

2020

The Influence of Cognitive Factors and Personality Traits on Mobile Device User's Information Security Behavior

Nils Lau

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



Part of the [Computer Sciences 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.

The Influence of Cognitive Factors and Personality Traits on Mobile Device
User's Information Security Behavior

by

Nils Lau

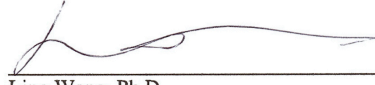
A dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Information Systems

College of Computing and Engineering

Nova Southeastern University

2020

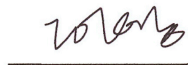
We hereby certify that this dissertation, submitted by Nils Lau conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Ling Wang, Ph.D.
Chairperson of Dissertation Committee

5/11/2020

Date



Inkyoung Hur, Ph.D.
Dissertation Committee Member

5/11/2020

Date




Marlon Clarke, Ph.D.
Dissertation Committee Member

5/11/2020

Date

Approved:



Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

05/11/2020

Date

College of Computing and Engineering
Nova Southeastern University

2020

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

The Influence of Cognitive Factors and Personality Traits on Mobile Device User's Information Security Behavior

by
Nils Lau
April 2020

As individuals have become more dependent on mobile devices to communicate, to seek information, and to conduct business, their susceptibility to various threats to information security has also increased. Research has consistently shown that a user's intention is a significant antecedent of information security behavior. Although research on user's intention has expanded in the last few years, not enough is known about how cognitive factors and personality traits impact the adoption and use of mobile device security technologies.

The purpose of this research was to empirically investigate the influence of cognitive factors and personality traits on mobile device user's intention in regard to mobile device security technologies. A conceptual model was developed by combining constructs from both the Protection Motivation Theory (PMT) and the Big Five Factor Personality Traits. The data was collected using a web-based survey according to specific inclusion and exclusion criteria. Respondents were limited to adults 18 years or older who have been using their mobile devices to access the internet for at least one year. The Partial Least Square Structural Equation Modeling (PLS-SEM) was used to analyze the data gathered from a total of 356 responses received.

The findings of this study show that perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, and mobile self-efficacy have a significant positive effect on user's intention. In particular, mobile self-efficacy had the strongest effect on the intention to use mobile device security technologies. Most of the personality traits factors were not found significant, except for conscientiousness. The user's intention to use mobile device security technologies was found to have a significant effect on the actual usage of mobile device security technologies. Hence, the results support the suitability of the PMT and personality factors in the mobile device security technologies context. This study has contributed to information security research by providing empirical results on factors that influence the use of mobile device security technologies.

Acknowledgments

I thank you God for giving me the strength to commence this doctoral program and the wisdom to complete this journey successfully. Through your grace I have overcome obstacles that seem insurmountable. Thank you God for all your blessings to me and my family.

I cannot express enough thanks to my committee chair, Dr. Ling Wang, for her direction, advice, and having patience with me throughout the dissertation process. Personally, I can truly say that without your continued support and encouragement I could not have achieved the milestone of completing the Dissertation Report. Dr. Wang is the best mentor that a Ph.D. student could have.

Further, I would like to thank Dr. Inkyoung Hur for her valuable feedback, thoughtful comments, and suggestions. Thank you Dr. Hur for encouraging my research and for allowing me to grow as a researcher. I would also like to express my special appreciation and thanks to Dr. Marlon Clarke, you have been a tremendous mentor for me. Your advice on both research as well as on my career have been invaluable. Thank you Dr. Hur and Dr. Clarke for serving as my dissertation committee members.

Thank you Melissa Champlain for your love and support throughout the years. I thank you for taking care of me and our daughters so I could accomplish this goal. Thank you for your understanding. To my daughters, thank you for always cheering me up. I am extremely grateful to my parents Glenda Sanchez and Ricardo Lau for their love, prayers, caring, and sacrifices for educating and preparing me for my future.

A huge thank you to Mark Gonzalez for providing me with a flexible work schedule so I could complete my study. Finally, I thank everyone who contributed in one form or another to this research. Those who gave up valuable time to participate in the survey, I thank you for your contribution. Lastly, to my friends and colleagues, who supported and cheered me on throughout the process - thank you!

May God bless you all!

Table of Contents

Abstract iii
List of Tables vii
List of Figures viii

Chapters

1. Introduction 1
Background 1
Problem Statement 3
Dissertation Goal 5
Research Question 9
Relevance and Significance 10
Barriers and Issues 12
Assumptions 12
Limitations 13
Delimitations 13
Definition of Terms 14
Summary 16

2. Literature Review 18
Overview 18
Theoretical Foundation 19
Hypotheses 21
Mobile Device Security 34
Past Literature and Identification of Gaps 37
Analysis of the Research Methods Used 40
Synthesis of the Literature 41
Summary 42

3. Methodology 44
Research Design 44
Instrument Development and Validation 46
 Expert panel 51
 Pilot test 52
 Instrument Validity and Reliability 53
 Internal validity 55
 External validity 56
Ethical Considerations 57
Population and Sample 57
Pre-analysis Data Screening 59
Data Analysis Strategy 61
Format for Presenting Results 62

Resource Requirements 62
Summary 63

4. Results 64

Overview 64
Phase One - Validation of Survey Instrument with an Expert Panel 64
Phase Two - Pilot Test 66
Phase Three - Main Data Collection Procedures 66
 Pre-analysis Data Screening 67
 Test of Assumptions 67
 Demographic Analysis 69
 Reliability and Validity 71
 Discriminant Validity 73
Research Questions and Hypotheses 74
Summary 78

5. Conclusions, Implications, Recommendations, and Summary 80

Conclusions 80
Limitations of the Study 85
Recommendation for Future Studies 86
Implications and Recommendations 87
Summary 90

Appendices 94

A. Constructs Items and Instrument Source 94
B. Institutional Review Board Approval Letter 103
C. Test of Assumptions 104
D. Outer Loadings Values after Factor Analysis 108
E. Square Root of Ave and the Correlations among the latent variables 109
F. PLS- SEM Results 110
G. Bootstrapping Significant Results 113

References 115

List of Tables

Tables

1. Original Study 50-items IPIP Instrument Reliability 49
2. Giwah (2018)'s study Instrument Reliability 49
3. Descriptive Statistics of the Population (N=356) 70
4. Construct Reliability and Validity for this Study's Constructs (N=356) 72
5. Construct Reliability and AVE for this Study's Constructs (N=356) 73
6. Summary of Hypotheses Testing for H1 to H11 (N = 356) 78
7. Construct Items and Instrument Source 94
8. Square Root of AVE and the Correlation Values among the Latent Variables 109

List of Figures

Figures

1. Research Model 8
2. Study Methodology 46
3. PLS Analysis Result for Mobile Device Security Usage (N=356) 75
4. Bootstrapping Results for Mobile Device Security Usage (N=356) 77
5. Scatterplot of the dependent variable MDSU 104
6. Durbin-Watson Statistics Results 104
7. Collinearity Statistics 105
8. Cook's Distance Statistics 105
9. Histogram of the dependent variable MDSU 106
10. Normal P-P Plot of the Regression Standardized Residual 107

Chapter 1

Introduction

Background

The use of mobile devices by organizations continues to rise, and with the increased usage, the numbers and levels of information security threats have increased (D'Arcy & Devaraj, 2012). As pointed out by Tu and Yuan (2012), as well as Tu, Turel, Yuan, and Archer (2015), mobile devices are more susceptible to data breaches than traditional computing systems as their mobility means data is carried everywhere and plugged into different insecure networks. Due to increasing mobility, small size, and processing ability, mobile devices are at much greater risk of being lost or stolen than traditional computing systems. Moreover, the problem of misplaced or stolen mobile devices is compounded by the fact that many users do not immediately report a mobile device's disappearance. According to a nationally representative survey conducted by the Kaspersky lab (2014), only 43 percent of users report the loss or theft of a mobile device the same day it occurs. Mobile devices certainly pose security challenges not common to traditional stationary computing systems, hence differences occur in the user behavior towards their security.

In the literature, the role of intention as a predictor of behavior has been well established (Mou, Cohen, & Kim, 2017; Venkatesh et al., 2003; Warkentin et al., 2012). As stated by Ajzen and Fishbein (1980), "intention is the immediate determinant of behavior" (p. 41). However, it is evident that mobile device users, despite knowing that

their individual information resources are at risk, fail to act on their intentions to practice mobile safe behavior. It is important for mobile device users to follow the intent to adopt secure technologies with actual usage behavior, however such follow-through is not universal. Mobile device users, despite having the intention to comply with information security policies, are still considered to be the weakest link in the defense against existing security threats as their actual security behavior may differ from their intended behavior (Han, Kwortnik Jr, & Wang, 2008; Vroom & Solms, 2004). It is a common observation that people often fail to act in accordance with their behavioral intention (Ajzen, Brown, & Carvajal, 2004). Despite management's concerns about security, companies have accepted the ubiquity of mobile devices in the work environment (Uffen, Kaemmerer, & Breitner, 2013; Xu, Frey, Fleisch, & Ilic, 2016). However, there is ample evidence to support the assertion that the majority of information security breaches in organizations occur internally and that users are responsible for most of the breaches (Besnard & Arief, 2004; Colwill, 2009; Shepherd & Kline, 2012; Shropshire, Warkentin, & Sharma, 2015).

While previous research has found user's intention to be a significant antecedent of information security adoption behavior, user's intention still covers only a small amount of variance of the actual usage behavior (Anderson & Agarwal, 2010; Crossler et al., 2013; Limayem, Hirt, & Cheung, 2007; Matt & Peckelsen, 2016; Shropshire et al., 2015). As a substantial part of the variance remains unexplained, other factors do notably influence the user's intention to use information security technologies. In the context of mobile device security behavior (such as data backup, biometric protection, password protection, etc.), it is evident that a great percentage of mobile device users have the intent to act in safe ways, but only some of these mobile device users will act on this

intent. According to Shropshire et al. (2015), empirical support for the relationship between user's intention and actual behavior is weak, indicating that there may be other factors that explain why certain individuals may not act on their intentions and follow through with appropriate behaviors. This gap between intention and actual behavior could be attributed to differences in cognitions or other unknown variables that influence user's intention (Matt & Peckelsen, 2016). According to Shropshire et al. (2015), as well as Matt and Peckelsen (2016), the user's intention, whether or not to adopt information security technologies, is not only cognitively governed, but also may depend on user's personality traits. As the security challenges presented by mobile devices and the need for secure user behavior has become more apparent, this study intends to understand how cognitive factors and personality traits explain user's intention to adopt mobile device security technologies.

Problem Statement

Although information security research is focused on measuring the actual behaviors based on behavioral intention (Giwah, 2018; Shropshire et al., 2015; Uffen et al., 2013), there have been intention-behavior discrepancies due to the presence of unknown variables that influence user's intention. This has led to lower accuracy among researchers in predicting information security compliance behavior (Crossler, Long, Loraas, & Trinkle, 2014). This dissertation study addresses a gap in the information security literature on the factors that influence user's intention to use mobile device security technologies. Previous researchers have focused on cognitive factors to explain mobile device security usage (Giwah, 2018; Uffen et al., 2013; Xu et al., 2016), however, user's intention whether or not to use mobile device security technologies is not only

cognitively governed. For instance, Giwah (2018)'s study leveraged the constructs within the PMT to understand the antecedent factors that contribute to the information security usage of mobile device users in the context of data breach. Giwah found the level of motivation of mobile device users explained 26 percent of actual mobile device security usage. While PMT cognitive components such as the assessments of threats and ways to cope with them help explain how to motivate users to adopt mobile device security behaviors, additional non-cognitive factors have an important influence on users' decisions processes. Similarly, Uffen et al. (2013) examined how behavioral cognitive determinants of the theory of planned behavior (TPB) and the technology acceptance model (TAM) affected the behavioral intention to use mobile device security measures. Uffen found that multiple facets of mobile device user's personalities significantly affected the cognitive factors, which determined the behavioral intention to use mobile device security measures. However, Uffen et al. (2013), as well as Giwah (2018) emphasized that factors that influence actual usage of mobile device security technologies are diverse and depend on the influence of other external variables such as individual differences in personality. Consequently, the authors recommended future studies that are underpinned by behavioral theories to consider mobile device user's personalities in order to deepen the understanding on the information security usage behavior of mobile device users.

The absence of literature on the relationship between cognitive, personality traits factors, mobile device user's intention, and actual usage of mobile device security technologies that are grounded in the behavioral science literature presents an opportunity to add to the body of knowledge on mobile device usage and information security. The

lack or minimal exploration in this area may be attributed to the fact that within the information security context, the human factor is complex to understand and manage because human behavior is unpredictable (Alhogail, Mirza, & Bakry, 2015). The unpredictability of human behavior makes it critical to try to understand mobile user's security behavior because users have become the weakest link, and the focus of information security compromises. Hence, in this dissertation study, the relationship between cognitive factors, personality traits, and the user's intention to use mobile device security technologies were investigated.

Dissertation Goal

The purpose of this study was to determine, with empirical data, the influence of the protection motivation theory and personality traits on mobile device user's intention to use mobile device security technologies. Specifically, the purpose of the research was to determine the effects of the independent variables (IVs) - extroversion, agreeableness, conscientiousness, neuroticism, intellect, perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, and mobile self-efficacy, on the dependent variable – mobile device user's intention, which indicates the behavioral usage of mobile device security technologies. By building on PMT, this study integrated a comprehensive concept that accounts for mobile device user's perceived threats, and their belief in the measures that could be taken to alleviate these threats. The big five factor model (BFFM) theory provides a picture of personality traits in the usage decision and was employed as a complement to the cognitive aspects. The usage of mobile device security technologies was chosen in order to provide a narrow and manageable focus for the study since it is considered an information security risky behavior (Giwah, 2018). To

accomplish this goal, this study used a research model and subsequent hypotheses based on the relationships between the constructs used. The research model combined both cognitive PMT factors and BFFM personality traits to explain mobile device user's intentions to adopt mobile device security technologies.

The rationale for leveraging the PMT was its potential to provide a theoretical explanation on the cognitive processes individuals undergo when faced with threats (Crossler, Andoh-Baidoob, & Menard, 2018; Rogers, 1983). These processes motivate users to engage in either adaptive or maladaptive responses. Adaptive behaviors are suggested responses that are deemed effective at protecting the individual against a threat (Rogers, 1975). In contrast, maladaptive responses are any variety of behaviors in which the individual fails to enact the recommended response (Rippetoe & Rogers, 1987). Information security behavior and decisions of mobile device users are based on cognitive and decisions heuristics (Almuhimedi et al., 2015). Consequently, cognitive factors influence user's information security behavior and their compliance or noncompliant decisions (Tsohou, Karyda, & Kokolakis, 2015; Uffen et al., 2013). Hence, the PMT constructs adapted for the development of the research model used in this study have perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, and mobile self-efficacy as determinants of intention which directly influence the adoption of mobile device security technologies. However, mobile device security usage is not only cognitively governed. Therefore, this study sought to place a stronger emphasis on the personality factors to explain mobile user's intention to adopt mobile device security technologies.

One emerging area of interest in applying behavioral science theories to understanding user security behaviors has to do with personality traits. A study conducted by Shropshire et al. (2015), in which a sample ($n = 170$) was drawn from a population of undergraduate college students, found that attitudinal constructs and two personality traits (conscientiousness and agreeableness) confirmed evidence of behavior toward, and intent to adopt, information security measures. Shropshire et al. (2015) recommended that new research should be conducted with a larger sample and for the sample to be made up of a more comprehensive range of varied users from within a wider range of institutions. Also, Shropshire et al. recommended that the role of all personality traits should be explored to further understand user information security behaviors. As they relate to information technology and information security, mobile device security behaviors have been described in terms of a wide range of actions that include activities such as creating secure passwords, biometric protection, following routinely data backup, email policies, software updates, mobile application activities, and protecting access to electronic files, among others (Giwah, 2018; Hayden, 2010; Herath & Rao, 2009, Shropshire et al., 2015; Whitty, 2015). Shropshire et al. (2015) recommended that these types of behaviors could be evaluated to further understand the relationships between user's security behaviors and user's intent to adopt information security measures. Following the recommendations of the Shropshire et al. (2015) study, for the present study the sample was composed of a broader spectrum of users from diverse organizations within the United States (U.S.).

The research model used for this study is presented in Figure 1. The PMT constructs (*perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, and mobile self-efficacy*) and the five broad dimensions of

personality traits (*intellect, agreeableness, conscientiousness, extroversion, and neuroticism*), which were the independent variables (IVs), and mobile device user's intention, as evidenced by their attitude toward adopting mobile device security technologies to protect their data, was investigated. The mobile device user's intention to adopt mobile device security technologies was the dependent variable. While studies have made excellent progress in predicting behavioral intentions, this study measured actual security behaviors. The mobile device user's adoption of security technologies to protect their data is labeled "*Mobile Device Security Usage*", which indicates the actual usage of mobile device security measures. The goal of the study was to contribute to the body of knowledge on mobile device security and to provide conclusions that are useful for understanding the mobile device user's information security behaviors. An additional goal of this study was to provide insight on mobile device user behavior in relation to the adoption of information security measures.

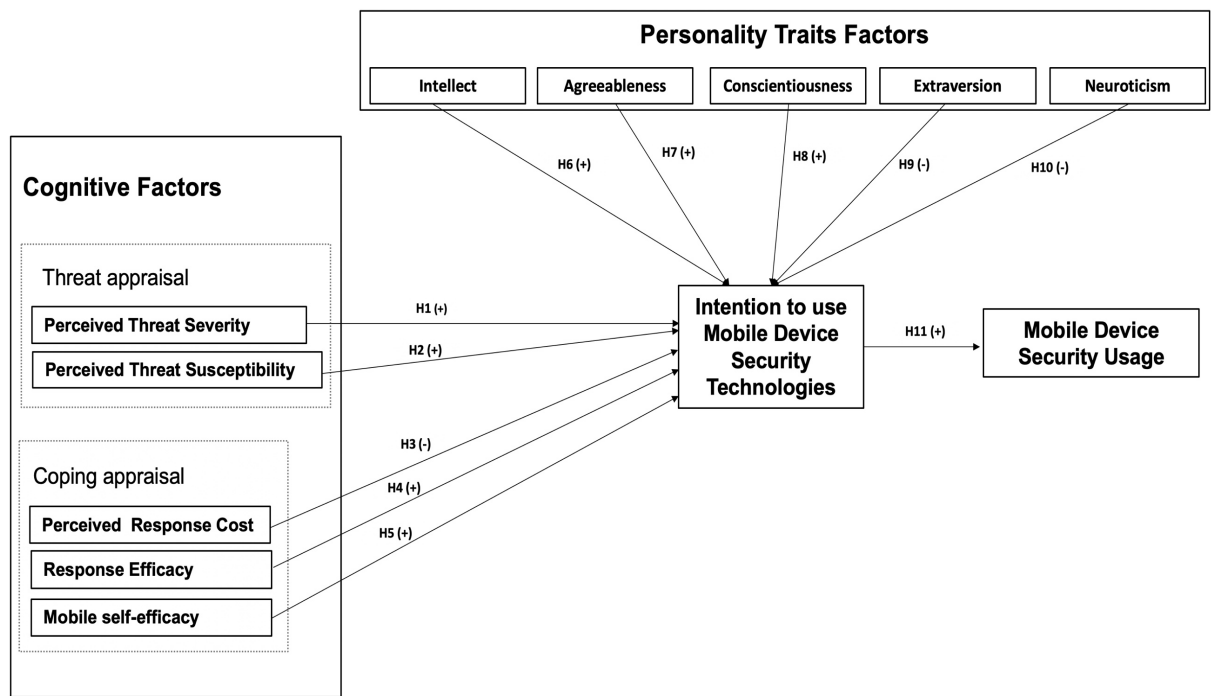


Figure 1: Research Model

Research Questions

The main question that guided this research was: To what extent do cognitive factors and personality traits influence the usage of mobile device security technologies? By applying the research model, the main question was broken down into three distinct research questions. The first research question incorporated the PMT predictors of behavior in the form of perceived threat severity, perceived threat susceptibility, perceived response costs, response efficiency, and mobile self-efficacy that shape behavioral intention, which leads to mobile device security usage (Giwah, 2018; Rogers, 1975; Rogers, 1983). The second research question incorporated the five personality traits constructs. These sets of constructs constituted the five dimensions of the BFFM personality traits theory which includes extraversion, agreeableness, conscientiousness, neuroticism, and intellect (Goldberg, 1993; McCrae & Costa, 1997). While prior research has made excellent progress in predicting behavioral security intentions (Visinescu, Olajumoke, Sherry, Yu, & Dan, 2016; Warkentin, Walden, Johnston, & Straub, 2016), the third research question aimed at measuring actual mobile device security usage. Based on these defined constructs, the research questions that drove the study are as follows:

Research Question 1 (RQ1)

Does perceived threat severity, perceived threat susceptibility, perceived response costs, response efficiency, and mobile self-efficacy influence mobile device user's intention to use mobile device security technologies?

Research Question 2 (RQ2)

Does intellect, agreeableness, conscientiousness, extroversion, and neuroticism influence mobile device user's intention to use mobile device security technologies?

Research Question 3 (RQ3)

Does mobile device user's intention influence mobile device security usage?

Relevance and Significance

This study is of significance to organizations across industries and has the potential to contribute to the emerging behavioral field of personality traits and information security studies. This study is of value to organizations because the use of personal mobile devices has been increasing among employees in the workplace. As a result, more organizations are becoming increasingly concerned about the risk of breaches to information security that these devices represent (Bernroider et al., 2014; Uffen et al., 2013; Xu et al., 2016). Researchers have argued that user behaviors are associated with as many as 95% of organization's internal information security incidents (Carlton & Levy, 2015). Moreover, mobile device user behaviors have been reported to be a contributing factor to data breaches (Leach, 2003; Ovelgönne et al., 2017). Since the aggregate cost of data breaches to organizations have been in the billions of dollars each year (Leszczyna, 2013; Levy, Ramin, & Hackney, 2013), this study may help organizations understand how mobile device security behavior might be explained by their personality traits. Consequently, organizational leaders and decision-makers might use this information to plan strategies to shape internal security policies.

Furthermore, while studies (Harris, Patten, & Regan, 2013; Koohang, Floyd, Rigole, Paliszkiwicz, 2018; Ratchford & Wang, 2019) have recommended technology

awareness practices that focus on ensuring that employees understand mobile device security, it is still a challenge to identify what exactly will get users to really observe and practice them (Johnston, Warkentin, & Siponen, 2015). According to Rizvi, Labrador, Hernandez, and Karpinski (2016), relying heavily on technology alone, such as firewalls, mobile device management software, and intrusion detection systems will not stop security breaches. To have a practical security plan, an organization must use a combination of technology while also dealing with the risk of human error. This study contributes to the body of knowledge by integrating both cognitive factors and personality traits as antecedents of mobile device user's intention to use mobile device security usage.

Since this study showed that personality traits and cognitive factors explained mobile device user's information security behavior, mobile device manufacturers such as Samsung, Apple, or Huawei could use this information to form unique strategies to influence mobile device user behaviors. According to McNeil and Fleeson (2006), although personality traits have been described as stable, they can change through intervention such as role-play. For instance, mobile device manufacturers could develop role-play games as part of their data breach reduction and privacy strategies for consumers.

This study has relevance to the field of information security and has the potential to extend cross-discipline value to the behavioral sciences as well. This study contributes to, and expands on, the very thin body of literature on how users of mobile devices should behave to ensure the security of their data, as well as personality traits and cognitive factors as explainers of mobile device user's information security behaviors.

Barriers and Issues

There were several barriers to overcome in conducting this research. One barrier was the ability to reach a sizeable number of participants for the survey. This study employed SurveyMonkey.com, a web-based survey to reach the participants. There were several benefits of conducting a web-based survey over traditional approaches. One advantage of web-based survey research is the ability to provide access to groups and individuals who would be difficult, if not impossible, to reach through other channels (Garton, Haythornthwaite, & Wellman, 1999). For the purpose of this research, it enabled the participation of mobile device users in different locations in the United States. Web-based surveys also tend to be more interactive and engaging, easier to complete, and less intrusive than traditional phone or mail surveys (Heiervang & Goodman, 2010).

Although the web-based survey was anonymous, due to the inclusion of the human subjects, another barrier was the requirement for Institutional Review Board (IRB) approval. Prior to conducting this research, the IRB confirmed the confidentiality of the information and compliance with institutional protocols. The last barrier that this research faced was the response rate. To overcome this barrier, this research followed up with the participants two weeks after the initial email invitation, reminding them of the study, and inviting those who had not completed the survey yet to do so.

Assumptions

Several assumptions were established for this research. First, it was assumed that the intended sample participants provided an accurate representation of the larger population of mobile device users in the United States. A second assumption was that the participants answered honestly and to their best ability the survey questions. Lastly, this

study assumed that each participant in the survey has used mobile devices for a considerable period of time.

Limitations

There are several limitations facing this research. One limitation may be insufficient identifiable personality traits from the sample group of mobile device users. Thus, an inadequate representation of the remaining mobile device user population may affect the overall generalizability of the research. Another possible limitation is the accuracy in sample responses due to the large size and number of items on the survey questionnaire. Lastly, Web-based surveys are susceptible to self-selection bias, which arises when prospective respondents decide entirely for themselves to participate in the survey. According to Bethlehem (2010), it is difficult to estimate the impact of any selection bias because information on non-participants is usually not available, and comparisons between the included and the excluded samples are not feasible. Nevertheless, this impacts the generalization of the research in terms of the entire population.

