867 | .172 | .050 | .145 | .115 |
| Response Efficacy [RE3: Preventive password policies available to me are adequate to prevent unauthorized persons from accessing my organizational password.] | .052 | .860 | .041 | .240 | .193 | .037 |
| Response Efficacy [RE4: Preventive password policies available to me are adequate to prevent password security attacks from guessing my organizational password.] | .088 | .850 | .071 | .152 | .215 | .049 |
| Response Efficacy [RE2: Password policies that protect organizational passwords are effective.] | .308 | .795 | .124 | .207 | .147 | .055 |
| Response Efficacy [RE1: If I were to engage in efforts to protect my organizational password, those efforts would be effective.] | .321 | .785 | .104 | .034 | .055 | .085 |
| Self-Efficacy [SE7: I can enable password policies on my organizational password.] | .142 | .609 | .056 | .108 | .034 | .463 |
| Perceived Severity Sanction [PSS3: If I were caught violating my organization’s password policies, I would be punished severely.] | .160 | .039 | .937 | .070 | .016 | .017 |
| Perceived Severity Sanction [PSS5: I would receive reprimand in written report if I were caught violating my organization’s password policies.] | .160 | .043 | .914 | .065 | .045 | .019 |
| Perceived Certainty Sanction [PCS1: If I don’t follow password policies, I will be punished.] | .134 | .028 | .886 | .220 | .127 | .050 |
| Perceived Severity Sanction [PSS1: My organization punishes employees who break password policies.] | .102 | .054 | .881 | .104 | .124 | .022 |
| Perceived Severity Sanction [PSS2: My organization terminates employees who violate password policies repeatedly.] | .099 | .007 | .801 | .077 | .167 | .055 |
| Perceived Severity Sanction [PSS4: I would receive reprimand in oral if I were caught violating my organization’s password policies.] | .181 | .110 | .737 | .112 | .044 | .003 |
| Perceived Certainty Sanction [PCS2: If I violate password policies, I would probably get caught.] | .244 | .046 | .710 | .243 | .130 | .069 |
| Self-Efficacy [SE5: Following password policies is easy.] | .218 | .243 | .043 | .175 | .124 | .681 |
| Self-Efficacy [SE1: I feel comfortable following password policies to protect my organizational password.] | .399 | .395 | .095 | .142 | .361 | .620 |
| Self-Efficacy [SE2: Following password policies is entirely under my control.] | .145 | .382 | .005 | .388 | .153 | .451 |
| Perceived Severity Threat [PS7: I believe that threat to my organizational password is significant.] | .496 | .064 | .300 | .284 | .476 | .251 |

Extraction Method: Alpha Factoring.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.
Appendix F: Test of Assumptions

Figure 5

*Histogram*

![Histogram of Regression Standardized Residuals]

- Mean: -2.69E-15
- Std Dev: 0.370
- N: 151

Figure 6

*P-P Plot*

![P-P Plot of Regression Standardized Residuals]

- Dependent Variable: AC
### Figure 7

**Collinearity Statistics**

<table>
<thead>
<tr>
<th>Model</th>
<th>Unstandardized Coefficients</th>
<th>Standardized Coefficients</th>
<th>Collinearity Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
<td>Std. Error</td>
<td>Beta</td>
</tr>
<tr>
<td>1</td>
<td>(Constant)</td>
<td>-796</td>
<td>.506</td>
</tr>
<tr>
<td></td>
<td>PV</td>
<td>.048</td>
<td>.050</td>
</tr>
<tr>
<td></td>
<td>PS</td>
<td>.173</td>
<td>.061</td>
</tr>
<tr>
<td></td>
<td>SE</td>
<td>.053</td>
<td>.097</td>
</tr>
<tr>
<td></td>
<td>RE</td>
<td>-241</td>
<td>.083</td>
</tr>
<tr>
<td></td>
<td>RC</td>
<td>.065</td>
<td>.037</td>
</tr>
<tr>
<td></td>
<td>PBS</td>
<td>.006</td>
<td>.058</td>
</tr>
<tr>
<td></td>
<td>PCS</td>
<td>.044</td>
<td>.055</td>
</tr>
<tr>
<td></td>
<td>PPD</td>
<td>-0.16</td>
<td>.026</td>
</tr>
<tr>
<td></td>
<td>IC</td>
<td>.995</td>
<td>.090</td>
</tr>
</tbody>
</table>

*a. Dependent Variable: AC*

### Figure 8

**Scatterplot**

![Scatterplot](image)
Figure 9

Durbin-Watson Statistics Results

\begin{center}
\textbf{Model Summary}\textsuperscript{b}
\end{center}

\begin{tabular}{|l|c|c|c|c|}
\hline
Model & R & R Square & Adjusted R Square & Std. Error of the Estimate & Durbin-Watson \\
\hline
1 & .838\textsuperscript{a} & .703 & .684 & .53113 & 1.956 \\
\hline
\end{tabular}

\textit{a.} Predictors: (Constant), IC, PPO, PSS, RC, PV, PS, RE, SE, PCS

\textit{b.} Dependent Variable: AC

Figure 10

Cook’s Distance Statistics

\begin{center}
\textbf{Residuals Statistics}\textsuperscript{a}
\end{center}

\begin{tabular}{|l|c|c|c|c|c|}
\hline
 & Minimum & Maximum & Mean & Std. Deviation & N \\
\hline
Predicted Value & 1.8725 & 7.4178 & 6.3775 & .79133 & 151 \\
Std. Predicted Value & -.5693 & 1.315 & .000 & 1.000 & 151 \\
Standard Error of Predicted Value & .067 & .349 & .128 & .048 & 151 \\
Adjusted Predicted Value & 1.6604 & 7.4575 & 6.3761 & .79053 & 151 \\
Residual & -2.75877 & 1.55186 & .00000 & .51495 & 151 \\
Std. Residual & -5.194 & 2.922 & .000 & .970 & 151 \\
Std. Residual & -5.390 & 3.089 & .001 & 1.026 & 151 \\
Deleted Residual & -2.97017 & 1.73501 & .00138 & .57807 & 151 \\
Std. Deleted Residual & -6.027 & 3.188 & -.006 & 1.070 & 151 \\
Mahal. Distance & 1.393 & 63.763 & 8.940 & 8.958 & 151 \\
Cook’s Distance & .000 & .357 & .013 & .047 & 151 \\
Centered Leverage Value & .009 & .425 & .060 & .060 & 151 \\
\hline
\end{tabular}

\textit{a.} Dependent Variable: AC
References