Delimitations

One delimitation of this study was the possibility that participants might not be familiar with mobile device security technologies. For this study, the population consisted of mobile device users who are technologically savvy as well as those who are not. Hence, it was possible that the participants were not familiar with the concept of mobile device security technologies. To address this issue, the first section of the web-based survey questionnaire presented participants with a brief explanation of what mobile

device security technologies are, along with some of the benefits of using this technology.

Definition of Terms

The following terms were used in the study and were defined in the literature as follows:

Construct - Characteristic or attribute that can be measured or observed, and that varies among the people or organization being studied (Creswell, 2008).

Construct Items - research questions presented to survey respondents to measure or study a construct (Monroe, 2000).

Information Security - Process to assure the confidentiality, integrity, and availability of information (Bishop, 2003).

Information Systems (IS) - An integrated group of processes within a user-computer environment which operate on structured data and are designed to facilitate the informational needs for management and functioning of the organization (Torres-Perez & March-Chorda, 2002).

Mobile Devices - This term refers to smartphones, tablets and other cell phones that can be used to process information (Leavitt, 2013). Computer desktop and laptops are out of the scope of this study.

Agreeableness - agreeableness is a tendency to be compassionate and cooperative, rather than suspicious and antagonistic towards others (Toegel & Barsoux, 2012). Most agreeable people are very trusting and trustworthy and are willing to volunteer information without a second thought (Rothmann & Coetzer, 2003).

Conscientiousness – conscientiousness is a tendency to pay attention to details (Toegel & Barsoux, 2012). The conscientiousness factor of the personality traits is made up of individuals who are known to be efficient, well disciplined, and regimented in their behaviors (Goldberg, 1992).

Extraversion – extraversion is a tendency to enjoy being the center of attention. It indicates how outgoing and social a person is (Toegel & Barsoux, 2012). Extraverts have the ability to influence others, since they are very sociable individuals with the tendency to encourage their peers (McCrae & Costa, 1997).

Neuroticism – neuroticism is a tendency to get stressed out easily (McCrae & Costa, 1997). “The polar opposite of neuroticism is emotional stability” (Goldberg, 1993, p.3). Individuals who are neurotic will see mundane circumstances and trivial annoyances as challenges (Norris, Larsen, & Cacioppo, 2007).

Intellect – intellect is a tendency to be open to new ideas and quick to understand things (McCrae & Costa, 1997). Alternately, the intellect trait is described as openness (Goldberg, 1993, p.3). Intellectual individuals are open to learning and experiencing new ideas (Toegel & Barsoux, 2012).

Threat Severity – Perceived seriousness of the consequences of a particular threat (Rogers, 1975). In terms of this research study, perceived severity was defined as the perceived seriousness of the consequences of falling victim to a mobile device security threat.

Threat Vulnerability – refers to the perception of the likelihood of a threat occurring (Rogers, 1975). In this research study, perceived vulnerability was defined as the perceived likelihood of becoming a victim of a mobile device security threat.

Response Costs - refers to any “inconvenience, expense, unpleasantness, difficulty, complexity, side effects, disruption of daily life, and overcoming habit strength” (Rogers, 1983, p. 169) that an individual perceives they could incur through performing the recommended protective behaviors against a threat. Response costs, in this study, was defined as any costs perceived to be incurred by the adoption of protective behaviors against a mobile device security threat.

Response Efficacy- refers to the belief that a particular recommended action will be effective in reducing a threat (Rogers, 1975). In this research study, response efficacy was defined as the belief that recommended behaviors will be effective in mitigating a mobile device security threat.

Mobile Self-efficacy – refers to a mobile device user’s belief in their own ability to accomplish the threat mitigation action recommended (Giwah, 2018). In this study, mobile self-efficacy was defined as an individual’s belief in their own ability to perform the recommended behaviors to protect against a mobile device threat.

Summary

The pervasiveness of mobile devices and their growing importance for private and business use have created unique challenges for information security research. Although mobile devices usage has numerous benefits, its connectivity to the internet also brings many security threats to its users (Xu et al., 2016). To protect against these security threats, it is important that mobile device users follow the intent to adopt secure technologies with actual usage behavior. Mobile device users are still considered to be the weakest link in defense against the existing information security as their actual

security behavior differ from the intended behavior (Han et al., 2008; Shropshire et al., 2015; Uffen et al., 2013).

This chapter presented the background that inspired this research study as well as an explanation of the theoretical underpinnings of the conceptual model. The research problem that this study addressed was the need for understanding the factors responsible for the adoption and usage of mobile device security technologies. The problem statement was followed by the identification of the overall research goal, and the three research questions that guided it. Also included in this chapter was a description of each of the research constructs derived from the PMT and big five personality traits model, and how each were conceptually applied to the research framework. Lastly, the initial challenges in the form of barriers, delimitation, limitations, and assumptions linked to this research were discussed.

Chapter 2

Review of the Literature

Overview

Electronic crimes in the U.S. caused a reported damage of 2.7 billion dollars in 2018 (FBI Internet Crime Report, 2018). These crimes were not limited to computers, but also extended to mobile devices. It has been noted that, as of January 2019, 95% of adults in the U.S. were using a mobile device, while 77% of those were using a smartphone device (Pew Research Center, 2019). With the rapid adoption of mobile devices for personal and work-related use in the workplace through programs such as bring your own device (BYOD), there has been an increase in risk to information security breaches (Bernroider et al., 2014; Uffen et al., 2013; Xu et al., 2016). Organizations have traditionally turned to technological solutions to manage information security breaches (Pfleeger & Caputo, 2012); however, the consistent conclusions that have been reported in the literature are that most data security breaches stem from both deliberate and accidental human behavior (Chen, X., Chen, L., & Wu, 2016; Ovelgönne et al., 2017; Patnayakuni, N., Patnayakuni, R., & Gupta, 2016). Intended user behavior in information security, however, is a complex area of research and cannot easily be predicted.

The research problem that this study addressed is the lack of understanding of whether the user's intention to use mobile device security technologies can be explained by their cognitive factors and personality traits. The lack of understanding in this area of information security (IS) presented an opportunity to conduct the present research.

According to Levy and Ellis (2006), an effective literature review should analyze and synthesize quality literature, provide a firm foundation to a research topic and methodology, and identify contributions of a proposed study. Following the recommendations of Levy and Ellis, this literature review synthesized both historical and recent literature related to PMT cognitive factors, personality traits, and mobile device security usage. Also, this review provided an understanding of the theories on which this study was built and discussed the factors at play in the IS behavior of mobile device users.

Theoretical Foundation

Protection Motivation Theory (PMT) (Rogers, 1975; Rogers, 1983), as a framework, postulates that the motivation to protect oneself from danger is related to the subject's cognitive belief on the following aspects: the severity of the threat, the susceptibility of the threat, the effectiveness of coping response in preventing the threat, the cost of response, and the ability to execute the coping response. According to Floyd, Prentice-Dunn, and Rogers (2000), "the protection motivation concept involves any threat for which there is an effective recommended response that can be carried out by an individual" (p. 409). When facing a specific threat, individuals seek either to get rid of the unpleasant feeling evoked by a threat or to come to grips with the situation (Johnston & Warkentin, 2010). If a certain fear threshold level fails to be reached, there is no motivation to take any action (Johnston, Warkentin, & Siponen, 2015). Building on expectancy-value theory, Rogers (1975; 1983) elaborated that two cognitive processes, threat appraisal and coping appraisal, determine individuals' protection motivation, which in previous research was considered the most immediate predictor of behaviors

(Burns, Posey, Roberts, & Lowry, 2017; Giwah, 2018; Matt & Peckelsen, 2016; Posey, Roberts, & Lowry, 2015).

Personality traits refer to a stable set of characteristics that determine the differences in individuals' thoughts, feeling, and actions (Goldberg, 1992). Due to its importance for human cognition and behavior, researchers have integrated a large number of personality traits to assess personality differences within the IS domain; however, there is now considerable agreement in the literature that personality can be represented by five constructs (Briggs, 1992; Matt & Peckelsen, 2016), all of which have been integrated into the Big Five-Factor Model (BFFM). Barrick, Mount, and Judge (2001) along with Shropshire et al. (2015) pointed out that BFFM is considered the most parsimonious model and useful taxonomy in personality research, and it enables researchers to cover individuals' personalities broadly and systematically.

The BFFM clusters all personality traits into five constructs: conscientiousness, extraversion, neuroticism, intellect, and agreeableness (Matt & Peckelsen, 2016). The rationale for leveraging these personality traits is its potential to explain differences between human beings and how certain measurable traits exhibited by those human beings can be used to understand and guide mobile device security behavior. The integration of personality also leads to substantially better model explanatory power, thus confirming that personality traits directly influence user's intention to use mobile device security technologies. The application of personality traits in the literature often use TAM or the Unified Theory of Acceptance and Use of Technology (UTAUT) models; however, it has been found that models that are based on the theory of planned behavior often fail to consider perception of risk adequately (Conner & Abraham, 2001; Matt &

Peckelsen, 2016). By contrast, PMT enables researchers to predict user's perceptions of the risk and threats inherent to mobile device security behavior.

Grounded in the PMT and BFFM conceptual foundations, this study's research model combined both cognitive factors and personality traits to explain intentions to use mobile device security technologies (Figure 1). By building on PMT, this study integrated a comprehensive concept that accounts for user's perceived threats of mobile device data breaches and their belief in the measures that could be taken to alleviate these threats. In addition, the personality traits provided a picture of the individual differences that are germane in the usage decision.

Hypotheses

Threat Severity

Herath and Rao (2009) defined threat severity as the "degree of harm associated with a threat" (p. 111). This definition is in line with an earlier definition by Witte and Allen (2000) that threat severity is the "magnitude of harm expected from the threat" (p. 529). Warkentin et al. (2016), in a recent study on fear appeals, suggested that users, when facing a specific threat, will seek either to get rid of the unpleasant feelings evoked by the threat or to cope with the situation. As explained by Burns et al. (2017) in their research on how to influence users to engage in protective security actions, they posited that a high level of perceived threat severity motivated users to take measures to protect themselves. In line with this tendency, previous researchers have asserted that users who received stronger messages about a threat's severity exhibited a higher motivation to engage in adaptive responsive actions (Posey et al., 2015; Tu et al., 2015). Adaptive response is explained by Vance, Siponen, and Pahnla (2012) as the positive response

appraised from the cognitively mediating process in individuals when they perceive a threat. The positive effect of perceived threat severity on behavioral intention has been widely supported in the literature (Alsaleh, Alomar, & Alarifi, 2017; Crossler et al., 2018; Lee & Larsen, 2009; Woon, Tan, & Low, 2005). For instance, Woon et al. (2005)'s study explored the cognitive psychological factors that influence the decision of home wireless network users to implement security features on their wireless networks. The results of the study conducted by Woon et al. found that perceived threat severity was a significant factor in determining if a user running a home wireless network will enable security measures. Crossler et al. (2018), also in a study on how culture and uncertainty avoidance affected individual's threat and coping appraisal, suggested that high level of severity drives users to behave in a secure manner in order to reduce or get rid of the threat. However, other studies examining the role of perceived threat severity in the IT security domain have found a negative relationship between threat severity and security policy compliance. For example, Mwangwabi, McGill, and Dixon (2018), while investigating how perceptions about passwords and security threats affected compliance with password guidelines, found that neither susceptibility to a security attack nor severity of an attack influenced password guideline compliance. While previous studies have concluded that threat severity was an important predictor of security-related protection, other studies have found that perceived threat severity was not a significant predictor of behavioral intention. This highlights the need for more research around this domain to understand how factors such as threat severity may influence intentions and the usage of mobile device security technologies. Based on this argument and the positive association between threat severity and intention, the below hypothesis was developed:

H1: Perceived severity positively influences the intention to use mobile device security technologies.

Threat Susceptibility

Witte and Allen (2000) defined threat susceptibility as the “degree to which one feels at risk for experiencing the threat” (p. 592). According to Thompson, McGill, and Wang (2017) threat susceptibility refers to the degree to which someone feels vulnerable to a particular threat. Behavioral economics have shown that when faced with uncertainty, users evaluate probabilistic outcomes differently, depending on their personal reference points (Lawson, 1985). Similarly, when users perceive there is a high chance of being susceptible to security threats, they tend to assess how it can be mitigated (Herath & Rao, 2009). However, perceived occurrences of a specific threat vary, subject to individual differences (Matt & Peckelsen, 2016). Dang-Pham and Pittayachawan (2015) advocated the view that users are motivated to protect themselves if they perceive susceptibility to the threats. The perception of being vulnerable to threats decreases the user’s intention to perform maladaptive behaviors (Menard, Warkentin, & Lowry, 2018). Maladaptive responses are undesired behaviors intended only to decrease fear, but not the danger posed by the threat (Rippetoe & Rogers 1987). Gutteling, Terpstra, and Kerstholt (2017) suggested that when users perceive high threat susceptibility, they are motivated to undertake adaptive responses that will protect them from the threat. This assertion was supported by Johnston and Warkentin (2010), as well as Vance et al. (2012); both studies emphasized that higher perceived threat susceptibility led to a positive impact on adopting recommended responses. Nevertheless, there have been less consistent findings about its impact on mobile security behavior. For example, Thompson et al. (2017) found

a positive influence of threat vulnerability on security behavior based on 629 home computer and mobile device users, while previously Crossler's (2010) study found that perceived susceptibility unexpectedly had a negative influence on security behavior. Moreover, neither Zhang and McDowell (2009) nor Tsai et al. (2016) observed any effect. Despite the mixed previous findings in the context of mobile devices, Posey et al. (2015) suggested threat susceptibility to be a "major component in the threat appraisal process and overall formation of insiders' protection motivation" (p. 14). It is evident that there is a need for more research on how perceived threat susceptibility influences mobile device user's intention to adopt mobile device security technologies. Based on this background, the below hypothesis was developed:

H2: Perceived susceptibility positively influences the intention to use mobile device security technologies.

In addition to the two threat appeal components, this study included three coping resources to obtain a more comprehensive picture of the antecedents of user's intention to use mobile device security technologies. Perceived response cost, response efficacy, and mobile self-efficacy form the coping appraisal component of the research model.

Response Cost

Fry and Prentice-Dunn (2005) defined response cost as the "social, physical, and monetary expenses of performing the recommended response" (p. 288). However, response costs refer to not only financial cost, but also to any time, effort or inconvenience that the user may associate with the protective behavior (Thompson, McGill, & Wang, 2017). In terms of this study, this would be the cost incurred by the mobile device user to adopt the mobile security technologies. Furthermore, the revised

PMT (Rogers, 1983; Rogers & Prentice-Dunn, 1997) described response costs as a negative influence on the intentions to perform protective behaviors. Therefore, as the response costs to perform protective behaviors increase, the intentions to perform these behaviors should decrease. Previous studies have confirmed the negative relationship between response costs and the intentions to perform protective behaviors against security threats. For instance, Chenoweth, Minch, and Gattiker (2009), as well as Liang and Xue (2010), found a negative relationship between response costs and the intention to use anti-spyware software. Similarly, Marett and Ratnamalala (2012) found a negative relationship between response costs and the intention to use personal firewalls. According to Crossler and Belanger (2014), response cost drives users toward maladaptive responses, and as noted by Posey et al. (2015), it reduces the desire of users to adopt protective behaviors. In addition, Rogers (1975) posited that if the response cost of performing a behavior is high, then it will hinder the performance of adaptive responses. Based on this argument and the noted negative association between response cost and intention to perform protective behaviors against security threat, the below hypothesis was developed:

H3: Response cost negatively influences the intention to use mobile device security technologies.

Response Efficacy

According to Posey et al. (2015), “response efficacy is the perception that the recommended coping strategies can successfully attenuate the threat” (p. 15). The two PMT efficacy factors self-efficacy and response efficacy are cognitive processes that are stimulated when users are faced with a threat, with the aim of motivating users to engage

in behaviors that can help to minimize the threat (Doane, Boothe, Pearson, & Kelley, 2016). Rogers (1975) in the seminal study that originated the PMT described response efficacy as the degree to which a person is convinced that a proposed response will effectively prevent a threat. In terms of this study, this would be the user's belief in a technology's effectiveness in mitigating the mobile device threat to which the user is exposed.

Posey et al. (2015) argued that response efficacy plays a more significant role in forming protection motivation than the threat appraisal components. PMT proposes that response efficacy directly influences the intention to perform protective behaviors such that as an individual's response efficacy increases, their intention to perform protective behaviors should also increase. Several studies have shown that response efficacy is positively related to the intention to perform protective behaviors against security threats (Arachchilage & Love, 2013; Boehmer, Larose, Rifon, Alhabash, & Cotten, 2015; Posey et al., 2015). For instance, Boss et al. (2015) found moderate to high levels of response efficacy were positively associated with the intentions to use anti-malware software. Giwah (2018) also found a positive relationship between response efficacy and protection motivation in the context of data breaches. The findings of the research studies presented suggest that an increase in a user's response efficacy for the recommended protective behaviors against mobile device security threats would result in an increase in their intention to use mobile device security technologies.

Although many studies have found response efficacy had a significant positive influence on IS intentions in different contexts (Doane et al., 2016; Ifinedo, 2012; Lwin, Li, & Ang, 2012; Tsai et al., 2016), there have been cases where the positive influence of

response efficacy was not supported (Thompson et al., 2017; Vance et al., 2012). This highlights the need for more research around this domain to understand how factors such as perceived response efficacy may influence intentions and the usage of mobile device security technologies. Therefore, the following hypothesis was developed:

H4: Response efficacy positively influences the intention to use mobile device security technologies.

Mobile Self-Efficacy

Grounded in social cognitive theory, Bandura (1986) defined self-efficacy as the “people’s judgments of their capabilities to organize and execute courses of action required to attain designated types of performances” (p. 391). As such, it relates to judgments of what individuals can do with the skills they possess and is not focused on the actual skill itself. While self-efficacy has demonstrated remarkable success in predicting behavior, Bandura argued that self-efficacy, determined by measures linked to a specific domain, has a stronger predictive capability than using general measures. Clarke (2010), citing Compeau and Higgins (1995), also emphasized that self-efficacy as a construct must be developed to reflect the context within which it is used. Thus, contextualizing the self-efficacy construct into “mobile self-efficacy” presents a more rigorous approach to understanding the adoption behavior of mobile device users.

Prior studies have found self-efficacy (Agarwal, Sambamurthy, & Stair, 2000; Crossler et al., 2014; Siponen, Mahmood, & Pahlila, 2014; Thompson et al., 2017; Vance et al., 2012), as well as mobile self-efficacy (Giwah, 2018; Keith, Babb, Lowry, Furner, & Abdullat, 2015), to be the strongest predictor of IS behavioral intentions. However, there have been a few cases where the positive influence of self-efficacy on

security intentions was not supported (Tsai et al., 2016). Posey et al. (2015) emphasized that self-efficacy is a highly significant factor of protection motivation, and the best measure of behavioral intention. A previous study conducted by Johnston and Warkentin (2010) also found self-efficacy to have a significant positive impact on behavioral intention. PMT proposes that self-efficacy positively influences the intention to perform protective behaviors. Therefore, as an individual's self-efficacy increases, so should their intention to perform protective behaviors. Based on this argument and the noted positive association between self-efficacy and intention to perform protective behaviors, the below hypothesis was developed:

H5: Mobile self-efficacy positively influences the intention to use mobile device security technologies.

Intellect

The intellect factor of personality traits is one that expresses "imagination, curiosity, and creativity" (Goldberg, 1993, p. 27). Individuals who score high on intellect are characterized by a broader and deeper scope of awareness and a higher need to examine experiences (McCrae & Terracciano, 2005), which leads to a higher willingness to try new and different things. According to Xu et al. (2016), users high on the intellect trait are more likely to become innovators and early adopters of new technologies and services than other personality traits. For example, mobile device users who scored high on the intellect trait were early adopters of social media and short messaging applications in the beginning of the online social networking era (Butt & Phillips, 2008; Correa et al., 2010). Given that mobile device security technologies are still niche products (Matt & Peckelsen, 2016), an intellectually inclined individual should have a higher interest in

adopting mobile device security technologies. An individual who scores high on the personality trait intellect is always willing to increase their knowledge and constantly look for new ventures in which to participate (Turiano et al., 2013). As a result, mobile device users who are open to the continuously changing landscape of IS would be highly open to use mobile device security technologies. Based on this argument and the noted positive association between intellect and intention to use mobile security technologies, the below hypothesis was developed:

H6: Intellect positively influences the intention to use mobile device security technologies.

Agreeableness

Agreeableness is a personality trait that takes into consideration how kind, cooperative, and dependable an individual is (Costa & McCrae, 2013). Individuals who possess this trait often enjoy team participation and are seen as kind and generous (John, Robins & Pervin, 2008). In the context of IS, research has shown that the agreeableness trait directly influences the intention to adopt protective behaviors. For instance, in a study exploring personality traits and intention to adopt a web-based security software program, it was found that high agreeableness was positively related to the intention and actual use of the security software (Shropshire et al., 2015). It has also been suggested that users who score high on the agreeableness trait show interest in the security of their own information, as well as the security issues affecting other individuals (Judge et al., 1999; Korzaan & Boswell, 2008; Rothmann & Coetzer, 2003). Furthermore, a study conducted by Farhadi, Fatimah, Nasir, and Shahrazad (2012) on the relationship between personality traits and deviant work behavior found that agreeable individuals were less

likely to be involved in deviant work behavior. This finding is consistent with Mount, Ilies, and Johnson (2006) as well as, Salgado (2002), who agreed there is a negative relationship between agreeableness and deviant behavior. According to Matt and Peckelsen (2016), an agreeable individual is more likely to follow the rules even if their behavior is not monitored. Thus, an agreeable individual is considered more likely to follow IS policies and be aware of the impact a compromised system will have on the organizations' resources. Based on this argument and the noted positive association between agreeableness and intention to use mobile security technologies, the below hypothesis was developed:

H7: Agreeableness positively influences the intention to use mobile device security technologies.

Conscientiousness

The conscientiousness factor of the personality traits is made up of individuals who are known to be efficient, reliable, and well-organized (Toegel & Barsoux, 2012). McCrae and Costa (1997) noted that people showing a high score for conscientiousness would be the type to "pay attention to details" (p. 49). Additional traits that describe conscientious individuals are responsible, proficient, achievement striving, accountable, disciplined, dutiful, and adept (Costa & McCrae, 1992; Goldberg, 1990). Previous studies revealed conscientious individuals are likely to take control of and protect their personal information, since they tend to be aware of the dangers associated with security breaches (Korzaan & Boswell, 2008; McComarc et al., 2017; Milne, Labrecque & Cromer, 2009). For instance, Pattinson et al. (2015) examined the relationship between non-malicious computer-based behavior and personality traits, as well as experience, age, and

familiarity with computers. Pattinson et al. suggested conscientious individuals were less prone to risky computer-based behaviors. This conclusion was also supported by Shropshire et al. (2015), who found a significant positive association between the conscientious personality trait and security intentions. Shropshire et al. also suggested that conscientious individuals tend to stick to established procedures and experience discomfort when deviating from familiar paths. Further, they are less willing to get involved in risky situations and will initiate efforts to protect themselves from potential threats (Matt & Peckelsen, 2016). Consequently, mobile device users who possess the conscientiousness trait would be highly open to use mobile device security technologies in order to protect themselves against potential threats. Based on this argument and the noted positive association between conscientiousness and intention to use mobile security technologies, the below hypothesis was developed:

H8: Conscientiousness positively influences the intention to use mobile device security technologies.

Extraversion

Individuals that exhibit the extraversion personality trait are described as outgoing, social, self-assured, and enthusiastic (Toegel & Barsoux, 2012). These individuals enjoy being “the center of attention” (McCrae & Costa, 1997, p. 49). Extraversion is a trait that has been linked to those who are inclined to take control of situations and portray a leadership role in situations where warranted (Korzaan & Boswell, 2008). They enjoy being around people, part of social gatherings, and work gatherings (Ilies & Dimotakis, 2015; Judge et al., 2017). However, research has found that individuals who are high on extraversion were more likely to violate cybersecurity

polices in comparison to more conscientious individuals (Hadlington, 2017; McBride et al., 2012; Shropshire et al., 2006). Since extroverted individuals tend to be more involved in opportunities to provide and obtain information in specific situations, they see IS polices as a barrier that prevents the exchange of information. Extroverted individuals also tend to live an action-oriented life that includes taking high risks (Uebelacker & Quiel, 2014; Welk et al., 2015). This suggests that extroverted individuals who score high on extraversion will be less likely to initiate the usage of mobile device security technologies. Based on this argument and the noted negative association between extraversion and intention to use mobile security technologies, the below hypothesis was developed:

H9: Extraversion negatively influences the intention to use mobile device security technologies.

Neuroticism

Neuroticism is related to emotional instability and characterized by attributes such as anxiety, anger, hostility, depression, self-consciousness, impulsiveness, and vulnerability (Costa & McCrae, 1992). Individuals high on neuroticism tend to develop negative emotions when meeting any change (Terzis, Moridis, & Economides, 2012). It is also reported that individuals of this sort regard using new technologies as a complicated and stressful process (Terzis et al., 2012) and avoid using them (Rosen & Kluemper, 2008). In addition, prior studies have demonstrated that one of the facets of neuroticism, anxiety, is negatively related to computer self-efficacy (Compeau & Higgins, 1995) and behavioral control (Uffen et al., 2013), which in turn reduced user's intention to adopt new technologies. Since neurotic individuals are more likely to be

stressful, fearful, and feel threatened by change (Camadan, Reisoglu, Ursavas, & Mcilroy, 2018; Lattuch & Young, 2011) they are less likely to accept the need for continued education towards mobile security than an emotionally stable person.

Furthermore, individuals who reveal neuroticism traits tend to score lower on the attitude toward cyber security behavior (Cox, 2012). The distrust inherent in neurotic individuals makes them more likely to regard security measures with skepticism, hence forming negative attitudes because of the belief that a potential action cannot make a significant difference in protecting their mobile device (Uffen et al., 2013). Based on this argument and the noted negative association between neuroticism and intention to use mobile security technologies, the below hypothesis was developed:

H10: Neuroticism negatively influences the intention to use mobile device security technologies.

Intention

Previous security studies based on the PMT have made excellent progress in predicting user's intentions based on models that used behavioral intention as a representation for actual behavior (Shropshire et al., 2015; Tsai et al., 2016; Tu & Yuan, 2015); however, literature suggests that users do not always act in accordance with their behavioral intention (Ajzen, Brown, & Carvajal, 2004; Bernroider et al., 2014; Boss et al., 2015). While studies have extended the PMT by including actual security behaviors, the models have found weak relationships between the intention to perform security behaviors and actual security behaviors. For instance, a study conducted by Giwah (2018) that examined the factors influencing the usage of mobile device security technologies found the level of intention explained 26 percent of actual mobile device security usage.

Similarly, Thompson, McGill, and Wang (2017) found the level of intention to adopt mobile device safe behaviors explained 22 percent of actual mobile security behavior. According to Matt and Peckelsen (2016), the low explanatory ability of PMT studies to explain actual security behavior might be due to additional non-cognitive factors that have an important influence on the user's decision processes. This suggests that using non-cognitive factors such as personality traits might help obtain greater explanatory ability to predict actual mobile device user security behaviors.

Another explanation for why users may not act on their intentions and follow through with actual behavior is that the relationship between intentions and actual behavior is contingent on whether the behavior is a single or multi-action behavior (Sheeran, 2002). According to Verkijika (2018), the relationship between intentions and actual behavior is stronger for single action behaviors. However, since IS behaviors are mostly composed of multiple actions, it is important for researchers to include the actual security behaviors in their studies to avoid wrong conclusions (Siponen et al., 2014; Siponen et al., 2015). There is ample evidence in the literature (Belanger & Crossler, 2019; Tu & Yuang, 2012; Venkatesh et al., 2003; Verkijika, 2018; Xu et al., 2016) that supports the significant positive association between security intentions and actual security behavior. Therefore, this study hypothesized that:

H11: Mobile device security intentions positively influence the actual usage of mobile device security technologies.

Mobile Device Security

Significant focus has been placed on the deployment of mobile device security protection technologies such as firewalls, mobile device management (MDM), intrusion

prevention systems (IPS), as well as passwords and encryption systems in organizations (Tu & Yuan, 2015). It has, however, been suggested that, regardless of the technical security components used, it is the behavior of the users that will result in effective system protection (Alohali, Clarke, Furnell, & Albakri, 2017; Giwah, 2018; Matt & Peckelsen, 2016; Uffen et al., 2013). Allowing personal data to coexist with sensitive business data on a personal mobile device that is largely outside the control of the organization introduces substantial risks to data security.

According to Goode, Hoehle, Venkatesh, and Brown (2017), data breaches occur when there is a disruption in service due to an unauthorized release of data or access to sensitive information by external entity. Lowry et al. (2015) suggested that most data breaches are the result of deliberate user actions, negligence, or accidental incidents. Furthermore, a significant number of companies' data breaches were caused by the use of mobile devices (Weiss & Miller, 2015). Although mobile devices allow users to be flexible and work remotely, they can also create issues with data security which was the focus of this study.

According to Romer (2014), data security breaches from mobile devices could be a non-issue if users monitor what applications they install on their devices. Similarly, Steiner (2014) proposed the use of authentication tokens as a data security solution. However, researchers have shown that mobile device security solutions that revolve around hardware and software alone are deemed ineffective (Alohali et al., 2017; Crossler & Belanger, 2014; Gharehchopogh, Rezaei, & Maleki, 2013; Ratchford & Wang, 2019). Moreover, O'Neill (2014) and Tu et al. (2015) pointed out that mobile device security solutions should focus on the human behavior of mobile device users

rather than on the technical issues. The security challenges of mobile devices are complex and the simple reason that they get lost and are stolen more often than computers make the effort to protect them from data breaches more challenging. While the number of stolen or lost mobile devices has augmented rapidly over the last few years, some of these devices may be used as a vehicle to spoof the real identity of the attacker (Dagon, Martin, & Starner, 2014). This may be performed by taking advantage of the sensitive personal information stored in the mobile device corresponding to its legitimate user. Another study revealed that one in four college students did not have a passcode to prevent access to their device and only half of them had software installed to wipe personal data if their mobile device was lost or stolen (Harris et al., 2013). Additionally, Das and Khan (2016) noted that besides the possibility of losing mobile devices and the data they carry, mobile device users expose themselves to risks of breach by connecting their devices to insecure and vulnerable wi-fi public networks.

As pointed out by Tu et al. (2015), mobile devices present unique security risks that can lead to data breaches, which explains the need for users to take special measures to reduce or prevent them. The minimal exploration in this area may be attributed to the suggestion made by Alhogail et al. (2015) that within the IS context, the human factor is complex to understand and manage because human behavior is unpredictable. Nevertheless, the necessity for such a study has become more relevant as vulnerabilities resulting from user behavior have become more commonly associated with security incidents.

Past Literature and Identification of Gaps

Previous IS studies have made excellent progress in predicting user's security intentions; however, most studies lack an explicit inclusion of actual security usage as the dependent construct in their models. Its minimal use in previous information systems research focusing on security behaviors has created a gap in the literature and a lack of understanding. In exploring the actual adoption of mobile device security technologies as a dependent construct to explain mobile device user security behaviors, this study adds to the body of knowledge on mobile device use and IS behaviors.

According to Burns et al. (2017), PMT studies have used behavioral intention as a proxy for actual security behavior. Burns pointed out many studies are derived from Ajzen's (1985) theory of planned behavior, which has behavioral intention as the primary driver of observed actual behavior. But while behavioral intentions are generally well correlated with security behaviors, as revealed by Boss et al. (2015), relatively few studies have investigated the actual user's security behavior. A review of the literature suggests that intentions result in behavior only about half of the time (Webb & Sheeran, 2016). This is a limitation of the studies that have used PMT as an explanatory model to predict security behavior. For example, Crossler and Belanger (2014) used the PMT components in their study to explain differences in security practices among home users. Crossler and Belanger found that perceived threat severity positively influenced user's intention, while perceived threat susceptibility was negative, and response cost had no strong relation with user's intention. However, it is worth pointing out that these findings did not consider actual user's security behavior towards the rapidly changing technological landscape and security risks. Contrary to the findings in the study by

Crossler and Belanger (2014), Menard et al. (2018)'s study found that threat severity and threat susceptibility did not have a significant influence on user's behavioral intention when considering psychological ownership and culture. As such, the universality of the positive influence of the constructs of the PMT has been questioned due to the lack of clarity (Tsai et al., 2016). According to Thompson et al. (2017), future studies should look beyond security intentions to actual behavior. Thus, further understanding of actual user behaviors in the mobile device security domain is required. The research model provides a framework to do so, and this study examined actual security behavior for mobile device use, and possible individual differences in personalities were explored.

While research has established that cognitive ability is a critical factor in IS behavior (Giwah, 2018; Thompson et al., 2017), this alone is not sufficient to fully explain user differences in actual usage of mobile device security technologies. For instance, Giwah (2018) confirmed the PMT's capacity to predict user behavior based on threat and coping appraisals within the context of mobile device security usage; however, Giwah's research model only explained 26 percent of actual behavior. Similarly, Thompson, McGill, and Wang (2017)'s PMT model, which examined the factors that influence mobile device security behavior, explained only 22 percent of the actual behavior of mobile device users. Both studies recognized the potential importance of additional external behavioral factors that are outside PMT and suggested future research should use other established factors, such as personality traits. With the wide adoption of mobile devices, researchers started to investigate the impact of personality on general internet usage. For example, McElroy et al. (2007)'s study directly tested the effect of personality and cognitive factors on internet usage. McElroy reported that personality

explained more variances in user's internet usage and online selling behavior than cognitive factors. Similarly, other researchers (Gratian et al., 2018; Matt & Peckelsen, 2016; Shropshire et al., 2015; Uffen et al., 2013) have argued that personality has the potential to explain even more variance of actual behavior, thus providing helpful insights into user behaviors. According to Matt and Peckelsen (2016), the integration of personality traits and PMT in a model can lead to substantially better model explanatory power, thus confirming that personalities directly influence user behaviors.

A study conducted by Harris, Furnell, and Patten (2014), which compared the security behavior of college students, noted that the "lack of policy and controls does not represent a problem if usage and behavior with mobile devices are naturally aligned with security and protection" (p. 187). However, the notion that mobile device users are aligned with security practices is far from reality. Contrary to the findings reported by Harris et al. (2014), Tu et al. (2015) argued that users do not naturally exhibit responsible security behaviors but tend to leverage technology countermeasures. Another study that evaluated the factors that influence mobile device user's behavior found that users make tradeoffs when weighing different security behaviors and may not always make optimal security-related choices (Jeske, Briggs, & Coventry, 2016). Furthermore, Mylonas, Kastania and Gritzalis (2013) suggested complacency and disregard for responsible IS behavior as traits exhibited by most mobile device users. It is evident that there are gaps in the literature on mobile device security behavior. Uffen et al. (2013), as well as Wang, Duon, and Chen (2016), pointed out that further research is needed on user security behaviors and its applicability on mobile devices. Hadlington (2017) pointed out that efforts to understand user security behaviors should consider behavior and shift the focus

of the research away from technical issues. Additionally, Giwah (2018) noted that there is the need for more research into the factors that can influence the human factors in the information systems and security area. Reviewing the existing literature, there is ample evidence of the need for further research and an opportunity for future research to build on the findings from this study.

Analysis of the Research Methods Used

Previous work related to mobile device security behavior that was reviewed for the purpose of this research used an array of research methods and designs. Quantitative research methods including surveys and experimental designs, as well as qualitative research methods such as interviews and case studies have been leveraged. From the prior studies reviewed, survey and experimental research designs were the most widely used methods in behavioral informational security research. For example, Posey et al. (2015) in their study on the impact of organizational commitment on user's behavior, used a survey of 380 participants. Another study conducted by Crossler and Belanger (2014) used an online and paper-based survey with 324 participants to develop a unified security practice instrument. Additionally, Gratian (2018) in their correlational study between personality and security behavior intentions, used a web-based survey to collect data from 369 participants. Similarly, Verkijika (2018)'s study on security adoption behavior used a web-based survey to collect data from 385 participants.

Construct, content, and discriminant validity were established in almost each of the studies reviewed. Few studies also conducted a partial least square (PLS) analysis to test their structural models, constructs validity, and associated hypothesis. Both descriptive and inferential statistics were used to analyze the results and draw

conclusions. According to Wyllys (1978), descriptive statistics include both measures of central tendency and measures of variability, while inferential statistics are techniques that allow researchers to use samples to make generalizations about the populations. The studies reviewed also included tests such as Cronbach's alpha, good-fit, and regression analysis to further strengthen the validity and reliability of their results. Lastly, most of the studies used the cross-sectional, instead of longitudinal method, signifying that there was no need of collecting data at different points in time.

Synthesis of the Literature

The purpose of the PMT is to clarify the cognitive processes which mediate IS user behavior in the face of a threat (Rogers, 1975, 1983). PMT suggests that, when facing a threatening event, users conduct two appraisal processes which are the threat appraisal and coping appraisal (Boss et al., 2015). These appraisals affect user's intention to take the precautionary action and result in adaptive or maladaptive behaviors (Alohali et al., 2017). This study leveraged the PMT to explain mobile device user's cognitive need to act and their assessment of the recommended course of action they could take. However, a mobile device user's decision whether or not to adopt mobile device security technologies is not only cognitively governed (Belanger & Crossler, 2019; Matt & Peckelsen, 2016; Shropshire et al., 2015; Uffen et al., 2013). Therefore, this study did not only use the existing constructs from the PMT theory but extended it by adding well-established personality factors related to mobile device security usage.

While PMT has been applied to IS user's behavior (Boss et al., 2015; Crossler & Belanger, 2014; Dang-Pham & Pittayachawan, 2015; Giwah, 2018), few studies have used actual behavior as the dependent variable (Giwah, 2018; Matt & Peckelsen, 2016;

Thompson et al., 2017) in their models. A review of the literature suggests that measuring intention rather than actual behaviors can be troublesome as intention does not always lead to actual behavior (Webb & Sheeran, 2016). According to Shropshire et al. (2015), it is common for mobile device users, despite knowing that their personal data is at risk, to fail to act on their intentions to adopt mobile device security behaviors. Mobile device users, even with having the intention to adopt mobile device security technologies, are still considered to be the weakest link as their actual security behavior may differ from the intended behavior (Belanger & Crossler, 2019; Gratian et al., 2018; Johnston et al., 2015).

As the IS literature shows, there have been previous studies conducted on IS user behavior, but there is a lack of research that focuses on actual usage of mobile device security technologies by determining the effects of perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, intellect, extroversion, agreeableness, conscientiousness, and neuroticism. Continuous efforts must be made to understand the IS behavior of mobile device users in order to recommend strategies that will direct them in their efforts to protect their personal data (Posey et al., 2015). While the foundation for this study was based on previous PMT work in the area of IS behavior, it extends their findings by integrating actual usage behavior and personality factors, which can lead to substantially better model explanatory power.

Summary

The main contribution of this study is the advancement of current research in mobile device security, thereby adding to the body of knowledge regarding IS user's

behavior through the PMT and personality constructs. Results from this study also provide information that could influence or support future strategies aimed at security mobile devices while addressing the need for further examination of IS user behavior with respect to mobile device security (Giwah, 2018; Shropshire et al., 2015; Uffen et al., 2013). Insights in future strategies for implementing mobile device security will benefit organizations, mobile device manufacturers, and those involved in the development of IS policies and procedures.

The literature review in this study examined the behavior of mobile device users and the implication toward IS. The literature review suggested that to achieve protection from unwilling or unintentional leakage of personal data via mobile devices, which can have negative consequences for both individuals and organizations, we must encourage users to use proper protective technologies on their mobile devices. Prior IS literature generally confirmed that additional research is needed to identify factors that influence mobile device users to engage in actual security behavior (Boss et al., 2015; Giwah, 2018; Verkijika, 2018; Warkentin et al., 2016). With the foregoing in mind, this study brought new insights to the existing body of knowledge as it attempted to understand the factors at play in the IS behavior of mobile device users through the lens of PMT and personality traits.

Chapter 3

Methodology

Research Design

This study utilized a quantitative post-positivist approach to assess the relationship between a set of independent variables (IVs) and a dependent variable (DV). The IVs include the personality traits intellect, extroversion, agreeableness, conscientiousness, and neuroticism, as well as the Protection Motivation Theory (PMT) cognitive factors perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, and mobile self-efficacy. The DV is the mobile device user's intention, which influences the actual usage of mobile device security technologies variable. The theoretical framework upon which the study rests is the PMT and the Big Five Factors Model (BFFM) of personality traits theory, which were leveraged to explain the DV with statistical significance. According to Aliaga and Gunderson (2000), using a quantitative approach allows researchers to explain a particular phenomenon by collecting numerical data that are analyzed using mathematically based methods. A quantitative design was suited to the present research because it allowed for the collection of numerical data to be statistically analyzed to test the hypotheses involving the above-mentioned variables.

This study was guided by a post-positivist research philosophy, which embraced many of the tenets of the positivist worldview. Post-positivist philosophy accepts that there is one objective, values free, reality separate from individual perceptions, which can

be objectively known, measured, and understood (Kuhn, 1996; Sharma, 2013). Positivist philosophy, when adopted, gives findings that are based on objective reality rather than just mere opinions or intuition (Burns, 2000). This study, in a broad perspective, aimed at revealing not only a relationship, but also predicting the impact of the IVs on the mobile device user's security behavior.

There were three phases in this study. In phase one, the survey instrument was developed based on validated measures from prior research, and an expert review process that followed the Delphi technique. In phase two, the survey instrument was used in a pilot test to examine its usability and identify potential problems with the study. Phase three was the main data collection of the measures that addressed the research questions, including data analysis and interpretation. Since human subjects were used in this study, approval was required from the IRB before the data was collected. Appendix B shows the IRB approval letter. Figure 2 shows the study's methodology.

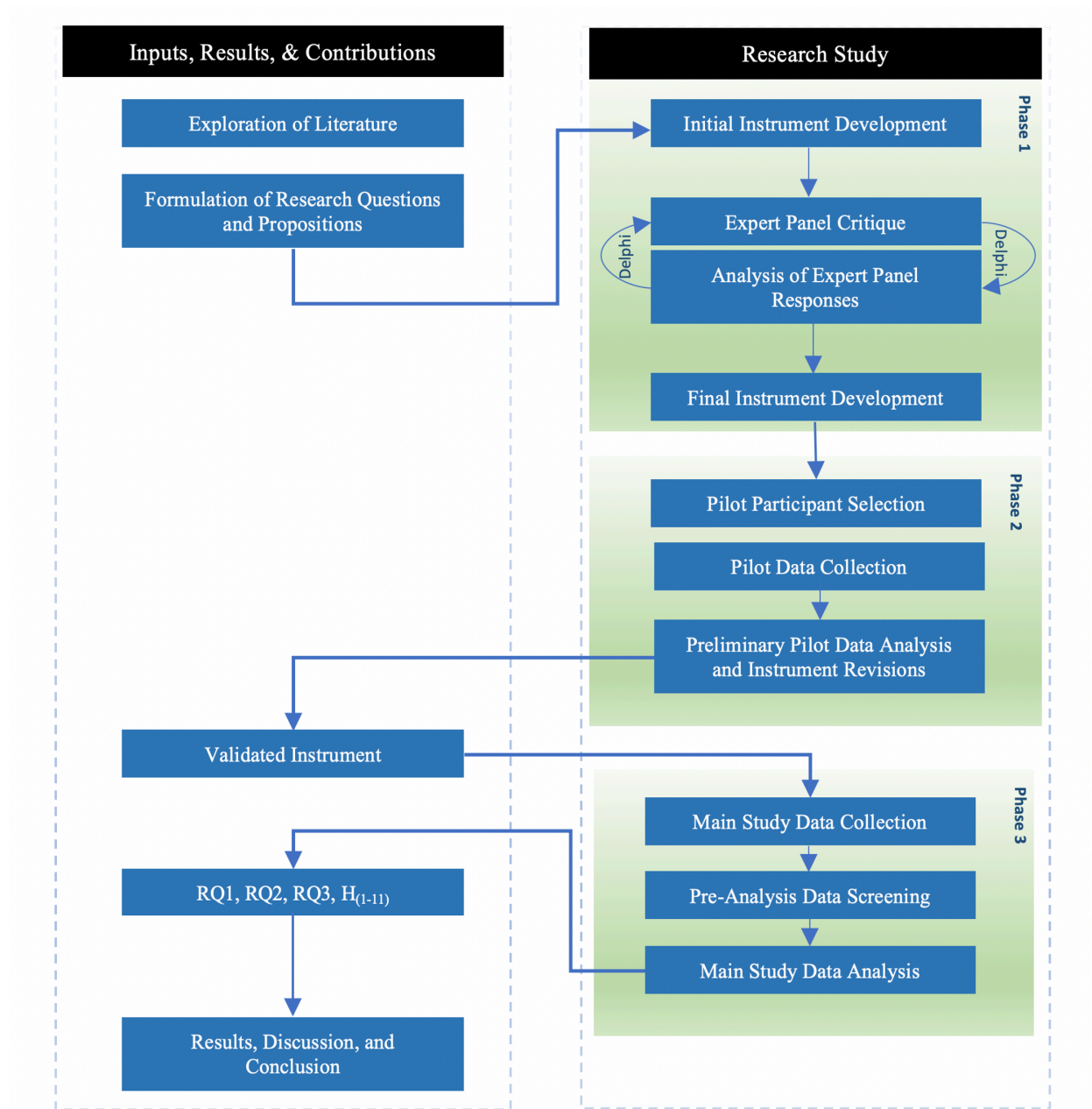


Figure 2: Study Methodology

Instrument Development and Validation

The survey instrument for this study was developed from validated, previously established, and well-accepted instruments. According to Saunders, Lewis, and Thornhill (2003), adopting items is more efficient than developing items yourself only as it enables you to gather the appropriate data needed to meet the demands of the study. A web-based

survey was appropriate for the present study since it enabled the collection of a large sample size which helped the researcher in testing the research hypotheses and the generalization of the results (Samani, 2016). This method of data collection can also significantly minimize issues relating to the accuracy of the data (Bachmann & Elfrink, 1996; Cooper & Schindler, 2006), as data captured from the survey was automatically transferred by the system into an electronic file, thereby eliminating the potential for human errors. Furthermore, a large number of people's views were needed, which made this method ideal due to its ability to reach thousands of people with common characteristics in a short amount of time, despite possibly being separated by great geographic distances (Cobanoglu, Moreo, & Warde, 2001; Yun & Trumbo, 2000).

For this study, the survey instrument measured twelve constructs and included six demographic control indicators. All the survey items were measured using a Likert-type scale, as using such a scale yields better results because it allows more accurate variability (Cicchetti, Shoinralter, & Tyrer, 1985). The level of measurement for all constructs was interval. Although the survey employed the Likert scale, which leans more towards an ordinal level of measurement, response wording ensured equal distance between the response options. To be precise, for this study, a 5-point multi-item Likert-style scale was used to collect data on the five factors of personality traits, which are extraversion, agreeableness, conscientiousness, neuroticism, and intellect, and a 7-point rating scale was used on the PMT factors, which are threat severity, threat susceptibility, response costs, response efficacy, mobile self-efficacy, mobile device user's intention, and mobile device security usage.

For this study, a Cronbach's alpha of 0.7 or more was considered an acceptable significant level of reliability. According to Gay, Mills, and Airasian (2009), the Cronbach's alpha (α) is the most widely used index for determining the reliability of measurement instruments and this statistic indicates whether the items on a scale are measuring the same construct. This numerical coefficient of reliability ranges from 0 to 1.0; however, a Cronbach's alpha of 0.7 or more is considered an acceptable significant level of reliability (Gefen, Straub, and Boudreau, 2000). Rovai, Baker, and Ponton (2013) further explained that a factor loading below 0.5 is regarded as a low Cronbach's alpha coefficient, while ranges of 0.50 and 0.70, and above 0.70 are considered high coefficients.

The International Personality Item Pool (IPIP) 50-item questionnaire instrument is one of the most frequently used measures of personality traits and its reliability and validity has been established in the seminal and contemporary literatures (Bowling & Burns, 2010; Goldberg, 1993; Holden, Dennie, & Hicks, 2013; McAbee & Oswald, 2013). The instrument is composed of five sub-scales, each of which is composed of 10 items or questions (50 items in total) that measure each of the five factors of personality traits.

Responses to the 50-item questionnaire instrument were measured on scales that range from 1 to 5, with 1 = disagree, 2 = slightly disagree, 3 = neutral, 4 = slightly agree, and 5 = agree. Then, a reliability calculation was performed to determine the psychometric quality of the 50-Item IPIP questionnaire instrument. Results of the reliability calculations for the present study are provided in Chapter 4; however, the IPIP questionnaire has very good psychometric properties (Original Cronbach's $\alpha = 0.84$),

which makes the instrument a reliable and valid instrument. Table 1 summarizes the reliability of the instrument in the original study conducted by Goldberg (1993).

Table 1
Original Study 50-item IPIP Instrument Reliability

Description	Original Cronbach's α
Extraversion	$\alpha = 0.87$
Agreeableness	$\alpha = 0.82$
Conscientiousness	$\alpha = 0.79$
Emotional Stability	$\alpha = 0.86$
Intellect	$\alpha = 0.84$
Overall Scale Reliability	$\alpha = 0.84$

The survey also included the following PMT constructs for the purpose of this study: perceived threat severity, perceived threat susceptibility, perceived response costs, response efficacy, mobile self-efficacy, and mobile device security usage. This study adopted the survey items developed by Giwah (2018) in order to measure these constructs. Giwah conducted the Cronbach alpha test and found all items returned a Cronbach's alpha of 0.7 or more, which indicated the instrument is reliable. Table 2 summarizes the reliability of the instrument in the study conducted by Giwah (2018).

Table 2
Giwah (2018)'s Study Instrument Reliability

Description	Original Cronbach's α
Mobile Device Security Usage	$\alpha = 0.75$
Mobile Self-Efficacy	$\alpha = 0.91$

Description	Original Cronbach's α
Perceived Response Cost	$\alpha = 0.93$
Perceived Threat Severity	$\alpha = 0.93$
Perceived Threat Susceptibility	$\alpha = 0.74$
Response Efficacy	$\alpha = 0.75$
Overall Scale Reliability	$\alpha = 0.84$

Giawah (2018)'s instrument reliability test was supported by previous studies. For example, the items for measuring perceived threat severity and susceptibility were adopted from Claar and Johnson (2012), where the reliability test had a Cronbach's alpha of 0.91 for severity and for 0.92 susceptibility. To measure perceived response cost, items were adopted from Boss et al. (2015) and Woon et al. (2005), which showed a 0.84 Cronbach's alpha. The response efficacy scale was adopted from Boss et al. (2015) and Johnston and Warkentin (2010). The reliability measure of the adapted items was a Cronbach's alpha of 0.89 (Boss et al., 2015; Johnston & Warkentin, 2010). Lastly, the items to measure mobile self-efficacy and mobile device security usage were adopted from Claar and Johnson (2012), based on a Cronbach's alpha of 0.94 and 0.92, respectively.

The survey items for measuring the intention to use mobile device security technologies were adopted from Uffen et al. (2013) as well as Shropshire et al. (2015)'s instruments. Both studies reported a consistency reliability test greater than 0.70 Cronbach's alpha. As previously shown, the items for the purpose of this study have very good psychometric properties (average Cronbach alpha = 0.84), which makes the

instrument a reliable and valid instrument. The items that were used for all the constructs being investigated in this study can be found in Appendix A.

As recommended by Straub (1989), all the constructs included items from prior research for validity purposes. However, to capture all the constructs, the survey instrument combined items from various studies. Creswell (2014) indicated that when an instrument is modified, or if different instruments are combined into a single study, the original reliability and validity may not hold true for the new instrument. Therefore, it becomes vital that reliability and validity be re-established during data analysis (Creswell, 2014). Since this study combined instruments from various studies, an expert panel following the Delphi technique and a pilot test were conducted to re-establish reliability and validity of the final instrument. The purpose of the first developed instrument was to obtain responses from the expert panel, with the aim of assessing the content validity of the identified measures. The responses from the expert panel were then used to revise the instrument. Following the revisions, the instrument was used in a pilot test to collect the quantitative data on the IVs and DV.

Expert Panel

Straub (1989) indicated that it was important to show that instruments that were developed were actually measuring what they were designed to measure, and this could be done through literature reviews, pre-testing, and expert panels. As part of validating the content of the survey instrument, this study followed the Delphi technique to elicit response from an expert panel. According to Skulmoski, Hartman, and Krahn (2007), a Delphi study is an “interactive process to collect and distill the anonymous judgments of experts using a series of data collection and analysis techniques interspersed with

feedback” (p. 1). Characterized as an iterative group communication process, the Delphi technique ensures both reliability and validity as it exposes the study to a panel of differing, and often contradictory, opinions while seeking convergence through experts’ feedback (Carlton & Levy, 2015). Key features that are regarded as the Delphi technique include secrecy, iteration, controlled feedback, and statistically clustering the responses (Okoli & Pawlowski, 2004; Rowe & Wright, 1999). This study will maintain the secrecy by using web-based questionnaires. Also, between each questionnaire, feedback will be controlled by incorporating the experts’ responses into the next questionnaire.

According to Gray and Hovav (2014), experts are qualified professionals knowledgeable in a particular discipline and have adequate experience to speak with authority on matters of that discipline. This study employed subject matter experts (SMEs) familiar with mobile device security technologies. The SMEs will be tasked with reviewing, validating, and recommending adjustments to the items of each construct. Based on Sumsion (1998)’s recommendation, an agreement between 70% or more among the SMEs will be considered a consensus.

Pilot Test

After the consensus and adjustments were made following the feedback from the expert panel, and prior to the main data collection, the final survey instrument was used in a pilot test to examine its usability. A pilot test is a trial before the main study is done; therefore, it administers the exact procedures that will be used in the main study to a small group of participants similar to those who will be used in the main study, and is very useful in refining the survey questions (Dane, 2011; Zikmund, 2013). Furthermore, a pilot test can enhance the content validity of a survey instrument as well as help to

improve the questions, the format, and the scales that are used (Creswell, 2014; Rea & Parker, 2014). Beck and Liao (2014) also suggested that conducting a pilot study supports other tests of validity by helping simplify survey items that are complex. Researchers have suggested a pilot study sample should include at a minimum of 10 to 30 participants (Isaac & Michael, 1995; Julious, 2005; Van belle, 2002). Therefore, the pilot study for this dissertation included 20 participants to ensure the survey instrument is reliable.

Instrument Validity and Reliability

A valid instrument is one that actually measures what needs to be measured, while a reliable instrument is one that measures the same thing more than once and produces the same outcomes (Salkind, 2012). Salkind (2012) further stated that validity and reliability were the first line of defense that a researcher had against making erroneous conclusions. In fact, “if the instrument fails, then everything else down the line fails as well” (Salkind, 2012, p. 115). The importance of instrument validation has also been emphasized in subsequent studies which indicated that in the absence of instrument validation, the findings and interpretations of studies lacked rigor and were not trustworthy (Boudreau, Gefen, & Straub, 2001; Straub, Boudreau, & Gefen, 2004). According to Straub (1989), the validity of the data and measurement may be improved through pilot tests. Hence, this study used a pilot test to minimize the threats to reliability and validity of the survey instrument. Two types of validation that can be used for the trustworthiness of the research results are content and construct validation (Brown, 1996; Salkind, 2012; Straub, 1989).

Samani (2016) defined content validity as “the degree in which a questionnaire’s content covers the extent and depth of the topics it was intended to cover” (p.56). Content validity ensures the questions within the survey are within the scope of the concept being studied (Zikmund, Babin, Carr, & Griffin, 2013). Content validity is important because it eliminates items that are irrelevant to answering the research questions (Diamantopoulos & Winklhofer, 2001). Content validity can be established through literature reviews, an expert panel, and pilot tests (Boudreau, Gefen, & Straub, 2001; Creswell, 2002; Straub, 1989). This study will use all three recommended techniques to establish both content and construct validity.

Construct validity, together with convergent and discriminant validity, assess the degree to which a measurement is represented and logically concerned (Samani, 2016). Construct validity refers to the degree in which a test measures an intended hypothetical construct (Kumar, 2010). For establishing the construct validity, this study conducted a confirmatory factor analysis on the items and constructs. Convergent validity is defined as “the degree to which concepts that should be related theoretically are interrelated in reality.” (Trochim & Donnelly, 2008, p. 68). According to Campbell and Fiske (1959), the convergent validity of the measurement model can also be assessed by the Average Variance Extracted (AVE) and Composite Reliability (CR). AVE refers to the ability of a construct to explain the variance in its reflective measurement items. It is recommended that AVE values calculated should be at least 0.5 to indicate that at least half of the variance of an item has been influenced by the construct itself (Hair, Hult, Ringle, & Sarstedt, 2014). CR is an indication of a measurement item’s total contribution to the construct it has been attributed to. According to Hair et al. (2014), loadings should be

statistically significant and have a value of at least 0.708. In contrast, discriminant validity refers to a construct existing as a separate and unique construct in itself and not having facets that could be characterized by any other construct in the PLS path model (Henseler, Ringle & Sarstedt, 2015). One method for determining discriminant validity is by using the Fornell-Larckner criterion to determine that the square root of a construct's AVE is larger than the correlation it has to any of the other constructs. If this criterion is met, it will indicate that a construct shares more variance with its own measurement items than it does with any other construct (Hair et al., 2014).

Internal Validity

According to Leedy and Ormrod (2005), internal validity of a research study is the “extent to which its design and the data that it yield allow the researcher to draw accurate conclusions about cause-and-effect and other relationship within the data” (p.103-104). Internal validity can refer to both the instrument used and the design of the study (Creswell, 2012; Sekaran & Bougie, 2013). Threats to internal validity of the survey instrument have been previously addressed. However, threats to internal validity regarding the design of the study includes history, maturation, regression, selection, mortality, testing, and instrumentation (Creswell, 2012; Sekaran & Bougie, 2013). The first five threats relate to the participants of the study, while the latter two relate to the procedures of the study (Creswell, 2012).

History and maturation threats involve uncontrollable changes during the length of the study that could influence the outcome, such as the study being conducted over a long period of time and the participants changing during the course of the study (Creswell, 2012). This study addressed these threats by collecting data for the study over

a short period and by using participants who are 18 years old or older. Regression and selection threats involves researcher bias for the selection of the participants (Creswell, 2012; Sekaran & Bougie, 2013). Random selection of participants has been recommended to increase internal validity and reduce sampling bias (Creswell, 2012; Sekaran & Bougie, 2013). Therefore, this study shared the survey via various methods to ensure that everyone in the target group had an equal chance of receiving an invite to respond to the survey. Mortality refers to the possibility of participants dropping out over the period of the study (Creswell, 2012; Sekaran & Bougie, 2013). Mortality was a threat to this study in two ways: experts from the expert panel could drop out during the Delphi process, and participants, who could drop out from the survey for any number of reasons. Since this study did not expect that 100% participation would be maintained over the period of the study, in order to account for mortality, at least 30 experts and over 1000 mobile device users were initially invited to participate in the study. Testing refers to when participants are exposed to a pre-test that can influence a post-test, in that the participants would become familiar with the outcomes measures during the pre-test and remember the responses for the post-test (Creswell, 2012; Sekaran & Bougie, 2013). This threat only occurs in experimental and quasi-experimental research designs; therefore, it was not a threat for this study. Instrumentation refers to a change in the measuring instrument over time (Creswell, 2012; Sekaran & Bougie, 2013). This study used the same measuring instrument throughout the entire period of the study.

External Validity

The extent to which the results of a study and the conclusions made can be generalized to other settings, people, or events is referred to as external validity (Ellis &

Levy, 2009; Leedy & Ormond, 2005; Sekaran & Bougie, 2013). Lynch (1982) more forcefully made the argument that if the findings supporting one's theory lack external validity, the theory lacks construct validity. Hair et al. (1998) suggested 15 to 20 observations for each variable for the results of a study to be generalizable. To demonstrate external validity, this study reached out to over 1000 mobile device users. Additionally, six demographic indicators were collected to ensure that the data collected was a good representative of the sample and population that the conclusions were drawn on (Compeau, Marcolin, Kelley, & Higgins, 2012).

Ethical Considerations

The Institutional Review Board (IRB) at Nova Southeastern University was contacted to obtain approval prior to the study being conducted. The researcher designed the web-based survey in an ethical manner, and one that accords with the IRB requirements and standards for the collection and handling of personal identifiable data. It was made clear to the participants in the survey that their participation was voluntary, and that all information collected was used only for the purposes of this study. Additionally, the survey assured participants of their anonymity and data confidentiality. Since the survey instrument required the participation of human subjects, the instrument was reviewed and approved by Nova Southeastern University's Institutional Review Board (IRB) prior to beginning the study. The approval letter is included in Appendix B.

Population and Sample

The population of interest for this study was individual mobile device users within the United States (US). A prerequisite for participation was that the potential participants use mobile devices regularly in their daily lives. Furthermore, anonymous demographic

data, such as age, gender, years of using mobile devices, years of using the internet, years of working in a corporate or formal organization, and level of education, was collected. According to Terrell (2012), collecting this type of data assists in identifying the characteristics of the participants.

The sample frame for the research was the individual mobile device user from the target population. The study of the individual unit of analysis was ideal because of the overall goal of this dissertation, which is to establish the mobile device security adoption of users. Sekaran and Bougie (2013) defined the individual unit of analysis as “treating each employee’s response as an individual data source” (p. 104). According to Cappelleri, Darlington, and Trochim (1994), Cohen (1992)’s statistical power analysis is one of the most popular approaches in the behavioral sciences in calculating the required sampling size. Cohen (1992)’s formula is recommended when the number of independent variables used in the path model is known. This study’s path model has a maximum of ten indicators. At a statistical power of 80%, significance level of 0.05, and medium effect size of .30, the resultant sample size based on Cohen’s look-up table for PLS-SEM is 116. This study used this calculated sample size. Lastly, convenience non-probability sampling design was adopted since the individual selection from the population as a sample was not based on any probabilities.

According to Dornyei (2007), convenience sampling is a non-probability sampling technique where subjects of the target population are selected because of their convenient accessibility and proximity to the researcher. The main assumption associated with convenience sampling is that the subjects are homogeneous (Etikan, Musa, & Alkassim, 2016). Specifically, there would be no difference in the research results

obtained from a random sample, or a sample gathered in some inaccessible part of the population. The web-based survey was sent to participants through email, social media platforms, and messaging applications. Also, a follow up message was sent to the participants two weeks after the initial invitation, reminding them of the study, and inviting those who had not completed the survey to do so.

Pre-analysis Data Screening

The very first step before analyzing data was to convert the raw data into a format suitable for decision-making and conclusion. For this study, the quantitative data collected by the web-based survey was pre-analyzed using Statistical Package for Social Sciences (SPSS) for data screening, cleaning, and preliminary analysis. Levy (2006), as well as Mertler and Vannatta (2013), have emphasized the importance of pre-analysis data screening to ensure the accuracy of the collected data before statistical analysis is done. Levy has suggested four main reasons for performing pre-analysis data screening: to ensure the accuracy of the data collected, to deal with the issue of response set, to deal with missing data, and to deal with extreme cases or outliers. Mertler and Vannatta (2013) further pointed out that inaccurate data in research will have direct impacts on the validity of the results and the ability to draw valid conclusions from the collected data. Similarly, Clarke (2010) suggested that inaccurate data will provide invalid results. Nevertheless, a major advantage of using web-based surveys is that since the computer captures the responses, they allow full automation of data entry into analysis programs, which minimizes data entry or transcription errors (Creswell, 2012; Fan & Yang, 2010).

This study conducted the following steps to address each of the four reasons for pre-analysis. Errors that can arise from manually transcribing data from the survey were

eliminated with the use of automatic exporting of the data captured into an electronic file. Additionally, a single valid answer for every survey question was required before submitting all the answers. This eliminated any instances of inaccurate data. It is important that instances of inaccurate data were mitigated, as inaccurate data can significantly affect the validity of the collected data, the conclusions that are drawn from the data, and the ability to generalize the results to a broader population (Clarke, 2010; Levy, 2006; Mertler & Vannatta, 2013).

Response set bias is another factor that produces a particular pattern of responses that lead to invalid conclusions (Mangione, 1995). According to Levy (2006), the response set occurs when participants in a survey select the same score for all the survey items, and this can negatively affect the validity of the results. To address the issue of response set bias, this study adopted the suggestion by Ferdousi and Levy (2010) to conduct a visual inspection of all responses to eliminate items that show 100% of the responses having the same value.

The concern of collecting partial data is another reason for pre-analysis data screening. According to Hair, Black, Babin, and Anderson (2010), the effects of using incomplete data as a result of not performing pre-analysis data screening can provide invalid statistical results. The survey design for this study prevented final submission until all items were answered, thereby eliminating the need to address the concern for missing data. This averted respondents from submitting the survey with questions unanswered.

The final reason for pre-analysis data screening is to deal with extreme cases or outliers. Outliers are extremely high or low values in the dataset that can influence the

outcome of the statistical analysis (Stevens, 2007). According to Mertler and Vannatta (2013), outliers can be detected by calculating the Mahalanobis Distance for each case. Mahalanobis Distance is defined as the distance of a case from the centroid of the remaining cases where the centroid is a point created by the means of all variables (Levy, 2006, p. 152). The Mahalanobis Distance is obtained from the probability density function of multivariate normal distribution (Sun et al., 2000). This study used the Mahalanobis Distance procedure to detect extreme responses, and any identifiable outlier was considered for elimination from the data analysis.

Data Analysis Strategy

Sekaran (2003) suggested that “in the data analysis we have three objectives: getting a feel for the data, testing for goodness of the data, and testing for hypotheses developed for the research” (p. 306). To address these objectives, this study utilized several statistical analyses, including data aggregation and descriptive statistics. In addition, the relationships among the IVs and DV were assessed using path analysis in Partial Least Square - Structural Equations Modeling (PLS-SEM). PLS-SEM is widely used in IS research because of the method’s ability to evaluate the measurement of variables, while also testing cause and effect relationships (Hair et al., 2014). Gefen et al. (2000) also indicated that PLS-SEM is the technique of choice for predictive applications and theory building as it is designed to explain variance, i.e. to assess the significance of relationships and their resulting coefficients of determination or R-squared (R²). The path in analyzing the data includes examining the relationship between INTEL, AGREE, CONS, EXTRA, NEURO, TSE, TSU, RC, RE, and MSE (IVs), their impact on intention (MDUI) to use mobile device security technologies (as the DV), and its impact on actual

mobile device security usage. Path analysis in PLS-SEM, therefore, addresses RQ1 to RQ3. Lastly, data visualization methods not limited to graphs, scatter plots, and scree were used to show irregular structures and variance, respectively (Mertler & Vannatta, 2013).

Format for Presenting Results

The results of the data analysis from the data collected in the main survey are presented to the readers in a format easy to follow. The figures and outputs from the PLS-SEM and SPSS tools used for the data analysis are presented in the results chapter for this report, and the screenshots also added in the appendices. All validity test results, such as the Cronbach's alpha, are presented in table form for easy interpretation. The survey questionnaire used for the data gathering is available in the appendices, as well as the IRB approval letter. This study follows the guidelines for presenting results found in the Nova Southeastern University Dissertation Guide for the College of Engineering and Computing Doctoral students.

Resource Requirements

This study required the following resources: IRB approval given the study involves human subjects, access to mobile device security experts for the expert panel, access to mobile device users, and computer software such as: Word, Excel, PowerPoint, Visio, SPSS[®], and Smart PLS 3.0. The software was required for writing the dissertation report and conducting the various statistical data analysis. An additional resource was the electronic software SurveyMonkey which was used to develop the survey questionnaire and collection of data. Finally, electronic and non-electronic library resources from the Alvin Sherman Library of Nova Southeastern University were used for this study.

Summary

The quantitative research design was used because this methodology was believed to be the most suitable to answer the research questions and test the statistical significance of the hypotheses. For the means of collecting data and based on the deductive approach of this study and a need for a large number of participants, the survey method for data collection was chosen. The survey method was appropriate for this study since it enabled the collection of data from a large sample size which helped in testing the research hypotheses and the generalization of the results (Samani, 2016). Ensuring the validity and reliability of the survey instrument was also important. Therefore, the instrument validation process included validation procedures such as content and construct validity, an expert panel following the Delphi Technique to validate the items that were drawn from literature (Ramim & Lichvar, 2014; Sekaran & Bougie, 2013; Straub, 1989), and a pilot test to identify problems that could arise in the main study (Creswell, 2014; Dane, 2011; Rea & Parker, 2014; Zikmund, 2013).

The main data collection process was followed by the data pre-screening process designed to detect irregularities or problems with the data collected. Next, the statistical methods to analyze the data were detailed. The PLS-SEM statistical methodology was adopted to answer the research questions. The specific population and sample for this study were also discussed. This included the participants for the study and the SMEs for the expert panel. The chapter concluded with the guidelines used for the overall report and resources utilized in completing this study.

Chapter 4

Results

Overview

This chapter contains the data collection, the analysis of responses, and the results of the research study. As previously mentioned, there were three phases in this study, and the results are presented in the order in which each phase was conducted. The survey instrument was developed based on measures from prior research, and further validated using an expert panel following the Delphi technique in phase one. Pilot testing using the web-based survey instrument was conducted in phase two. The main data collection that addressed the research questions, including data analysis and interpretation, was done in phase three.

Phase One - Validation of Survey Instrument with an Expert Panel

The survey instrument for this study was developed to communicate the questions clearly, while at the same time being concise and simple to ensure ease of response (Dolnicar, 2003). According to Straub (1989), all measures should include items from prior research to ensure validity and reliability. Furthermore, Creswell (2014) suggests that instrument validity and reliability be re-established if the instrument is modified, or if different instruments are combined into a single study. As previously mentioned, this study combined instruments from various studies; therefore, an expert review process was used to re-establish the reliability and validity of the survey instrument.

To ensure validity and reliability, an expert panel was asked to review the survey instrument and indicate if the survey covered the full breadth of content, and if each question measured what it was intended to measure. Also, the expert panel was asked for feedback on the presentation, content, clarity, terminology, and usability of the instrument. Direct emails were sent to 20 information systems (IS) experts soliciting participation on the expert panel. The 20 experts included IS faculty members, IS doctoral students, and cyber security professionals in various industries. Of the 20 contacted, 11 responded, a response rate of 55.0%. A link to the web-based survey that included the draft survey instrument was sent to the experts and they provided feedback via comment boxes on each question. This method allowed for the collection of feedback directly into SurveyMonkey, instead of sending feedback back-and-forth via email. The experts' recommendations included the following:

- The addition of the text "I see myself as someone who...." in front of each personality trait item as this makes it easier for the participants to remember (rather than placing it once at the top of the personality trait section).
- The addition of virus and malware definitions to the perceived threat section as these can be confusing terms for participants.
- The removal of one of the demographic questions as it made the survey too long. Also, it was redundant.
- Other minor modifications to the layout of the survey instrument, as well as grammar corrections to some of the survey items to improve clarity.

Overall, the experts' feedback was positive. Based on the recommendations, revisions were made to the survey instrument before it was approved by expert consensus. Subsequent to the expert-review process, a pilot test was conducted using the survey instrument to further improve validity.

Phase Two - Pilot Test

Prior to the main data collection, a pilot study was conducted with 20 participants. The participants were representative of the target demographic population, that is, mobile device users, 18 years or older, who have been using their mobile devices to access the internet for at least one year. Emails soliciting participation were directly sent to neighbors, work colleagues, and friends. Feedback from the pilot test study participants did not result in any changes to the survey instrument, indicating that the questions, their format, and the scales that were used were appropriate for this study, and hence provided content validity.

Phase Three - Main Data Collection Procedures

The main data collection period lasted two months, from February to March 2020. Emails with an attached web-based survey link were sent to the heads (e.g. Executive Director) of the Office of Innovation and Information Technology (OIIT) at Nova Southeastern University. The heads then sent an email blast to all OIIT employees asking them to voluntarily participate in the study. The web-based survey link was also sent to friends, previous employers, and individuals at the researcher's local church. Convenience sampling was used for this study to collect the data through the web-based survey link sent to approximately 1,200 individuals. In addition to emails, the web-based survey link was sent to potential participants using social media platforms (Facebook,

LinkedIn, and Instagram), as well as the WhatsApp messaging application. There were 358 responses received thus meeting the 30% to 40% response rate that was anticipated.

Pre-Analysis Data Screening

Prior to the main data analysis, a pre-analysis data screening was conducted to ensure data accuracy (Levy, 2006). The responses obtained from the web-based survey were downloaded from SurveyMonkey into Microsoft Excel in order to conduct the pre-analysis screening. First, the data was visually inspected for response-set biases where no significant response-set issues were identified. Second, descriptive statistics were used to identify missing values, means, standard deviations, and minimum and maximum values. It should be noted that all questions on the Web-based survey were marked as required to eliminate missing data, and participants had to choose from a standard set of responses. The descriptive statistics confirmed that there were no missing values, all responses were within the specified ranges, and the frequencies were valid. Lastly, outlier detection was conducted using Mahalanobis Distance. Using SPSS analysis, two records were identified as potential multivariate outliers and were considered for elimination. According to Mertler and Reinhart (2017), “the accepted criterion for outliers is a value for Mahalanobis distance that is significant beyond $p < .001$, determined by comparing the obtained value for Mahalanobis distance to the chi-square critical value” (p. 31). After further analysis, the two highest extreme values (Case ID #13 and #224) were eliminated. Therefore, a total of 356 responses were kept for the data analysis.

Test of Assumptions

Six assumptions about the data sets that were evaluated in order to perform path analyses are related to linearity, independence of cases/error terms, multicollinearity,

homoscedasticity, presence of significant outliers, and normality of distribution. Results of the test of assumptions were as follows:

1. *Linearity* was determined by examining a scatterplot of the standardized residuals versus predicted values (Tabachnick & Fidell, 2019). The scatterplot (Appendix C, Figure 3) showed the residuals were scattered randomly and evenly around the regression line, hence, satisfying this assumption.
2. *Independence of cases/errors* was assessed by examining the Durbin-Watson (D-W) statistics test. Independence of residuals or errors is indicated by a Durbin-Watson value that is 2 or close to 2 (Mertler & Vanatta, 2010). Results showed the D-W statistic was 2.275, indicating that this assumption was not violated (Appendix C, Figure 4).
3. *Multicollinearity* exists when two or more of the predictors in a regression model are highly correlated (Mertler & Vanatta, 2010). This condition makes it difficult to understand which variable contributes to the variance explained. The variance inflation factor (VIF) values were examined to determine the absence or presence of multicollinearity. A collinearity problem might exist if the VIF value is greater than 10 (Menard, 1995; Myers, 1990). Results showed each predictor value was below 10, indicating that this assumption was met (Appendix C, Figure 5).
4. *Homoscedasticity* was assessed by examining the scatterplot of the standardized residuals versus predicted values (Tabachnick & Fidell, 2019), which was the same scatterplot used to check for linearity (Appendix C, Figure 3). The data points in the scatterplot do not have an obvious pattern; there are points equally distributed above and below zero on the X axis, and to the left and right of zero on

the Y axis. This pattern indicated that the assumption of homoscedasticity was not violated.

5. *No significant outliers or influential points* was assessed by examining the Cook's distance statistics (Tabachnick & Fidell, 2019), which identifies observations that negatively influence the overall regression model. Results of the Cook's distance values were all below 0.74 (Appendix C, Figure 6). A value greater than 1.0 is cause for concern (Cook, 1977). Therefore, there was no need to remove additional cases after conducting the Mahalanobis distance outlier detection test. This assumption was considered satisfied.
6. *Normality of Distribution* was assessed by inspecting two different graphs: the histogram of the regression standardized residuals, and the normal P-P plot of the expected cumulative probability values versus the observed cumulative probability values (Tabachnick & Fidell, 2019). The histogram (Appendix C, Figure 7) showed the spread of the data formed a bell-shaped curve representing the curve of normality, while the normal P-P plot residuals (Appendix C, Figure 8) approximately followed the regression line. Therefore, a normal distribution of the data can be confirmed (Ghasemi & Zahediasl, 2012).

Demographic Analysis

This study collected data on five demographic indicators. A breakdown is shown in Table 3. Of the 356 participants, 146 (41.0%) were females while 210 (59.0%) were males, with most, 208 (58.0%) falling between the 25 to 44 age groups. Additionally, over 227 (64.0%) reported using mobile devices to access the internet for more than 10 years. Moreover, 245 (69.0%) are full-time employees, approximately 40 (11.0%) are

self-employed, and the majority have a bachelor's or master's degree, 141 (39.0%) and 84 (24.0%), respectively.

Table 3
Descriptive Statistics of the Population (N=356)

Items	Frequency	Percentage
<i>Gender</i>		
Male	210	59%
Females	146	41%
<i>Age Range</i>		
18-24	21	6%
25-34	118	33%
35-44	90	25%
45-54	75	21%
55-64	40	11%
65+	12	4%
<i>Years using Internet-Mobile Devices</i>		
4 or under	18	5%
5-9	92	26%
10-14	117	33%
15-19	60	17%
20-24	35	10%
25+	34	9%
<i>Employment Status</i>		
Full-time	245	69%
Part-time	24	7%
Unemployed	13	3%
Self-employed	40	11%
Homemaker	3	1%
Student	17	5%
Retired	14	4%
<i>Highest Level of Education</i>		
High School/GED	29	8%
Some college	51	14%
Associate's degree	27	8%
Bachelor's degree	141	39%
Master's degree	84	24%
Doctoral degree	11	3%
Professional degree	13	4%

After the pre-analysis data screening process, reliability and validity was checked before answering the research questions and hypothesis.

Reliability and Validity

Cronbach's Alpha and average variance extracted (AVE) in SmartPLS 3.0 were used as measures of internal reliability consistency and convergent validity, respectively. According to Hair et al. (2014), Cronbach's Alpha provides a measure or indication of how closely related a set of items are in the same group, while the AVE is the extent to which an item correlates positively with alternative items of the same constructs. In addition to the Cronbach's Alpha values, the composite reliability values were used to assess the reliability of the constructs. These two criteria were expected to indicate construct reliability. The Cronbach Alpha's and composite reliability coefficients of 0.7 or higher was used to suggest internal reliability and AVE values of at least 0.5 as acceptable validity (Hair et al., 2014; Levy & Danet, 2010). As shown in Table 4, both the Alpha and composite reliability values exceed the 0.7 minimum. Therefore, high levels of internal consistency reliability have been confirmed among all the latent variables.

Further analysis on the construct's convergent validity using AVE revealed that seven out of the twelve latent variables have been found to be equal to or greater than the minimum acceptable value of 0.5 (Wong, 2013); however, the remaining five showed values below 0.50. Those five latent variables were AGREE, CONS, EXTRA, INTEL, and MDSU, with values of 0.422, 0.369, 0.446, 0.343, and 0.375, respectively.

Table 4
Construct Reliability and Validity for this Study's Constructs (N = 356)

Constructs	Cronbach Alpha's	rho_A	Composite Reliability	AVE
Intellect	0.791	0.801	0.835	0.343
Agreeableness	0.854	0.885	0.873	0.422
Conscientiousness	0.819	0.833	0.853	0.369
Extraversion	0.906	0.777	0.883	0.446
Neuroticism	0.901	0.889	0.909	0.504
Perceived Threat Severity	0.937	0.942	0.952	0.798
Perceived Threat Susceptibility	0.942	0.963	0.955	0.811
Mobile Self-Efficacy	0.891	0.904	0.924	0.753
Perceived Response Cost	0.939	0.965	0.949	0.703
Response Efficacy	0.949	0.951	0.959	0.797
Mobile Device User Intention	0.813	0.822	0.870	0.574
Mobile Device Security Usage	0.747	0.789	0.815	0.375

According to Ringle, Bido, and Silva (2014), a factor analysis can be conducted to elevate the value of latent variables that have an AVE below 0.5. Generally, indicators with outer loadings between 0.4 and 0.7 should be considered for removal only when deleting the indicators leads to an increase in AVE (Bagozzi, Yi & Philipps, 1991; Hair et al., 2014). After eliminating the outer loading below than or equal to 0.4, the AVE for AGREE, EXTRA, and MDSU were found to be equal to or greater than the minimum acceptable value of 0.5. Using Table 5, it can be seen that the AVE for CONS and INTEL, with values 0.411 and 0.422, remained below the recommended level of 0.5. According to Fornell and Larcker (1981), the AVE is a more conservative estimate of the

validity of the measurement model, and “on the basis of compositive reliability alone, the researcher may conclude that the convergent validity of the construct is adequate, even though more than 50% of the variance is due to error” (p. 46). As the composite reliability of CONS and INTEL is well above the recommended level of 0.7, the convergent validity is acceptable (See Appendix D for the outer loadings values).

Table 5

Construct Reliability and AVE for this Study's Constructs (N = 356)

Constructs	Cronbach Alpha's	rho_A	Composite Reliability	AVE
Intellect	0.773	0.780	0.834	0.422
Agreeableness	0.848	0.884	0.883	0.522
Conscientiousness	0.813	0.817	0.848	0.410
Extraversion	0.901	0.842	0.899	0.534
Neuroticism	0.901	0.887	0.909	0.503
Perceived Threat Severity	0.937	0.942	0.952	0.798
Perceived Threat Susceptibility	0.942	0.963	0.955	0.811
Mobile Self-Efficacy	0.891	0.904	0.924	0.753
Perceived Response Cost	0.939	0.965	0.949	0.703
Response Efficacy	0.949	0.951	0.959	0.797
Mobile Device User Intention	0.813	0.822	0.870	0.574
Mobile Device Security Usage	0.760	0.789	0.845	0.536

Discriminant Validity

The Fornell and Larcker (1981) criterion for examining discriminant validity was used for this study. As stated by Henseler, Ringle, and Sarstedt (2015), “discriminant validity ensures that a construct measure is empirically unique and represents phenomena

of interest that other measures in a structural equation model do not capture” (p. 116). The square root of the AVE values for each latent variable was taken from SmartPLS 3.0 and presented in Appendix E. According to Hair et al. (2014), if the computed square root of each construct’s AVE is greater than the other correlation values among any other latent variables, then discriminant validity would have been demonstrated.

By examining Table 6 in Appendix E, the square root of the AVE values recorded for INTEL (0.649), AGREE (0.723), CONS (0.641), EXTRA (0.731), NEURO (0.708), TSE (0.893), TSU (0.901), RC (0.838), RE (0.893), MSE (0.868), MDUI (0.757), and MDSU (0.732), it can be seen that these values are larger than or equal to the other values in their corresponding rows and columns. Discriminant validity is therefore evident in the measurement’s items of this study.

Research Questions and Hypotheses

The main research question that this study addressed was: to what extent do cognitive factors and personality traits influence the usage of mobile device security technologies? There were three specific research questions and eleven hypotheses. As noted in Chapter 3, the relationships among the IVs and DVs, that is, the influence of the IVs on the DV, were assessed using path analysis in SmartPLS 3.0. Therefore, path analysis in SmartPLS 3.0 addressed RQ1 to RQ3, as well as H1 to H11. Figure 9 shows the results of the standardized path coefficients (β), along with the R-squared (R^2) values for the hypothesized causal model. The numbers that are noted above the arrows represent the path coefficients (β), while the R^2 values are noted within the given constructs where R^2 is applicable (MDUI and MDSU). Path coefficients are used to estimate the strengths of the relationship between constructs in the model, while R^2 is a

measure of the predictive accuracy of the model (Hair et al., 2014; Mertler & Vannatta, 2013). Path coefficients have range values between -1 and +1, with values that are closer to +1 indicating strong positive relationships, values closer to -1 depicting strong negative relationships, and values that are closer to zero indicating weak relationships (Hair et al. 2014). R^2 values of 0.75, 0.50, and 0.25 have been classified as substantial, moderate, and weak, respectively, and indicate that the amount of variance in the DVs can be explained by the IVs (Hair et al., 2014).

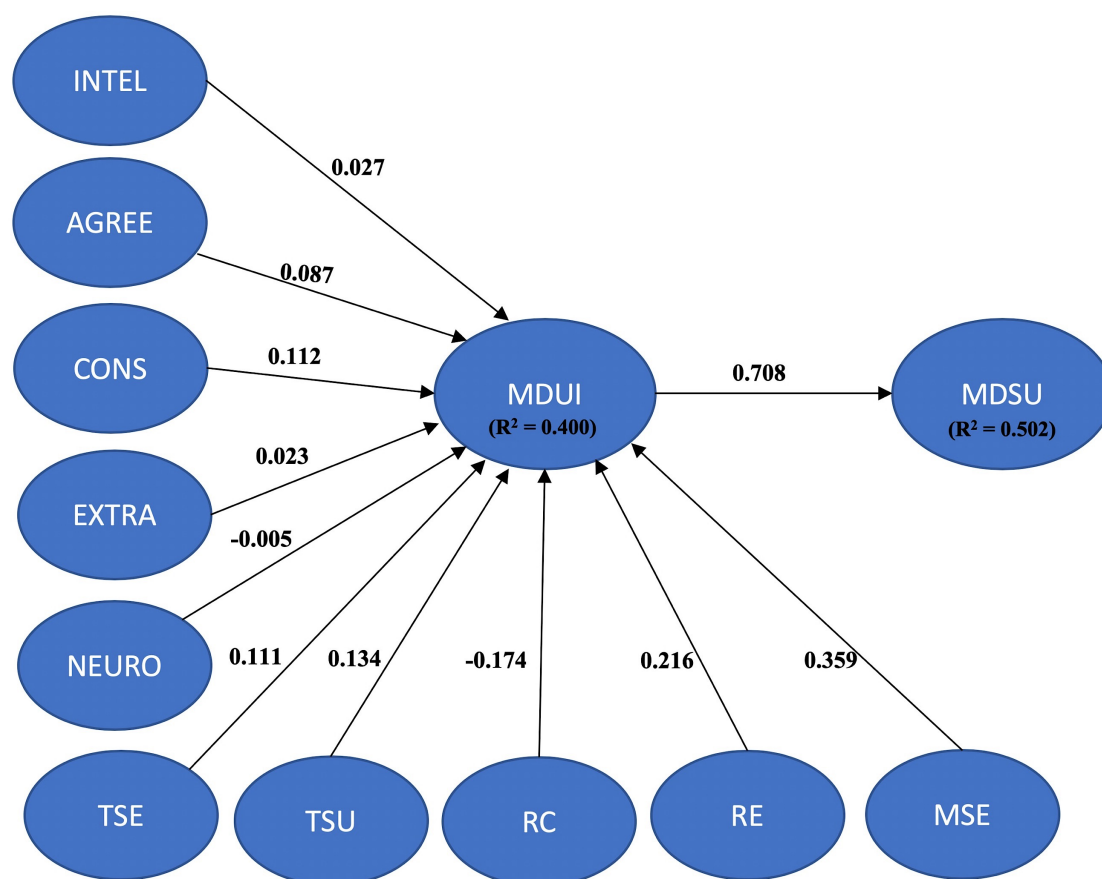


Figure 9. PLS Analysis Result for Mobile Device Security Usage (N=356)

As shown in Figure 9, the coefficient of determination, R^2 , is 0.400 for MDUI and 0.502 for MDSU latent variables. This means that personality factors (EXTRA, AGREE, CONS, INTEL, and NEURO) as well as cognitive factors (TSE, TSU, RC, RE, and

MSE) moderately explain 40% of the variance in MDUI, while MDUI moderately explains 50.2% of the variance in MDSU. The path coefficient sizes suggested that MDUI has the strongest effect on MDSU ($\beta = 0.708$). Additionally, MSE has the strongest effect on MDUI ($\beta = 0.359$), followed by RE ($\beta = 0.216$) and RC ($\beta = -0.174$). Many of the paths had very low path coefficients such as EXTRA ($\beta = 0.023$), AGREE ($\beta = 0.087$), INTEL ($\beta = 0.027$), and NEURO ($\beta = -0.005$). These low values indicate weak positive relationships for the paths with positive values and weak negative relationships for the paths with negative values (See Appendix F for the PLS-SEM results).

The SmartPLS 3.0 tool can also generate *t-statistics* for significance testing of both the inner and outer model, using a procedure called bootstrapping. Figure 10 shows the results of the bootstrapping analysis with 500 re-sampling used to test the significance of the hypotheses in this study. The numbers that are noted above the arrows represent the *t-statistics* values (See Appendix G for the bootstrapping p-values results).

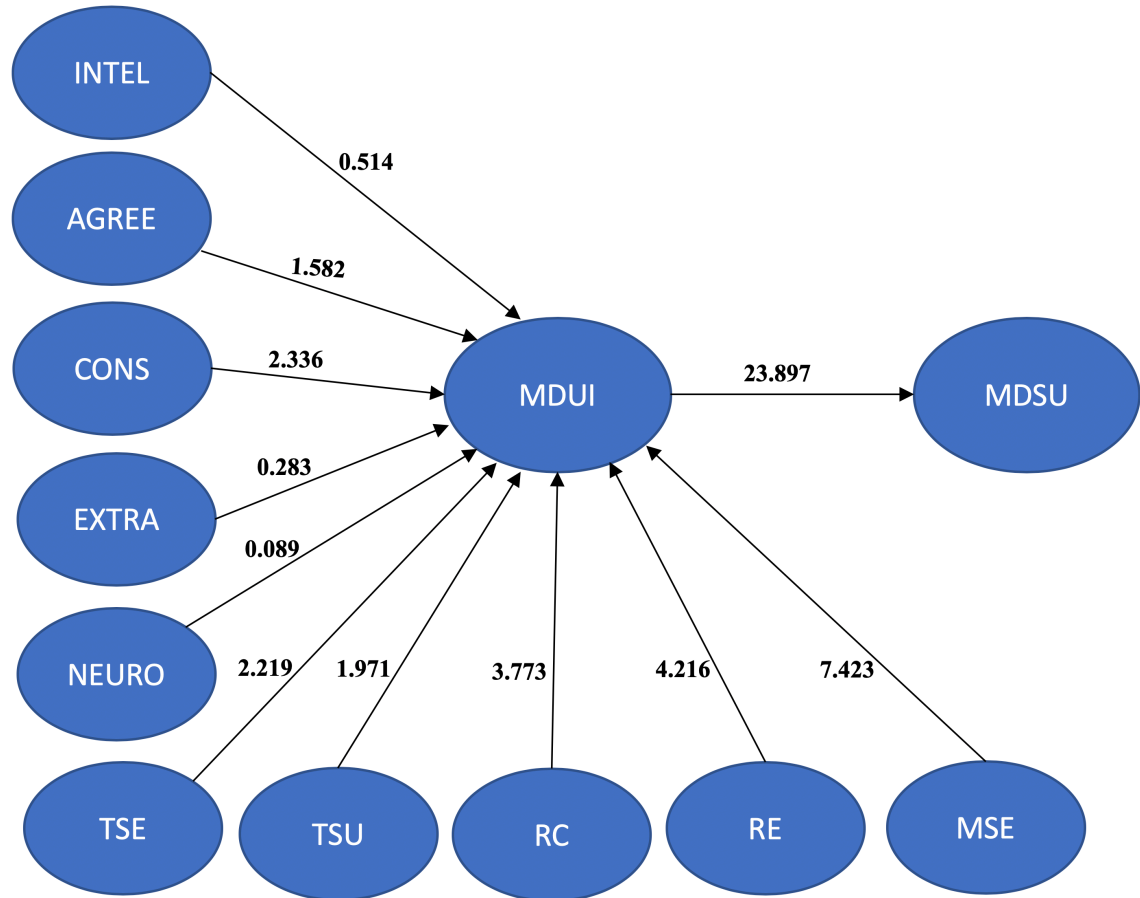


Figure 10. Bootstrapping Results for Mobile Device Security Usage (N=356)

Based on the path analysis and bootstrapping results in SmartPLS 3.0, TSE ($\beta = 0.111, p < 0.05$) and TSU ($\beta = 0.134, p < 0.05$) has a significant positive contribution on MDUI. Thus, **H1** and **H2** were fully supported. RC ($\beta = -0.174, p < 0.001$) has a significant negative contribution on MDUI, hence, there was full support for **H3**. In contrast, RE ($\beta = 0.216, p < 0.001$) as well as MSE ($\beta = 0.359, p < 0.001$) have a significant positive contribution on MDUI. Thus, **H4** and **H5** were fully supported. The analysis also showed that personality factor INTEL ($\beta = 0.027, p > 0.05$) surprisingly had no significant effect on MDUI. Similarly, AGREE ($\beta = 0.087, p > 0.05$) did not show to have a significant effect on MDUI. Nevertheless, the personality factor CONS ($\beta =$

0.112, $p < 0.05$) had a significant positive contribution on MDUI. Thus, **H6** and **H7** were not supported, while **H8** was supported. The direction of the effect of EXTRA ($\beta = 0.023$, $p > 0.05$) on MDUI was non-significant. Hence, **H9** was not supported. Interestingly, NEURO ($\beta = -0.005$, $p > 0.05$) also had no significant effect on MDUI. This implies that the path relationship between NEURO and MDUI **H10** was not supported. The model further suggested that MDUI ($\beta = 0.708$, $p < 0.001$) had a significant and direct positive effect on MDSU. Thus, **H11** was supported. A summary of the results of the hypotheses testing is shown in Table 7 below.

Table 7

Summary of Hypotheses Testing for H1 to H11 (N = 356)

	Path	Path Coefficients (β)	t-value	p-value	Supported
H1	TSE \rightarrow MDUI	0.111	2.219	0.027	Yes
H2	TSU \rightarrow MDUI	0.134	1.971	0.049	Yes
H3	RC \rightarrow MDUI	-0.174	3.773	0.000	Yes
H4	RE \rightarrow MDUI	0.216	4.216	0.000	Yes
H5	MSE \rightarrow MDUI	0.359	7.423	0.000	Yes
H6	INTEL \rightarrow MDUI	0.027	0.514	0.608	No
H7	AGREE \rightarrow MDUI	0.087	1.582	0.114	No
H8	CONS \rightarrow MDUI	0.112	2.336	0.020	Yes
H9	EXTRA \rightarrow MDUI	0.023	0.283	0.777	No
H10	NEURO \rightarrow MDUI	-0.005	0.089	0.929	No
H11	MDUI \rightarrow MDSU	0.708	23.897	0.000	Yes

Summary

This chapter presented the results of this study. First, the results of phase one, the validation procedures for the survey instrument, were outlined. This included an expert review panel in which some adjustments were made to the survey instrument. Next the results of the pilot test conducted with 20 participants in phase two was outlined. Based

on the pilot test feedback, there were no necessary changes or modifications made to the survey instrument. Finally, phase three, which included the main data collection of the measures that addressed the research questions, including pre-analysis data screening and data analysis, were presented.

The eleven hypotheses presented in this study were tested in SmartPLS 3.0. Of the eleven hypotheses, the results showed that (H1 to H5, H8, and H11) had a significant effect on mobile device user intention (MDUI), and were, hence, fully supported. The remaining hypotheses (H6, H7, H9, and H10) were found to have no significant effect on mobile device user intention (MDUI), and were hence, not supported. Some very interesting and unexpected results were found which will be further discussed in the next chapter.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Internet use by mobile device users continues to rise, and with increased usage, the number and level of information security threats have also increased (D'Arcy & Devaraj, 2012; Tu et al., 2015). The promise of information security implies protection and prevention, which, in turn, implies technological and human behavioral interventions (Pfleeger et al., 2014; Safa et al., 2016). However, the literature has suggested that technology alone cannot provide the solution for information security threats. For this reason, this study examined the role that behavioral science theories can play in expanding research, in deepening the industry understanding of risk to information security, and in contributing to reducing the risk of data breaches. Consequently, the main goal of this study was to identify the cognitive factors and personality traits that influence the usage of mobile device security technologies. By applying the research model, the main goal was achieved by answering three research questions.

The first research question incorporated the PMT predictors of behavior in the form of perceived threat severity, perceived threat susceptibility, perceived response costs, response efficiency, and mobile self-efficacy, and their influence on the mobile device user's intention to use mobile device security technologies. Based on the performed data analysis, mobile device user intention was positively influenced by

perceived threat severity. Reports in the literature indicated that there was a relationship between perceived threat severity and behavioral intention (Lee & Larsen, 2009; Woon, Tan, & Low, 2005). While some research indicates a positive relationship in that increased level of threat severity will influence user's intention to use security measures and motivate mitigating actions (Crossler et al., 2018; Thompson et al., 2017; Woon et al., 2005), others have reported a negative relationship. For example, Mwangabi et al. (2018) found that neither susceptibility to a security attack nor the level of severity of an attack influenced password guideline compliance, while Giwah (2018) reported a negative relationship between the level of perceived threat severity and mobile device security usage. However, the findings of this study support the positive relationship reports, as overall, in the information security domain, perceived threat severity has generally been found to positively influence security intentions (Alsaleh, Alomar, & Alarifi, 2017; Crossler et al., 2018; Siponen et al. 2014; Vance et al., 2012).

The findings of this study suggest that perceived threat susceptibility is a necessary factor for mobile device users to adopt mobile device security measures. The positive contribution of perceived threat susceptibility on mobile device user intention is not surprising as it is supported by the existing literature. For instance, Giwah (2018) suggested that the more individuals consider themselves threatened by the negative consequences of losing their data, the better the chance that they will protect themselves against mobile device threats. Similarly, Posey et al. (2015) considered threat susceptibility to be a "major component in the threat appraisal process and overall formation of insider's protection motivation" (p. 14). Matt and Peckelsen (2016) also found that user's adoption of privacy-enhancing technologies can be predicted from their

perceptions of the degree of harm that they would face as a result of a privacy-invading incident.

Furthermore, the results of this study show that response cost has a significant negative contribution on mobile device user intention. This finding is consistent with previous literature that suggests that perceived response costs in terms of effort, time, and money influence the intention of adopting protective behaviors against information security threats (Arachchilage & Love, 2013; Boss et al., 2015; Burns et al., 2017; Posey et al., 2015; Vance et al., 2012). Although this finding was expected, there are reports in the literature of contradictory findings regarding the relationship between response cost and intention. For example, Giwah (2018) found that the response cost of security measures did not influence the protection motivation of individuals to secure their devices from information security threats. Mou et al. (2017) also reported that response cost is not a significant predictor of intention. However, there are more reports in the literature that support the significant negative relationship between perceived response cost and intention. Thus, it can be inferred from this study's findings that an increase in response costs results in a decrease in the intention to perform recommended protective behaviors.

This study shows that response efficacy has a significant positive contribution on intention to use mobile device security technologies. This finding is not contrary to the literature. For instance, Johnston and Warkentin (2010) observed that, "moderate to high levels of response efficacy are associated with positive inclinations of threat mitigation whereby a recommended response is enacted" (p. 553). Similarly, Posey et al. (2015), as well as Giwah (2018), agree that response efficacy is a significant predictor of intention.

This implies that as an individual's response efficacy increases, their intention to use mobile device security technologies should also increase.

Interestingly, mobile self-efficacy not only had a significant positive contribution on mobile device user intention, but also was the strongest predictor of intention. Prior research has also found mobile self-efficacy to be the most significant factor in explaining security behavior in the context of mobile devices (Chan et al. 2006; Giwah, 2018; Keith et al., 2015; Posey et al., 2015). Similarly, Thompson et al. (2017), as well as Verkijika (2018), suggest that self-efficacy is the strongest predictor of information security intentions of both home computer and mobile devices. The finding of this study is consistent with such reports and indicates that an increase in an individual's self-efficacy in using the recommended mobile device security technologies against security threats should result in an increase in their intention to use these protective technologies.

One unexpected conclusion drawn from this study is that coping appraisal factors such as response cost, response efficacy, and mobile self-efficacy were more significant for behavior intention than threat appraisal factors within the research model. This implies that individuals' coping appraisal is a more significant determinant of one's actions in the mobile device security context than are one's perceptions of their vulnerability and the potential for harm that may arise from a threat. Even if the level of severity and susceptibility are high, individuals may not take action if they do not believe in their ability to take action or do not believe the action will be effective against the threat.

The second research question incorporated the five personality traits constructs and their influence on the mobile device user's intention to use mobile device security

technologies. The personality traits constructs included extraversion, agreeableness, conscientiousness, neuroticism, and intellect (Goldberg, 1993; McCrae & Costa, 1997). Results indicated that there was no significant effect of any personality traits on mobile device user's intention except for conscientiousness. As proposed, conscientiousness had a significant positive contribution on intention. Similarly, Gratian (2018) found conscientiousness to be the only significant predictor on security behavior intentions. Xu et al. (2016) also found conscientiousness to have a significant positive impact on an individual's adoption behavior of mobile applications. Xu et al. argue that conscientious people are found to be less likely to adopt leisure mobile applications to avoid distraction from their productive activities. A conscientious individual tends to stick to established rules and procedures; hence, they are less willing to get involved in risky situations and will initiate efforts to protect themselves from potential threats (Goldberg, 1993; Matt & Peckelsen, 2016; McCrae & Costa, 1997). This implies that, within the context of mobile device security usage, individuals that score high in terms of the degree of their conscientiousness would be more likely to adopt protective technologies.

The third and final research question examined the role of intention as a predictor of actual mobile device security usage. The results of the study suggest that actual mobile device security usage is significantly influenced by the user's intention to adopt mobile device security technologies. The existing literature fully supports this finding. According to Posey et al., (2015), the impact of intention on behavior is not only significant, but positively so. Giwah (2018), citing Rogers (1983), asserts that when threat and coping appraisals are at moderate to high levels, an individual's intention is equally increased, thereby significantly influencing actual behavior.

Results show that most personality factors have no influence on an individual's intention, except for conscientiousness. However, the integration of personality factors led to a substantially better explanatory model, thus confirming that personality traits influence the usage of mobile device security technologies. For instance, Giwah (2018)'s study found that the protection motivation theory factors explain 30 percent of the variance in an individual's motivation. Similarly, Gratian (2018)'s study found individuals' personalities accounted for 23 percent of the variance in security behavior intentions. In contrast, the research model combined both cognitive factors and personality traits to explain actual usage of mobile device security technologies. The results show that mobile device user's intention explained 50.2 percent of the variance in mobile device security usage. This implies that, within the context of this study, conscientious individuals with moderate to high levels of coping appraisals are more likely to use mobile device security technologies.

Limitations of the Study

Similar to other studies, this study has several limitations. The first limitation is that the scope of this research was restricted to mobile device security behaviors, and the population consisted of only United States individuals. Additionally, this study did not consider other factors such as culture, language, or socio-economic conditions that might influence the usage of mobile device security technologies. As such, caution should be exercised when generalizing the results from this study. Further studies may be required using other populations to better validate and enhance the generalizability of the results.

Another limitation to this study is that the measured data was based on self-reported data. The limitations of self-reported data entail certain risks to validity,

including self-selection biases, problems with accuracy, and the individual participant's desire to be viewed in a positive way (Rosenbaum et al., 2006). According to Knapp and Kirk (2003), participants may be reluctant to report certain behaviors with concern over the confidentiality and security of the data, fearing that the information could be used against them. A further limitation of self-reported data is the inability of the researcher to verify the honesty of the participant (Emerson, Felce, & Stancliffe, 2013). Finally, due to the survey being close to a hundred questions, it is possible that random clicking, fatigue, or failures to carefully read questions affected the accuracy of the responses.

Recommendation for Future Studies

Based on the findings of this study, future research can continue to explore the factors that will influence the actual usage of mobile device security technologies so that mobile device users can adequately protect themselves from information security threats. While this study examined the usage of mobile device security technologies as it relates to data breaches, other information security behaviors such as password selection, data encryption, or data backup procedures could be analyzed to further establish the relationships evident in this study. Future research could also consider developing a shorter instrument to assess an individual's personality traits. The feedback from many of the participants was that they felt many of personality traits questions were too repetitive. After the development of a shorter assessment tool, this study could be repeated to see if similar results emerge.

Another area of future research might be an examination of the effects of security education, training, and awareness programs on mobile device users based on the differences in personality traits. Results show that the personality trait conscientiousness

has an impact on how individuals react to information security threats. It is therefore recommended that future research in mobile device security pay particular attention to conscientiousness and study this construct further. Finally, future research could include other countries and cultures to investigate the consistency of the results of this study. Research of this nature will serve to enhance the generalizability of this study.

Implications and Recommendations

This study makes theoretical and practical contributions to the emerging knowledge of behavioral issues in regard to the use of mobile device security technologies. Prior literature has shown that protection motivation theory (PMT) was an important behavioral model that could be used to examine the usage of mobile device security technologies (Giwah, 2018; Verkijika, 2018). However, this study makes a theoretical contribution with the integration of both PMT factors and personality traits as antecedents of user's intention to use mobile device security technologies. Prior studies focusing on PMT showed that intention accounted for less than 26 percent of the variance in information security behavior (Giwah, 2018; Liang & Xue, 2010; Shropshire et al., 2015; Thompson et al., 2017). However, by including personality trait factors, the findings of this study showed mobile device user's intention accounted for 50.2 percent of the variance. This supports the view of Thompson et al. (2017), as well as Giwah (2018), that intention is a strong predictor of actual security behavior.

The findings of this study also offer some important practical contributions. First, results identified that coping appraisal factors were the best determinant of intentions, and subsequently the usage of mobile device security technologies. This implies that any efforts to increase a user's belief in the effectiveness of a protective behavior against

mobile device threats (Response Efficacy), and their confidence in performing these behaviors (Mobile Self-Efficacy), as well as reducing the perceived costs to perform these behaviors (Response Costs), would increase a user's intention to perform these behaviors. This would then encourage the actual usage of mobile device security technologies.

One recommendation is for training materials and resources relating to mobile device security threats to include recommended behaviors that can both be perceived to be effective, and that a user feels confident enough to perform themselves. This would work towards increasing the user's response efficacy and mobile self-efficacy, respectively. In addition, information presented to users should also emphasize the small costs required to use the recommended protective behaviors against mobile device threats, particularly in comparison to the potentially large costs of becoming a mobile device data breach victim. This would work towards reducing the perceived response costs for the usage of mobile device security technologies. Furthermore, including detailed descriptions of how to implement recommended mobile device security technologies (e.g. how-to setup and scan for viruses) would make these technologies seem less burdensome to an individual and reduce response costs. Including detailed instructions on how to use the mobile device security technologies could also potentially increase a user's confidence to perform these behaviors themselves, increasing mobile self-efficacy.

Another recommendation is for educational training material and resources to include hyperlinks to available mobile device security tools where possible, to provide users with an easy and effortless way to access them. This would not only inform users

that they should use these technologies, but also provide them with a way to obtain these tools and to begin their usage without any further effort required. This practical approach works towards the reduction of response costs for adopting these technologies, thereby increasing user willingness to use them in their mobile devices (Giwah, 2018; Tu et al., 2015).

According to Filkins and Hardy (2016), large organizations spend nearly 35 percent of their annual security budget on end user training and awareness. The second practical recommendation of this study is for information security professionals to prioritize their training efforts on end users who exhibit individual differences that are significant predictors of poor security behavior intentions. For example, low conscientious individuals who procrastinate and tend to make a mess of things were found to exhibit significantly weaker intentions for using mobile device security technologies. Therefore, low conscientiousness users may be a demographic group in need of additional security training and guidance.

Despite prior literature (Gratian et al., 2018; Matt & Peckelsen, 2016; Shropshire et al., 2015; Uffen et al., 2013; Xu et al., 2016), this study found that personality traits agreeableness, extraversion, intellect, and neuroticism have no influence or very weak influence on mobile device security usage. Since the model did not find these personalities significant, the third practical recommendation of this study is for an organization to take the position that employees of all age groups, regardless of personality traits, may be susceptible to risky behavior in the context of data breaches. This reinforces the need for organization-wide security training of all employees and for strong policies and procedures (McCormac et al., 2017).

Summary

This study addressed the need for the identification and a better understanding of the factors responsible for the usage of mobile device security technologies (Anderson & Agarwal, 2010; Crossler et al., 2013; Limayem et al., 2007; Matt & Peckelsen, 2016; Shropshire et al., 2015). Given the lack of understanding about the predictors of actual usage of mobile device security technologies (Uffen et al., 2013; Xu et al., 2016), research has been recommended to identify the factors responsible for this behavior. The main goal of this study was to assess the effect that cognitive factors and personality traits have on the intention of mobile device users and to determine whether intention leads to the actual use of mobile device security technologies. The cognitive factors incorporated the protection motivation theory predictors of behavior in the form of perceived threat severity, perceived threat susceptibility, perceived response costs, response efficiency, mobile self-efficacy, mobile device user intention, and mobile device security usage. Also, the five broad personality trait constructs included for this study were extraversion, agreeableness, conscientiousness, neuroticism, and intellect (Goldberg, 1993; McCrae & Costa, 1997).

The main research question that this study addressed was: To what extent do cognitive factors and personality traits influence the usage of mobile device security technologies? By applying the research model, the main question was broken down into three distinct research questions:

RQ1: Will perceived threat severity, perceived threat susceptibility, perceived response costs, response efficiency, and mobile self-efficacy influence mobile device user's intention to use mobile device security technologies?

RQ2: Will intellect, agreeableness, conscientiousness, extroversion, and neuroticism influence mobile device user's intention to use mobile device security technologies?

RQ3: Will mobile device user's intention influence mobile device security usage?

To answer these research questions, a quantitative method was employed to develop and validate the research model. The research methodology followed a three-phased approach as follows. In phase one, the survey instrument was developed based on validated measures from prior research, and further validated using an expert-review process that followed the Delphi technique. The expert's feedback helped finalized the survey instrument, which was then used in phase two in the pilot test. The revised survey instrument consisted of nine sections and 99 items, with each section measuring one of the research model's variables.

In phase two, prior to the main data collection, there was a pilot study with 20 participants. Descriptive data analysis for the pilot test was conducted using SPSS to get a feel for the data, however, there were no changes to the survey instrument during the pilot test phase.

In phase three, the main data collection that addressed the research questions, including data analysis and interpretation, was conducted. Using a web-based survey instrument, data was collected from 358 participants, ranging in age from 18 to 65, with most falling in the 25 to 34 age groups. At the end of the data collection period, which lasted for two months, pre-analysis data screening was conducted using SPSS. The descriptive statistics from SPSS confirmed that there were no missing values, all responses were within the specified ranges, and the frequencies were valid. Outlier

detection for the data collected was conducted using Mahalanobis Distance. The outlier analysis detected some IDs as potential multivariate outliers. However, after further analysis, including examining the chi-square distribution, two IDs were significant and were removed. Thus, 356 survey responses were kept. Path analysis in SmartPLS 3.0 addressed RQ1 to RQ3 as well as H1 to H11. Overall, seven of the eleven hypotheses tested in SmartPLS 3.0 were fully supported. These include H1 TSE → MDUI, H2 TSU → MDUI, H3 RC → MDUI, H4 RE → MDUI, H5 MSE → MDUI, H8 CONS → MDUI, and H11 MDUI → MDSU. The remaining hypotheses were not supported, i.e., H6 INTEL → MDUI, H7 AGRE → MDUI, H9 EXTRA → MDUI, and H10 NEURO → MDUI.

This study identified a number of limitations, such as the generalization of the findings, as the study did not consider factors such as culture and socio-economic conditions. Another limitation relates to self-reported data where participant's answers may be exaggerated. Ideas for future research were also presented in this study. For example, future research can consider developing a shorter survey instrument to assess individual's personality traits. Future studies can also explore other information security behaviors such as password selection, data encryption, or data backup procedures to further establish the relationships presented in this study.

Theoretically, this study adds to the body of knowledge on the factors that influence the adoption of mobile device security technologies. The focus and findings of this study are believed to have brought some clarity on the cognitive process and personality trait differences that lead to the actual usage of mobile device security technologies by mobile device users. Furthermore, this study is one of the few that

combines the protection motivation theory factors and the big five personality traits into a single research model within the context of mobile device security usage. As studies of this nature gain traction in the information security domain, researchers will find unexpected results and bring additional insight to the existing literature.

Appendix A

Table 8
Constructs Items and Instrument Source

Constructs/Items	Description	Source
Intellect	Describe yourself as you generally are now, not as you wish to be in the future.	
INTEL1	Have a rich vocabulary.	Goldberg (1993, 2006)
INTEL2	Have difficulty understanding abstract ideas.	Goldberg (1993, 2006)
INTEL3	Have a vivid imagination.	Goldberg (1993, 2006)
INTEL4	Am not interested in abstract ideas.	Goldberg (1993, 2006)
INTEL5	Have excellent ideas.	Goldberg (1993, 2006)
INTEL6	Do not have a good imagination.	Goldberg (1993, 2006)
INTEL7	Am quick to understand things.	Goldberg (1993, 2006)
INTEL8	Use difficult words.	Goldberg (1993, 2006)
INTEL9	Spend time reflecting on things.	Goldberg (1993, 2006)
INTEL10	Am full of ideas.	Goldberg (1993, 2006)
Agreeableness	Describe yourself as you honestly see yourself.	
AGREE1	Feel little concern for others.	Goldberg (1993, 2006)

AGREE2	Am interested in people.	Goldberg (1993, 2006)
AGREE3	Insult people.	Goldberg (1993, 2006)
AGREE4	Sympathize with other's feeling.	Goldberg (1993, 2006)
AGREE5	Am not interested in other people's problems.	Goldberg (1993, 2006)
AGREE6	Have a soft heart.	Goldberg (1993, 2006)
AGREE7	Am not really interested in others.	Goldberg (1993, 2006)
AGREE8	Take time out for others.	Goldberg (1993, 2006)
AGREE9	Feel other's emotions.	Goldberg (1993, 2006)
AGREE10	Make people feel at ease.	Goldberg (1993, 2006)
Conscientiousness	Describe yourself in an honest manner.	
CONS1	Am always prepared.	Goldberg (1993, 2006)
CONS2	Leave my belongings around.	Goldberg (1993, 2006)
CONS3	Pay attention to details.	Goldberg (1993, 2006)
CONS4	Make a mess of things.	Goldberg (1993, 2006)
CONS5	Get chores done right away.	Goldberg (1993, 2006)
CONS6	Often forget to put things back in their proper place.	Goldberg (1993, 2006)

CONS7	Like order.	Goldberg (1993, 2006)
CONS8	Shirk my duties.	Goldberg (1993, 2006)
CONS9	Follow a schedule.	Goldberg (1993, 2006)
CONS10	Am exacting in my work.	Goldberg (1993, 2006)
Extraversion	Describe yourself as you generally are now, not as you wish to be in the future.	
EXTRA1	Am the life of the party.	Goldberg (1993, 2006)
EXTRA2	Don't talk a lot.	Goldberg (1993, 2006)
EXTRA3	Feel comfortable around people.	Goldberg (1993, 2006)
EXTRA4	Keep in the background.	Goldberg (1993, 2006)
EXTRA5	Start conversations.	Goldberg (1993, 2006)
EXTRA6	Have little to say.	Goldberg (1993, 2006)
EXTRA7	Talk to a lot of different people at parties.	Goldberg (1993, 2006)
EXTRA8	Don't like to draw attention to myself.	Goldberg (1993, 2006)
EXTRA9	Don't mind being the center of attention.	Goldberg (1993, 2006)
EXTRA10	Am quiet around strangers.	Goldberg (1993, 2006)

Neuroticism	Please indicate how much you agree with the statements.	
NEURO1	Get stressed out easily.	Goldberg (1993, 2006); Johnson (2014)
NEURO2	Am relaxed most of the time.	Goldberg (1993, 2006); Johnson (2014)
NEURO3	Worry about things.	Goldberg (1993, 2006); Johnson (2014)
NEURO4	Seldom feel blue.	Goldberg (1993, 2006); Johnson (2014)
NEURO5	Am easily disturbed.	Goldberg (1993, 2006); Johnson (2014)
NEURO6	Get upset easily.	Goldberg (1993, 2006); Johnson (2014)
NEURO7	Change my mood a lot.	Goldberg (1993, 2006); Johnson (2014)
NEURO8	Have frequent mood swings.	Goldberg (1993, 2006); Johnson (2014)
NEURO9	Get irritated easily.	Goldberg (1993, 2006); Johnson (2014)

NEURO10	Often feel blue.	Goldberg (1993, 2006); Johnson (2014)
Threat Severity	Please indicate the impact that each of these scenarios would have on you if it would occur.	
TSE1	My mobile device becoming corrupted by a virus.	Claar and Johnson (2012)
TSE2	My mobile device being taken over by a hacker.	Claar and Johnson (2012)
TSE3	My sensitive personal data (bank account, social security, etc.) being stolen from my mobile device.	Claar and Johnson (2012)
TSE4	My data being lost due to a virus on m mobile device.	Claar and Johnson (2012)
TSE5	My mobile device downloading a virus or bug infected application.	Claar and Johnson (2012)
Threat Susceptibility	Please indicate how likely you feel each of these scenarios will occur with your mobile device.	
TSU1	My mobile device becoming corrupted by a virus	Claar and Johnson (2012)
TSU2	My mobile device being taken over by a hacker.	Claar and Johnson (2012)
TSU3	My sensitive personal data (bank account, social security, etc.) being stolen from my mobile device.	Claar and Johnson (2012)
TSU4	My data being lost due to a virus on m mobile device.	Claar and Johnson (2012)
TSU5	My mobile device downloading a virus or bug infected application.	Claar and Johnson (2012)

Response Cost	Please indicate the degree to which you agree or disagree with the following statements.	
RC1	Using an anti-virus software on my mobile device decreases the device's convenience.	Boss et al. (2015); Woon et al. (2005).
RC2	Using an anti-malware software on my mobile device decreases the device's convenience	Boss et al. (2015); Woon et al. (2005).
RC3	Using an anti-virus software on my mobile device involves too much work.	Boss et al. (2015); Woon et al. (2005).
RC4	Using an anti-malware software on my mobile device involves too much work.	Boss et al. (2015); Woon et al. (2005).
RC5	Using an anti-virus software on my mobile device requires considerable investment.	Boss et al. (2015); Woon et al. (2005).
RC6	Using an anti-malware software on my mobile device requires considerable investment.	Boss et al. (2015); Woon et al. (2005).
RC7	Using an anti-virus software on my mobile device is time consuming.	Boss et al. (2015); Woon et al. (2005).
Response Efficacy	Please indicate the degree to which you agree or disagree with the following statements.	
RE1	Using anti-virus software works to protect my mobile device from data breach.	Boss et al. (2015); Johnston and Warkentin (2010).

RE2	Using anti-malware software works to protect my mobile device from data breach.	Boss et al. (2015); Johnston and Warkentin (2010).
RE3	Using an anti-virus software is effective to protect my mobile device from data breach.	Boss et al. (2015); Johnston and Warkentin (2010).
RE4	Using an anti-malware software is effective to protect my mobile device from data breach.	Boss et al. (2015); Johnston and Warkentin (2010).
RE5	Using an anti-virus software would more likely protect my mobile device from data breach.	Boss et al. (2015); Johnston and Warkentin (2010).
RE6	Using an anti-malware software would more likely protect my mobile device from data breach.	Boss et al. (2015); Johnston and Warkentin (2010).
Mobile Self-Efficacy	Please indicate the degree to which you agree or disagree with the following statements.	
MSE1	I am confident of selecting the appropriate security software to use on my mobile device.	Claar and Johnson (2012).
MSE2	I am confident of selecting the appropriate security settings on my mobile device.	Claar and Johnson (2012).
MSE3	I am confident of correctly installing security software on my mobile device.	Claar and Johnson (2012).

MSE4	I am confident of easily finding information on using security software on my mobile device.	Claar and Johnson (2012).
Mobile Device User Intention	Please indicate the degree to which you agree or disagree with the following statements.	
MDUI1	I intend to use mobile security software to protect my mobile device from threats.	Uffen et al. (2013); Shropshire et al. (2015).
MDUI2	I will execute data backups on my mobile device in regular intervals.	Uffen et al. (2013); Shropshire et al. (2015).
MDUI3	I plan to change my mobile device authentication password in regular intervals.	Uffen et al. (2013); Shropshire et al. (2015).
MDUI4	I intend to execute updates for firmware and applications in regular intervals	Uffen et al. (2013); Shropshire et al. (2015).
MDUI5	I predict I will use mobile security software to protect my mobile device from threats.	Uffen et al. (2013); Shropshire et al. (2015).
Mobile Device Security Usage	Please indicate the frequency you perform the following tasks	
MDSU1	I use a method to backup my mobile device (to PC, external hard drive, cloud, network storage, etc...).	Giwah (2018)
MDSU2	I use the firewall protection on my mobile device.	Claar and Johnson (2012)
MDSU3	I use an anti-virus software on my mobile device.	Claar and Johnson (2012)

MDSU4	I use an anti-malware software on my mobile device.	Claar and Johnson (2012)
MDSU5	I use password protection on my mobile device.	Giwah (2018)
MDSU6	I use biometric protection on my mobile device.	Giwah (2018)
MDSU7	I use software updates on my mobile device whenever they are available.	Giwah (2018)
MDSU8	I use operating system updates on my mobile device whenever they are available.	Giwah (2018)

Appendix B



MEMORANDUM

To: **nils lau**

From: **Wei Li, Ph.D,
Center Representative, Institutional Review Board**

Date: **November 12, 2019**

Re: **IRB #: 2019-530; Title, "The Influence of Cognitive Factors and Personality Traits on Mobile Device User's Information Security Behavior"**

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

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Wei Li, Ph.D, respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

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

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

Appendix C

Figure 3 Scatterplot of the Dependent Variable MDSU

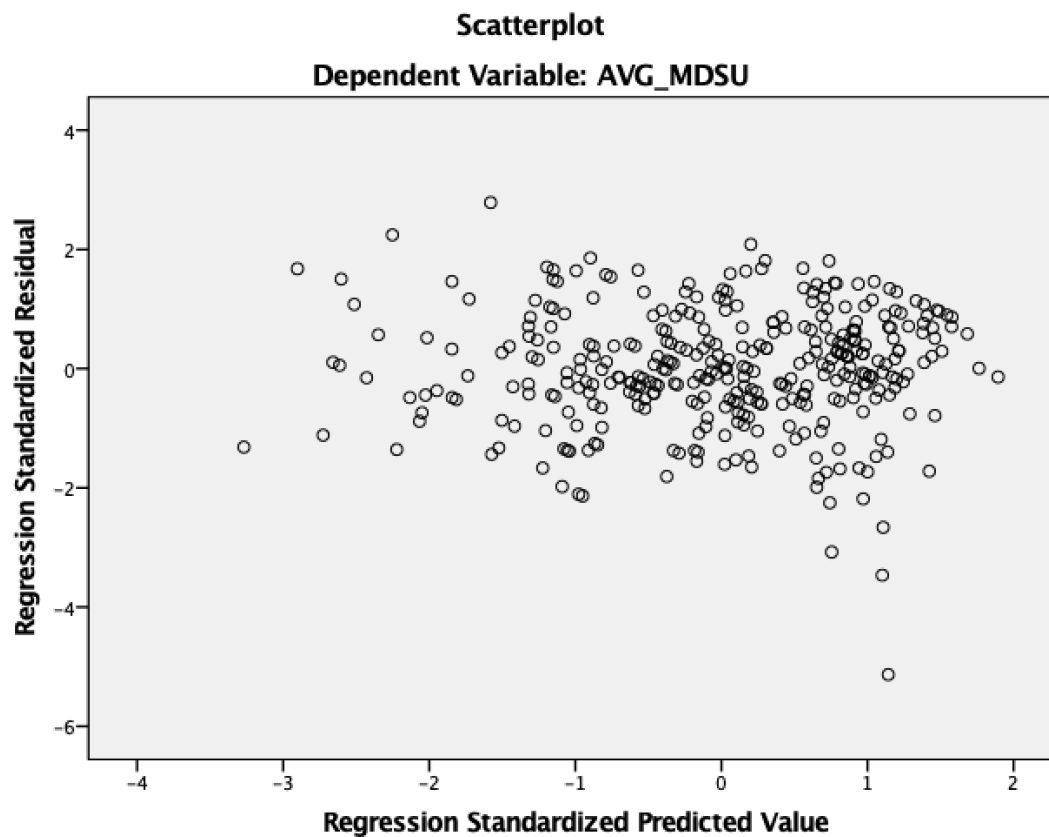


Figure 4 Durbin-Watson Statistics Results

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	Change Statistics			Durbin-Watson	
						F Change	df1	df2		
1	.752 ^a	.565	.551	.771060	.565	40.651	11	344	.000	2.275

a. Predictors: (Constant), AVG_MDUI, AVG_EXTRA, AVG_TSU, AVG_AGREE, AVG_RC, AVG_TSE, AVG_RE, AVG_CONS, AVG_MSE, AVG_NEURO, AVG_INTEL

b. Dependent Variable: AVG_MDSU

Figure 5 Collinearity Statistics

		Coefficients ^a										
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics		
		B	Std. Error	Beta			Zero-order	Partial	Part	Tolerance	VIF	
1	(Constant)	.555	.443		1.252	.211						
	AVG_EXTRA	.076	.049	.066	1.567	.118	.061	.084	.056	.720	1.389	
	AVG_AGREE	-.068	.066	-.044	-1.037	.301	.072	-.056	-.037	.710	1.408	
	AVG_CONS	.165	.066	.103	2.491	.013	.219	.133	.089	.744	1.344	
	AVG_NEURO	-.080	.051	-.070	-1.574	.116	.026	-.085	-.056	.644	1.552	
	AVG_INTEL	-.047	.079	-.027	-.597	.551	.191	-.032	-.021	.628	1.593	
	AVG_TSE	.018	.028	.026	.629	.530	.233	.034	.022	.762	1.312	
	AVG_TSU	.049	.032	.063	1.530	.127	.096	.082	.054	.735	1.361	
	AVG_RC	.011	.032	.015	.363	.717	-.158	.020	.013	.744	1.344	
	AVG_RE	.048	.042	.047	1.146	.253	.338	.062	.041	.755	1.325	
	AVG_MSE	.201	.034	.247	5.834	.000	.493	.300	.207	.705	1.418	
	AVG_MDUI	.707	.056	.567	12.609	.000	.709	.562	.448	.626	1.597	

a. Dependent Variable: AVG_MDSU

Figure 6 Cook's Distance Statistics

		Residuals Statistics ^a				
		Minimum	Maximum	Mean	Std. Deviation	N
	Predicted Value	2.14026	6.60791	4.96945	.865377	356
	Std. Predicted Value	-3.269	1.893	.000	1.000	356
	Standard Error of Predicted Value	.077	.231	.138	.032	356
	Adjusted Predicted Value	2.21597	6.61332	4.96901	.865976	356
→	Residual	-3.957178	2.147891	.000000	.759020	356
	Std. Residual	-5.132	2.786	.000	.984	356
	Stud. Residual	-5.215	2.852	.000	1.002	356
	Deleted Residual	-4.086434	2.251791	.000447	.786307	356
	Stud. Deleted Residual	-5.427	2.882	-.001	1.008	356
	Mahal. Distance	2.571	30.775	10.969	5.717	356
	Cook's Distance	.000	.074	.003	.006	356
	Centered Leverage Value	.007	.087	.031	.016	356

a. Dependent Variable: AVG_MDSU

Figure 7 Histogram of the Dependent Variable MDSU

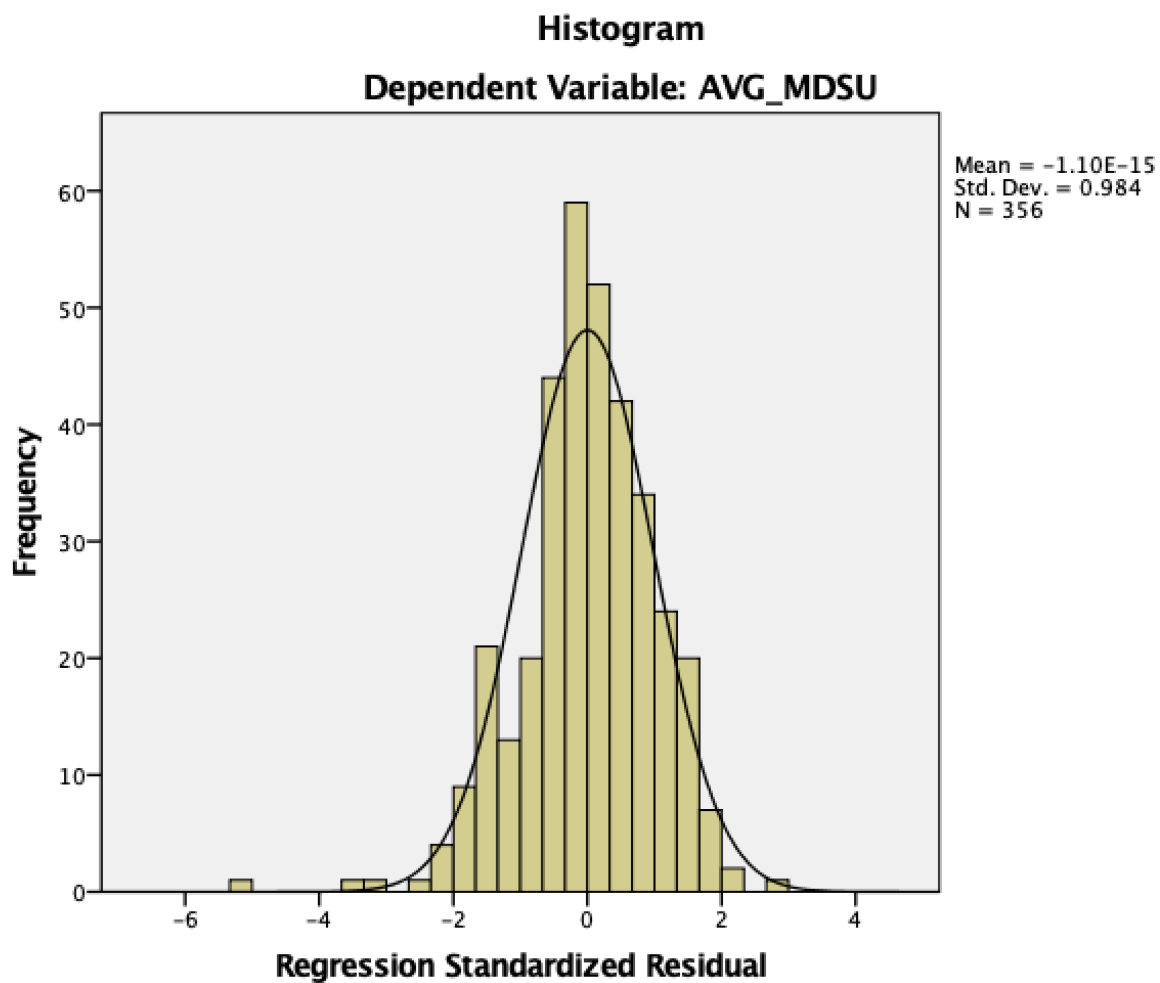
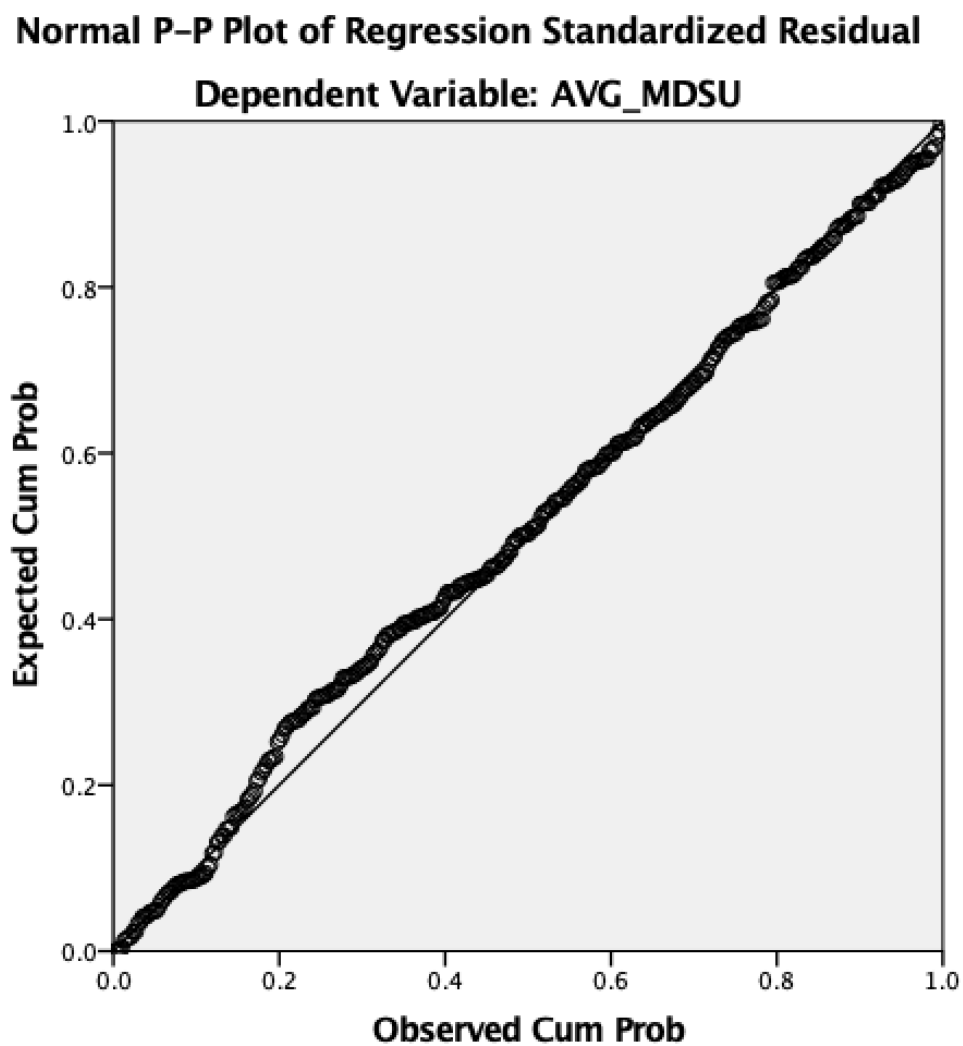


Figure 8 Normal P-P Plot of the Dependent Variable MDSU



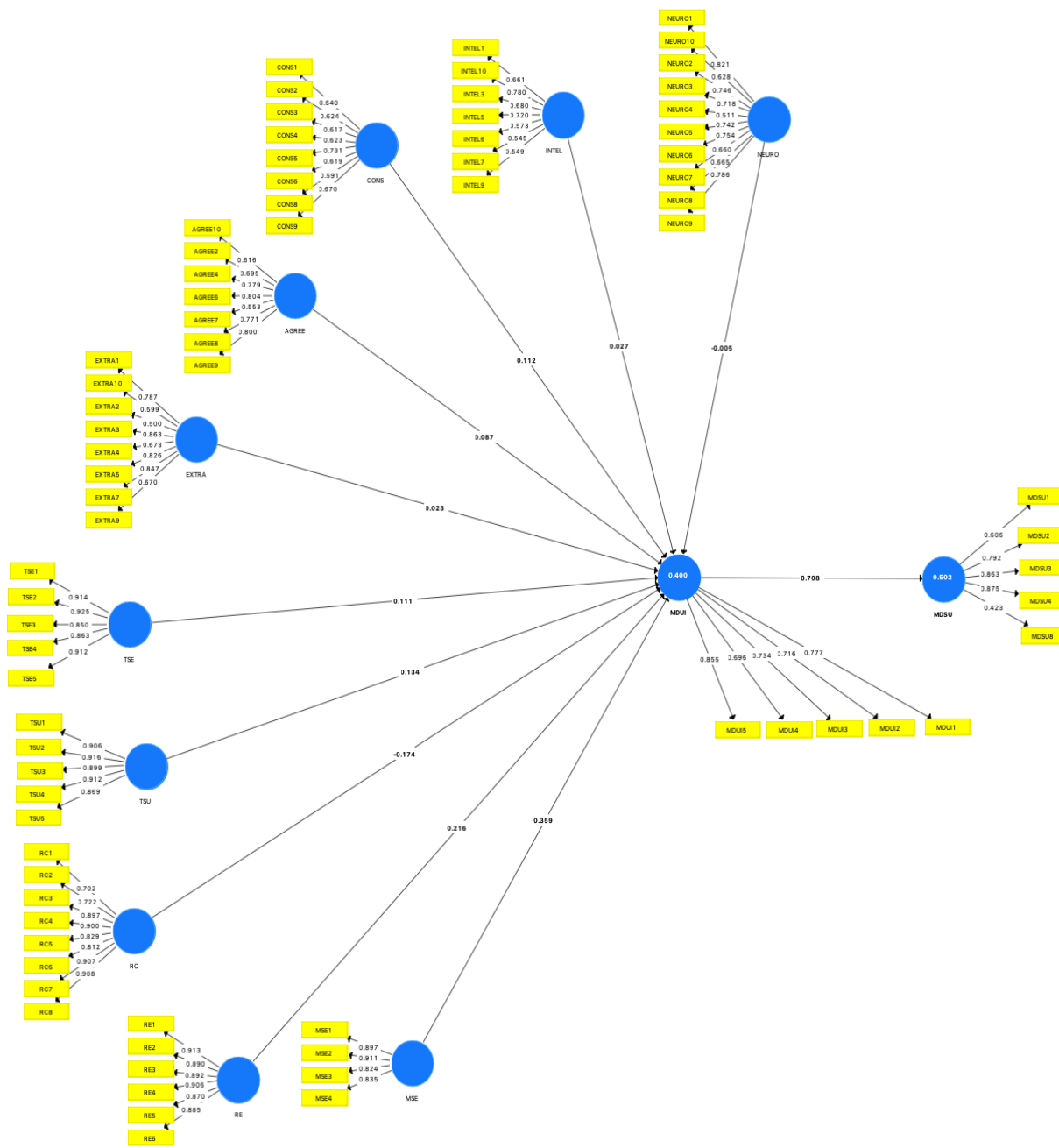
Appendix E

Table 6
Square Root of AVE and the Correlation Values among the Latent Variables

	AGREE	CONS	EXTRA	INTEL	MDSU	MDUI	MSE	NEURO	RC	RE	TSE	TSU
AGREE	0.723											
CONS	0.305	0.641										
EXTRA	0.378	0.228	0.731									
INTEL	0.472	0.348	0.455	0.649								
MDSU	0.104	0.226	0.143	0.242	0.732							
MDUI	0.237	0.269	0.145	0.291	0.708	0.757						
MSE	0.045	0.154	0.025	0.254	0.513	0.452	0.868					
NEURO	0.207	0.32	0.35	0.277	0.112	0.145	0.194	0.708				
RC	-0.077	-0.214	0.04	-0.137	-0.0195	-0.283	-0.204	-0.277	0.838			
RE	0.246	0.153	0.174	0.197	0.312	0.41	0.196	0.027	-0.207	0.893		
TSE	0.12	0.108	0.027	0.194	0.174	0.257	0.06	-0.093	-0.093	0.27	0.893	
TSU	0.002	-0.15	0.087	-0.026	0.115	0.074	-0.141	-0.244	-0.244	0.075	0.328	0.901

Appendix F

PLS- SEM Results





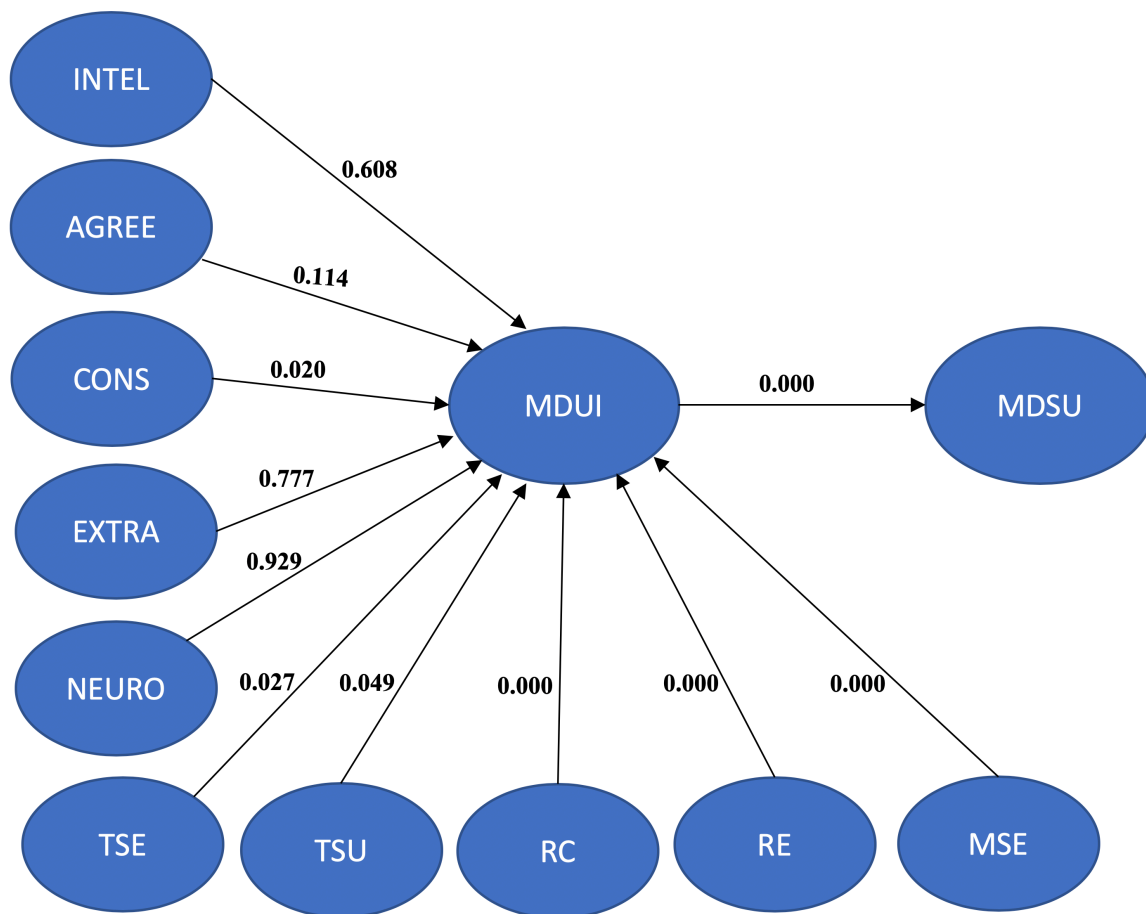
R Square Results

Matrix

	R Square	R Square Adjusted
MDSU	0.502	0.500
MDUI	0.400	0.382

Appendix G

Bootstrapping Significant Results



Path Coefficients

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O/STDEV)	P Values
AGREE -> MDUI	0.087	0.084	0.055	1.582	0.114
CONS -> MDUI	0.112	0.115	0.048	2.336	0.020
EXTRA -> MDUI	0.023	0.020	0.080	0.283	0.777
INTEL -> MDUI	0.027	0.026	0.052	0.514	0.608
MDUI -> MDSU	0.708	0.708	0.030	23.897	0.000
MSE -> MDUI	0.359	0.348	0.048	7.423	0.000
NEURO -> MDUI	-0.005	0.012	0.058	0.089	0.929
RC -> MDUI	-0.174	-0.178	0.046	3.773	0.000
RE -> MDUI	0.216	0.209	0.051	4.216	0.000
TSE -> MDUI	0.111	0.116	0.050	2.219	0.027
TSU -> MDUI	0.134	0.122	0.068	1.971	0.049

Total Effect

Mean, STDEV, T-Values, P-Values	Confidence Intervals	Confidence Intervals Bias Corrected	Samples		
	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (O/(STDEV))	P Values
AGREE -> MDSU	0.061	0.059	0.038	1.598	0.111
AGREE -> MDUI	0.087	0.084	0.055	1.582	0.114
CONS -> MDSU	0.079	0.082	0.035	2.289	0.022
CONS -> MDUI	0.112	0.115	0.048	2.336	0.020
EXTRA -> MDSU	0.016	0.014	0.056	0.284	0.776
EXTRA -> MDUI	0.023	0.020	0.080	0.283	0.777
INTEL -> MDSU	0.019	0.019	0.037	0.514	0.608
INTEL -> MDUI	0.027	0.026	0.052	0.514	0.608
MDUI -> MDSU	0.708	0.708	0.030	23.897	0.000
MSE -> MDSU	0.254	0.247	0.038	6.672	0.000
MSE -> MDUI	0.359	0.348	0.048	7.423	0.000
NEURO -> MDSU	-0.004	0.008	0.041	0.090	0.929
NEURO -> MDUI	-0.005	0.012	0.058	0.089	0.929
RC -> MDSU	-0.123	-0.126	0.033	3.706	0.000
RC -> MDUI	-0.174	-0.178	0.046	3.773	0.000
RE -> MDSU	0.153	0.148	0.037	4.185	0.000
RE -> MDUI	0.216	0.209	0.051	4.216	0.000
TSE -> MDSU	0.078	0.083	0.036	2.194	0.029
TSE -> MDUI	0.111	0.116	0.050	2.219	0.027
TSU -> MDSU	0.095	0.086	0.048	1.978	0.049
TSU -> MDUI	0.134	0.122	0.068	1.971	0.049

References

- Agarwal, R., Sambamurthy, V., & Stair, R. (2000). The Evolving Relationship between General and specific Computer Self-efficacy-an Empirical Assessment. *Journal of information system research*, 11(4), 418-430.
- Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. Berlin, Heidelberg: Springer.
- Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.
- Ajzen, I., Brown, T. & Carvajal, F. (2004). Explaining the discrepancy between intentions and actions: the case of hypothetical bias in contingent valuation. *Personality and Social Psychology Bulletin*, 30(9), 1108-1121.
- Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology*, 78(2), 201-211.
- Aliaga, M., & Gunderson, B. (2000). Interactive Statistics, 3rd Edition. New York, NY.
- Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., & Agarwal, Y. (2015). Your location has been shared 5,398 times: A field study on mobile app privacy nudging. *Proceedings of the 33rd annual ACM conference on human factor in computing systems*, Seoul, Republic of South Korea, 787-796.
- Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017). Information security behavior: Recognizing the influencers. *Proceedings of Computing Conference*, London, UK, 844-853.
- Alsaleh, M., Alomar, N., Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS One*, 12(3), 1-35.
- Anderson, C., & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of Home computer user security behavioral intentions. *MIS Quarterly* 34(3), 613-614.
- Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29, 706-714.
- Arachilage, N., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Journal of Computers in Human Behavior*, 38, 304 - 312.

- Bachmann, D., & Elfrink, J. (1996). Tracking the progress of e-mail versus snail-mail. *Marketing Research*, 8(2), 31-35.
- Bagozzi, R., Yi, Y., & Philipps, L. (1991). Assessing Construct Validity in Organizational Research. *Administrative Science Quarterly*, 36(3), 421- 458.
- Bandura, A. (1986). *Social foundations of thought and action*. Englewood Cliffs, NJ: Prentice Hall.
- Barrick, M.R., Mount, M.K., & Judge, T.A. (2001). Personality and Performance at the Beginning of the New Millennium: What Do We Know and Where Do We Go Next?. *International Journal of Selection and Assessment*, 9(1), 9-30.
- Belanger, F. & Crossler, R. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *Journal of Strategic Information Systems*, 28(1), 34-49.
- Bernroider, E., Krumay, B., & Margiol, S. (2014). Not without my smartphone! Impacts of Smartphone Addiction on Smartphone Usage. *Proceedings of the 25th Australasian Conference on Information Systems*, Auckland, New Zealand, 1-10.
- Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, 23(3), 253-264.
- Bethlehem J. (2010). Selection bias in Web surveys. *International Statistical Review*, 8(2), 161-188.
- Bishop, M. (2003). *Computer security: Art and science*. Boston, MA: Addison-Wesley Publishing.
- Boehmer, J., Larose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behavior: Towards an intervention strategy for college students. *Behavior & Information Technology*, 34(10), 1022-1035.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.
- Boudreau, M., D. Gefen, & D. Straub (2001). Validation in IS research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1-23.
- Bowling, N., & Burns, G. (2010). A comparison of work-specific and general personality measures as predictors of work and non-work criteria. *Personality and Individual Differences*, 48(2), 95-101.

- Bowling, N., & Eschleman, K. (2010). Employee personality as a moderator of the relationships between work stressors and counterproductive work behavior. *Journal of occupational health psychology, 15*(1), 91-103.
- Briggs, S.R. (1992). Assessing the Five-Factor Model of Personality Description. *Journal of Personalities, 60*(2), 253-293.
- Brown, J. D. (1996). *Testing in language programs*: Prentice Hall Regents New Jersey.
- Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68*, 190-209.
- Burns, B. R., (2000). *Introduction to research methods. 4ed.* Australia: Sage Publications Limited.
- Butt, S., & Phillips, J. G. (2008). Personality and self-reported mobile phone use. *Computers in Human Behavior, 24*, 346-360.
- Camadan, F., Reisoglu, I., Ursavas, O., & Mcilroy, D. (2018). How teachers' personality affect on their behavioral intention to use tablet PC. *The International Journal of Information and Learning Technology, 35*(1), 12-28.
- Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin, 56*(2), 81-105.
- Cappelleri, J., Darlington, R., & Trochim, W. (1994). Power Analysis of Cutoff-Based Randomized Clinical Trials. *Evaluation Review, 18*, 141-152.
- Carlton, M., & Levy, J. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. *Proceedings of the IEEE Southeast Conference*, Florida, USA, 1-6.
- Chen, X., Chen, L., & Wu, D. (2016). Factors that influence employees' security policy Compliance: An Awareness-Motivation-Capability Perspective. *Journal of Computer Information Systems, 1-13*.
- Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii International Conference on Systems Science*, Big Island, HI, 1-11.
- Cicchetti, D. V., Shoinralter, D., & Tyrer, P. J. (1985). The effect of number of rating scale categories on levels of interrater reliability: A Monte Carlo investigation. *Applied Psychological Measurement, 9*(1), 31-36.

- Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, 52(4), 20-29.
- Clarke, M. (2010). The Role of Self-Efficacy in Computer Security Behavior: Developing the Construct of Computer Security Self-Efficacy (CSSE). Available from ProQuest Dissertation and Theses database. (UMI No. 3434244).
- Cobanoglu, C., Moreo, P., & Warde, B. (2001). A Comparison of Mail, Fax and Web-Based Survey Methods. *International Journal of Market Research*, 43(4), 1-17.
- Cohen, J. (1992). Statistical power analysis. *Current Directions in Psychological Science*, 1(3), 98-101.
- Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (6th ed.). Oxford, UK: Routledge.
- Cook, D. (1977). Detection of Influential Observation in Linear Regression. *Journal of Technometrics*, 19(1), 1-18.
- Colwill, C. (2009). Human factors in information security: The insider threat - who can you trust these days. *Information security Technical Report*, 14(4), 186-196.
- Compeau, D. R., & Higgins, C. A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly*, 19(2), 189-211.
- Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Generalizability of information systems research using student subjects – a reflection of our practices and recommendations for future research. *Information Systems Research*, 23(4), 1093-1109.
- Comrey, A., & Lee, H. (1992). *A first course in factor analysis* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.
- Conner, M., & Abraham, C. (2001). Conscientiousness and the Theory of Planned Behavior: Toward a More Complete Model of the Antecedents of Intentions and Behavior. *Journal of Personality and Social Psychology*, 27(11), 1547-1561.
- Cooper, D. R., & Schindler, P. S. (2006). *Business research methods* (9th ed.). New York: McGraw-Hill.
- Correa, T., Hinsley, A. W., & Zuniga, H. G. (2010). Who Interacts on the Web. The intersection of users' personality and social media use. *Computers in Human Behavior*, 26(2), 247-253.
- Costa, P. T., & McCrae, R. R. (1992). NEO-PI-R Professional manual. Odessa, FL: Psychological Assessment Resources.

- Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5), 1849-1858.
- Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Upper Saddle River, New Jersey: Merrill Prentice Hall.
- Creswell, J. W. (2008). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage.
- Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research, 4th Edition*. Boston, MA: Pearson Education Inc.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches, 4th Edition*. Thousand Oaks, CA: Sage Publication.
- Crossler, R. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *Proceedings of the 43rd IEEE Hawaii International Conference on System Sciences (HICSS)*, Honolulu, HI, USA, 1-10.
- Crossler, R. E., & Belanger, F. (2014). An extended perspective on individual security behaviors: Protection Motivation Theory and a Unified Security Practices (USP) instrument. *The Database for Advances in Information Systems*, 45(4), 51-71.
- Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1-15.
- Crossler, R., Andoh-Baidoo, F., & Menard, P. (2018). Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of U.S. and Ghana. *Information & Management*, 1-13.
- Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computer and Security*, 32(1), 90-101.
- Crossler, R., Long, J., Loraas, T., & Trinkle, B. (2014). Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems*, 28(1), 209-226.
- D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model: Employee misuse of information technology resources. *Decision Sciences*, 43(6), 1091-1124.

- Dagon, D., Martin, T., & Starner, T. (2014). Mobile phones as computing devices: the viruses are coming. *Journal of IEEE Pervasive Computing*, 3(4), 1-5.
- Dane, F. C. (2011). *Evaluating research, 1st Edition*. Thousand Oaks, CA: Sage Publications.
- Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, 48, 281-297.
- Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security*, 24(1), 116-134.
- Devaraj, S., Easley, R., & Crant, M. (2008). How Does Personality Matter? Relating Five-Factor Model to Technology Acceptance and Use. *Information Systems Research*, 19(1), 93-115.
- Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration. *British Journal of Management*, 17(4), 263-282.
- Doane, A., Boothe, L., Pearson, M., & Kelley, M. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computer in Human Behavior*, 60, 508-513.
- Dolnicar, S. (2003). Simplifying three-way questionnaires - do the advantages of binary answer categories compensate for the Loss of information. *Proceedings of the (ANZMAC) Marketing Academy Conference*, Australia and New Zealand, 1-8.
- Dornyei, Z. (2007). *Research methods in applied linguistics*. New York: Oxford University Press.
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323-337.
- Emerson, E., Felce, D., & Stancliffe, R. J. (2013). Issues concerning self-report data and population-based data sets involving people with intellectual disabilities. *Journal of intellectual and developmental disabilities*, 51(5), 333-348.
- Etikan, I., Musa, S., & Alkassim, R. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4.
- Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behavior*, 26, 132-139.

- Farhadi, H., Fatimah, O., Nasir, R., & Shahrazad, W. S. (2012). Agreeableness and conscientiousness as antecedents of deviant behavior in workplace. *Asian Social Science*, 8(9), 1-6.
- FBI Internet Crime Report. (2018). IC3 Annual Report Released. Retrieved from <https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219>
- Ferdousi, B., & Levy, Y. (2010). Development and validation of a model to investigate the impact of individual factors on instructors' intention to use e-learning systems. *Interdisciplinary Journal of E-Learning and Learning Objects*, 6(1), 1-21.
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407-429.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 18(1), 39-50.
- Fry, R. B., & Prentice-Dunn, S. (2005). Effects of coping information and value affirmation on responses to a perceived health threat. *Health Communication*, 17(2), 133-147.
- Garton, L., Haythornthwaite, C., & Wellman, B. (1999). Studying online social networks. *Doing Internet Research: Critical Issues and Methods for Examining the Net*. London, United Kingdom: Sage Publications.
- Gay, L. R., Mills, G. E., & Airasian, P.W. (2009). *Educational research: Competencies for analysis and applications, student value edition*. Upper Saddle River, NJ: Merrill.
- Gefen, D., Straub, D., & Boudreau, M. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communications of AIS*, 7(7), 1-78.
- Gharehchopogh, F. S., Rezaei, R., & Maleki, I. (2013). Mobile cloud computing: Security challenges for threats reduction. *International Journal of Scientific & Engineering Research*, 4(3), 8-14.
- Giwah, A. (2018). Empirical Assessment of Mobile Device Users' Information Security Behavior towards Data Breach: Leveraging Protection Motivation Theory (Doctoral dissertation). Available from ProQuest Dissertation and Theses database. (UMI No. 13814783).

- Giwah, D. A. (2018). User Information Security Behavior Towards Data Breach in Bring Your Own Device (BYOD) Enabled Organizations - Leveraging Protection Motivation Theory. *Proceeding of IEEE Southeast Conference*, Florida, USA, 1-5.
- Goldberg, L. R. (1992). The development of markers for the Big-Five factor structure. *Psychological Assessment*, 4(1), 26-42.
- Goldberg, L. R. (1993). The structure of phenotypic personality traits. *American Psychologist*, 48(1), 26-34.
- Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, 41(3), 703-727.
- Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security*, 73, 345-358.
- Gray, P., & Hovav, A. (2014). Using scenarios to understand the frontiers of IS. *Information Systems Frontiers*, 16(3), 337-345.
- Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: A guide for non-statisticians. *International Journal of Endocrinology and Metabolism*, 10(2), 486-489.
- Gushta, M., & Rupp, A. (2010). Encyclopedia of research design edited by Salkind, N. J. Thousand Oaks, CA: SAGE.
- Gutteling, J. M., Terpstra, T., & Kerstholt, J. H. (2017). Citizens' adaptive or avoiding behavioral response to an emergency message on their mobile phone. *Journal of risk research*, 1466-4461.
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, 3(7), 1-18.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th Ed.). Upper Saddle River, NJ: Prentice Hall.
- Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). A primer on partial least squares structural equation modeling (PLS-SEM): Sage Publications.
- Han, X., Kwortnik Jr, R., & Wang, C. (2008). Service loyalty: An integrative model and examination across service contexts. *Journal of Service Research*, 11(1), 22-42.

- Harris, M. A., Furnell, S., & Patten, K. (2014). Comparing the mobile device security Behavior of college students and information technology professionals. *Journal of Information Privacy and Security*, 10(4), 186-202.
- Harris, M., Patten, K., & Regan, E. (2013). The Need for BYOD Mobile Device Security Awareness and Training. *Proceedings of the Nineteenth Americas Conference on Information Systems*, Chicago, USA, 1-11.
- Hayden, L. (2010). Human Information Security Behaviors: Differences across Geographies and Cultures in a Global User Survey. *Proceedings of the American Society for Information Science and Technology*, 46(1), 1-16.
- Heiervang, E., & Goodman, R. (2010). Advantages and limitations of Web-based surveys: evidence from a child mental health survey. *Social Psychiatry and Psychiatric Epidemiology*, 46, 69-76.
- Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2015). The use of partial least squares path modeling in international marketing. *Advances in International Marketing (AIM)*, 20, 277-320.
- Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.
- Holden, C., Dennie, T., & Hicks, A. (2013). Assessing the reliability of the M5-120 on Amazon's mechanical Turk. *Journal of Computers in Human Behavior*, 29(4), 1749-1754.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Computer & Security*, 31(1), 83-95.
- Ilies, R., & Dimotakis, N. (2015). *Genetic Influences on Attitudes, Behaviors, and Emotions in the Workplace*. The University of Chicago Press, Chicago, USA.
- Isaac, S., & Michael, W. B. (1995). *Handbook in research and evaluation*. San Diego, CA: Educational and Industrial Testing Services.
- Jeske, D., Briggs, P., Coventry, L. (2016). Exploring the relationship between impulsivity and decision-making on mobile devices. *Personal and Ubiquitous Computing*, 20(4), 545-557.
- John, O.P., Robins, R.W., & Pervin, L.A. (2008). *Handbook of Personality: Third Edition Theory and research*. New York: Guilford Press.

- Johnson, J. (2014). Measuring thirty facets of the Five Factor Model with a 120-item public domain inventory: Development of the IPIP-NEO-120. *Journal of Research in Personality*, 51, 78-89.
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.
- Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-134.
- Judge, T. A., & Erez, A. (2007). Interaction and intersection: The constellation of emotional stability and extraversion in predicting performance. *Personnel Psychology*, 60(3), 573-596.
- Judge, T. A., Higgins, C. A., Thoresen, C. J. & Barrick, M. R. (1999). The big five personality traits, general mental ability, and career success across the life span. *Personnel Psychology*, 52(3), 621-652.
- Judge, T. A., Weiss, H. M., Kammeyer-Mueller, J. D., & Hulin, C. L. (2017). Job attitudes, job satisfaction, and job affect: A century of continuity and of change. *Journal of Applied Psychology*, 102(3), 356-374.
- Julious, S. A. (2005). Sample size of 12 per group rule of thumb for a pilot study. *Pharmaceutical Statistics*, 4, 287-291.
- Junglas, I., Johnson, N., & Spitzmuller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4), 387-402.
- Kaspersky lab. (2014). Global IT Security Risks Survey. *Kaspersky Enterprise IT Security*. Retrieved from <https://www.kaspersky.com/blog/stolen-mobile-devices-how-much-of-this-is-personal-business/15001/>.
- Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile- computing self-efficacy in consumer information disclosure. *Information Systems Journal*, 25(6), 637-667.
- Knapp, H., & Kirk, S. A. (2003). Using pencil and paper, Internet, and touch-tone phones for self-administered surveys: Does methodology matter. *Journal of Computers in Human Behavior*, 19(1), 117-134.
- Koohang, A., Floyd, K., Rigole, N., Paliszkievicz, J. (2018). Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs. *Online Journal of Applied Knowledge Management*, 6(2), 1-16.

- Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, 48(4), 15-24.
- Kuhn, T. S. (1996). *The Structure of scientific revolutions*. Chicago, U.S.A.
- Kumar, R. (2010). *Research Methodology: A Step-by-Step Guide for Beginners*. London: SAGE Publications.
- Lattuch, F., & Young, S. (2011). Young professionals' perceptions toward organizational change. *Leadership & Organization Development Journal*, 32(6), 605-627.
- Lawson, A. E. (1985). A review of research on formal reasoning and science teaching. *Journal of Research in Science Teaching*, 22(7), 569-617.
- Leach, J. (2003). Improving user security behavior. *Computers & Security*, 22(8), 685-692.
- Leavitt, N. (2013). Today's mobile security requires a new approach. *Computer*, (11), 16-19.
- Lee, Y., & Larsen, K. (2009). Threat or coping appraisal: determinants of SMB executive's decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187.
- Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th Ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Leszczyna, R. (2013). Cost assessment of computer security activities. *Computer Fraud & Security*, 2013(7), 11-16.
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.
- Levy, Y., & Danet, T. (2010). Implementation success model in Government agencies: A case of a centralized identification system at NASA. *International journal of Information Systems in the Service Sector*, 2(2), 19-32.
- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science Journal*, 9, 181-212.
- Levy, Y., Ramin, M., & Hackney, R. (2013). Assessing Ethical Severity of e-Learning Systems Security Attacks. *Journal of Computer Information Systems*, 53(3), 1-11.

- Lewis-Beck, M., & Liao, T. F. (2014). The SAGE Encyclopedia of Social Science Research Methods. *Sage Research Methods*, 156-178.
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.
- Limayem, M., Hirt, S., & Cheung, C. (2007). How habit limits the predictive power of intention: the case of information systems continuance. *MIS Quarterly* 31(4), 705-737.
- Lowry, B. P., Posey, C., Bennet, J. R. & Roberts, L. T (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organizational information security policies: An empirical study of the influence of counterfactual reasoning and organizational trust. *Information Systems Journal*, 25, 193-230.
- Lwin, M., Li, B., & Ang., R. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of Adolescence*, 35(1), 31-41.
- Lynch, J. G. (1982). On the external validity of experiments in consumer research. *Journal of Consumer Research*, 9, 225-239.
- Mangione, T. (1995). *Mail surveys: Improving the quality*. Thousand Oaks, CA: Sage Publications, Inc.
- Marett, K., & Ratnamalala, N. (2012). Examining the coping appraisal process in end user security. Proceeding of ICIS Workshop on Information Security and Privacy (SIGSEC). Orlando, FL, 1-13.
- Matt, C., & Peckelsen, P. (2016). Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior. *Proceedings of the 49th International Conference on System Sciences (HICSS)*, Hawaii, USA, 4832-4841.
- McAbee, S. T., & Oswald, F. L. (2013). The criterion-related validity of personality measures for predicting GPA: A meta-analytic validity competition. *Psychological Assessment*, 25(2), 532-544.
- McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *Institute of Homeland Security Solutions*, 1-40.
- McComarc, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behaviors*, 69(19), 151-156.

- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Journal of Computers in Human Behavior*, 69, 151-156.
- McCrae, R. & Costa, P. (2013). Introduction to the empirical and theoretical status of the five-factor model of personality traits. Washington, DC, US: American Psychological Association.
- McCrae, R., & Costa, P. (1997). Personality trait structure as a human universal. *American Psychologist*, 52(5), 509-516.
- McCrae, R.R., & Terracciano, A. (2005). Personality profiles of cultures: Aggregate personality traits. *Journal of Personality and Social Psychology*, 89(3), 407-425.
- McElroy, J. C., Hendrickson, A. R., Townsend, A. M., & DeMarie, S. M. (2007). Dispositional factors in internet use e personality versus cognitive style. *MIS Quarterly*, 31(4), 809-820.
- McNeil, J. M., & Fleeson, W. (2006). The causal effects of extraversion on positive affect and neuroticism on negative affect: Manipulating state extraversion and state neuroticism in an experimental approach. *Journal of Research in Personality*, 40(5), 529-550.
- Menard, P., Warkentin, M., & Lowry (2018). The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination. *Computer and Security*, 75(10), 1-20.
- Mertler, C. A., & Reinhart, R. V. (2017). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). New York, NY: Routledge.
- Mertler, C., & Vannatta, R. A. (2013). *Advanced and multivariate statistical methods*. Glendale, CA: Pyrczak Publishing.
- Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3), 449-473.
- Monroe, A. (2000). *Essentials of political research*. Boulder, CO: Westview Press.
- Mou, J., Cohen, J., & Kim, J. (2017). A Meta-Analytic Structural Equation Modeling Test of Protection Motivation Theory in Information Security Literature. *Proceeding by the thirty-eight international Conference on information systems (ICIS), South Korea*.

- Mount, M., Ilies, R., & Johnson, E. (2006). Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction. *Personnel Psychology, 59*(3), 591-622.
- Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems, 42*, 147-182.
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Journal Computers and Security, 34*, 47-66.
- Norris, C. J., Larsen, J. T., & Cacioppo, J. T. (2007). Neuroticism is associated with larger and more prolonged electrodermal responses to emotionally evocative pictures. *Psychophysiology, 44*(5), 823-826.
- O'Neill, M. (2014). The Internet of things: Do more devices mean more risks? *Computer Fraud & Security, 1*, 16-17.
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, Design considerations and applications. *Information & management, 42*(1), 15-29.
- Ovelgönne, M., Dumitras, T., Prakash, B., Subrahmanian, V., & Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyber-attacks: A data-driven approach. *ACM Transactions on Intelligent Systems and Technology (TIST), 8*(4), 1-25.
- Patnayakuni, N., Patnayakuni, R., & Gupta, J. N. (2016). Towards a model of social media impacts on cybersecurity knowledge transfer: An exploration. *Harnessing Social Media as a Knowledge Management Tool, 249*, 1-23.
- Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security Behavior: An Australian Web-based study. In *Proceedings of the third human international conference on human aspects of information security, privacy, and trust*. Springer International Publishing, New York, NY, USA.
- Pew Research Center. (2019). Mobile Fact Sheet. Retrieved from <https://www.pewinternet.org/fact-sheet/mobile/>
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. *Computers & Security, 31*(4), 597-611.

- Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179-214.
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.
- Ratchford, M., & Wang, Y. (2019). BYOD-Insure: A Security Assessment Model for Enterprise BYOD. *Proceedings of the Fifth Conference on Mobile and Secure Services*, Florida, USA, 1-10.
- Rea, L. M., & Parker, R. A. (2014). *Designing and conducting survey research: A comprehensive guide (4th Ed.)*. San Francisco, CA: Jossey-Bass.
- Reynaldo, J. & Santos, A. (1999). Cronbach's alpha: A tool for assessing the reliability of scales. *Journal of Extension*, 37(2), 1-5.
- Ringle, C., Bido, D., & Silva, D. (2014). Structural Equation Modeling with the SmartPLS. *Brazilian Journal of Marketing*, 13(2), 56-73.
- Rippetoe, P., & Rogers, R.W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, 52(3), 596-604.
- Rizvi, S., Labrador, G., Hernandez, W., & Karpinski, K. (2016). Analysis of Mobile Threats and Security Vulnerabilities for Mobile Platforms and Devices. *Security, Privacy and Reliability in Computer Communications and Networks*, 139, 1-3.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114.
- Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochmans (Ed.). *Handbook of health behavior research* New York: Plenum.
- Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology*. New York: Guilford Press.
- Romer, H. (2014). Best practices for BYOD security. *Journal of Computer Fraud & Security*, 14(1), 13-15.
- Rosen, P.A., & Kluemper, D.H. (2008). The impact of the big five personality traits on the acceptance of social networking Website. *Proceedings of Americas Conference on Information Systems (AMCIS)*, Toronto, ON, 1-11.

- Rosenbaum, A., Rabenhorst, M. M., Reddy, M. K., Fleming, M. T., & Howells, N. L. (2006). A comparison of methods for collecting self-report data on sensitive topics. *Journal of Violence and Victims, 21*(4), 461-71.
- Rothmann, S., & Coetzer, E. (2003). The big five personality dimensions and job performance. *SA Journal of Industrial Psychology, 29*(1).
- Rovai, A.P., Baker, J.D., & Ponton, M.K.(2013). *Social science research design and statistics: A practitioner's guide to research methods and IBM SPSS*. Watertree Press LLC.
- Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting, 15*(4), 353-375.
- Sadler, G., Lee, H., Lim, R., & Fullerton, J. (2010). Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing and Health Sciences 12*(3), 369-374.
- Salgado, J. F. (2002). The Big Five personality dimensions and counterproductive behaviors. *International Journal of Selection and Assessment, 10*, 117-125.
- Salkind, Neil J. (2012). *Exploring research, 8th Edition*. Upper Saddle River, NJ: Pearson Education Inc.
- Samani, S. (2016). Steps in Research Process (Partial Least Square of Structural Equation Modeling (PLS-SEM)). *International Journal of Social Science and Business, 1*(2), 1-13.
- Saunders, M. Lewis, P. & Thornhill, A., (2003). *Research methods for business students* 3rd ed. Essex, England: Pearson Education Limited.
- Sekaran, U. (2003). *Research methods for business. A skill building approach* (4th ed.). New York, NY: John Wiley and Sons.
- Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill building approach*. New Jersey: John Willey and Sons.
- Sharma, N. (2013). Theoretical Framework for Corporate Disclosure Research. *Asian Journal of Finance & Accounting, 5*(1), 183-196.
- Sheeran, P. (2012). Intention-Behavior Relations: A Conceptual and Empirical Review. *Journal European Review of Social Psychology, 12*(1), 1-36.
- Shepherd, M. M., & Klein, G. (2012). Using deterrence to mitigate employee internet abuse. *Proceedings from the 45th Hawaii International Conference on System Sciences*, Maui, HI, USA.

- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Explaining initial adoption of information security behavior. *Computers & Security, 49*(0), 177-191.
- Shropshire, J., Warkentin, M., Johnston, A.C., & Schmidt, M.B. (2006). Personality and IT security: An application of the five-factor model. *Proceedings of the Americas Conference on Information Systems (AMCIS)*, Acapulco, Mexico, 1-8.
- Siponen, M., Mahmood, A., & Pahlila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*, 217-224.
- Skulmoski, G., Hartman, F., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education: Research, 6*(1), 1-21.
- Steiner, P. (2014). Going beyond mobile device management. *Journal of Computer Fraud & Security, 14*(4), 19-20.
- Stevens, J. (2007). *Intermediate statistics: A modern approach*. New York, NY. Lawrence Erlbaum Associates.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.
- Straub, D., Boudreau, M., & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the Association for Information Systems, 13*(1), 380-427.
- Sumsion T. (1998). The Delphi technique: an adaptive research tool. *British Journal of Occupational Therapy, 61*(4), 153-156.
- Sun, F., Omachi, S., Kato, N., Aso, H., Kono, S., & Takagi, T. (2000). Two-stage computational cost reduction algorithm based on Mahalanobis distance approximations. *Proceedings 15th International Conference on Pattern Recognition '00*, 700-703.
- Tabachnick, B., & Fidell, L. (2019). *Using Multivariate Statistics 7th Edition*. California State University Press.
- Terrell, S. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York, NY: The Guilford Press.
- Terzis, V., Moridis, C.N., & Economides, A.A. (2012). How student's personality traits affects computer-based assessment acceptance: integrating BFI with CBAAM. *Computers in Human Behavior, 28*(5), 1985-1996.

- Thompson, McGill, & Wang. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. *Computer & Security*, 70, 376-391.
- Toegel, G., & Barsoux, J. L. (2012). How to become a better leader. *MIT Sloan Management Review*, 53(3), 51-60.
- Torres-Perez, A., & March-Chorda, I. (2002). *Information systems and business strategy: a concurrent planning model*. Hershey, PA: Idea Publishing Group.
- Trochim, W. M. K. & Donnelly, J. P. (2008). *The research methods knowledge base* (3rd ed.). Mason, OH: Atomic Dog.
- Tsai, H., Jiang, M., Alhabash, S., LaRose, R., Rifon, N., & Cotton, S. (2016). Understanding online safety behaviors: a protection motivation theory perspective. *Computer & Security*, 59, 138-150.
- Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & Security*, 52, 128-141.
- Tu, Z., & Yuan, Y. (2012). Understanding user's behaviors in coping with security threat of mobile devices loss and theft. *Proceedings of the System Science (HICSS) Forty-Fifth International Conference*, Hawaii, USA, 1393-1402.
- Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52(4), 506-517.
- Turiano, N. A., Mroczek, D. K., Moynihan, J., & Chapman, B. P. (2013). Big 5 personality traits and Interleukin-6: Evidence for "healthy Neuroticism" in a US population sample. *Brain, Behavior and Immune Journal*, 28(11), 83-89.
- Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. *IEEE Workshop on Socio-Technical Aspects in Security and Trust*, 24-30.
- Uffen, J., Kaemmerer, N., & Breitner, M. H. (2013). Personality traits and cognitive determinants-An empirical investigation of the use of smartphone security measures. *Journal of Information Security*, 4(4), 203-212.
- Van belle, G. (2002). *Statistical rules of thumb*. New York: John Wiley.
- Van Teijlingen, E. & Hundley, V. (2002). The importance of pilot studies. *Nursing Standard*, 16(40), 33-36.

- Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49(3-4), 190-198.
- Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, 27(3), 425-478.
- Verkijika, S.P. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computer & Security*, 77, 860-870.
- Visinescu, L., Olajumoke, A., Sherry, R., Yu, W., & Dan, K. (2016). Better Safe than Sorry: A Study of Investigating Individuals' Protection of Privacy in the Use of Storage as a Cloud Computing Service. *International Journal of Human Computer Interaction*, 32(11), 1-17.
- Vogt, W. P. (2007). Quantitative research methods for professionals. Boston, MA: Pearson Education.
- Vroom, C., & Solms, R. V. (2004). Towards information security behavioral compliance. *Computer and Security*, 23(3), 191-198.
- Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 36(4), 531-542.
- Warkentin, M., McBride, M., Carter, L., & Johnston, A. (2012). The role of individual characteristics on insider abuse intentions. *Proceedings from the 28th Conference of Association for Information Systems*, Seattle, Washington, USA.
- Warkentin, M., Walden, E., Johnston, A., & Straub, D. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems*, 17(3), 1-22.
- Webb, T. L., & Sheeran, P. (2006). Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychological Bulletin*, 132(2), 249-268.
- Weiss, N. E., & Miller, R. S. (2015). The target and other financial data breaches: Frequently asked questions. In *Congressional Research Service, Prepared for Members and Committees of Congress*, 4, 1-14.
- Welk, A.K., Hong, K.W., Zielinska, O.A., Tembe, R., Murphy-Hill, E., Mayhorn, C.B. (2015). Will the Phisher-Men Reel You In. *International Journal of Cyber Behavior Psychology and Learning* 5(4), 1-17.

- Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, behavior, and social networking*, 18(1), 3-7.
- Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, 27(5), 591-615.
- Wong, K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Journal of marketing bulletin*, 24, 1-32.
- Woon, I., Tan, G., & Low, R. (2005). A protection Motivation Theory Approach to Home Wireless Security, 31, 367-380.
- Wyllys, R. (1978). Teaching Descriptive and Inferential Statistics in Library Schools. *Journal of Education for Librarianship*, 19(1), 3-20.
- Xu, R., Frey, R. M., Fleisch, E., & Ilic, A. (2016). Understanding the impact of personality traits on mobile app adoption Insights from a large-scale field study. *Computers in Human Behavior*, 62, 244-256.
- Yun, G., & Trumbo, C. (2000). Comparative Response to a Survey Executed by Post, E-mail, & Web Form. *Journal of Computer-Mediated Communication*, 6(1), 1-13.
- Zhang, L., & McDowell, WC. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet & Commerce*, 8(3), 180-197.
- Zikmund, W. G. (2013). *Business research methods, 9th Edition*. New York, NY: Dryden Press.
- Zikmund, W., Babin, B., Carr, J., & Griffin, M. (2012). *Business Research Methods (9ed)*: Business & Economics.